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

C. LEHR [1] M. MATIGNON[2]

[1]MPI Bonn [2]Laboratoire A2X Bordeaux

Séminaire "Variétés rationnelles"
Mai 2006

Plan

Introduction

Monodromie et groupes d'automorphismes

Groupes d'automorphismes des courbes en car.$p > 0$

Revêtements p -cycliques de la droite affi ne

Structure de $G_{\infty,1}(f)$

Bornes sur $|G_{\infty,1}(f)|$

Caractérisation de $G_{\infty,1}(f)$

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

Grosses actions (I)

Condition (N) et G_2

Surfaces de Riemann

Corps de classes de rayon

Grosses actions (II)

Courbes maximales

Références

Plan

Plan

Plan

Introduction

Monodromie et groupes d'automorphismes

Groupes d'automorphismes des courbes en car.$p > 0$

Revêtements p -cycliques de la droite affi ne

Structure de $G_{\infty,1}(f)$

Bornes sur $|G_{\infty,1}(f)|$

Caractérisation de $G_{\infty,1}(f)$

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

Grosses actions (I)

Condition (N) et G_2

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'inégales caractéristiques $(0, p)$.
  $K := \mathrm{Fr} R$; par exemple $K/\mathbb{Q}_p^{nr}$ finie.
  π une uniformisante.
  $k := R/\pi R$.
  C/K courbe projective lisse, $g(C) \geq 1$.
- 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'inégales caractéristiques $(0, p)$.
  $K := \mathrm{Fr}R$; par exemple $K/\mathbb{Q}_p^{nr}$ finie.
  π une uniformisante.
  $k := R/\pi R$.
  C/K courbe projective lisse, $g(C) \geq 1$.
- 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'inégales caractéristiques $(0, p)$.
  $K := \mathrm{Fr}R$; par exemple $K/\mathbb{Q}_p^{nr}$ finie.
  π une uniformisante.
  $k := R/\pi R$.
  C/K courbe projective lisse, $g(C) \geq 1$.
- 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'inégales caractéristiques $(0, p)$.
  $K := \mathrm{Fr}R$; par exemple $K/\mathbb{Q}_p^{nr}$ finie.
  π une uniformisante.
  $k := R/\pi R$.
  C/K courbe projective lisse, $g(C) \geq 1$.
- 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'inégales caractéristiques $(0, p)$.
  $K := \mathrm{Fr} R$; par exemple $K/\mathbb{Q}_p^{nr}$ finie.
  π une uniformisante.
  $k := R/\pi R$.
  C/K courbe projective lisse, $g(C) \geq 1$.
- 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 ℓ 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 ℓ^{n_ℓ} est majoré par l'ordre maximal d'un sous-groupe cyclique de $\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ i.e. $\ell^{n_\ell} \leq O(g)$.
- 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 (74).

- 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 ℓ 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 ℓ^{n_ℓ} est majoré par l'ordre maximal d'un sous-groupe cyclique de $\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ i.e. $\ell^{n_\ell} \leq O(g)$.
- 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 (74).

- 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 ℓ 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 ℓ^{n_ℓ} est majoré par l'ordre maximal d'un sous-groupe cyclique de $\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ i.e. $\ell^{n_\ell} \leq O(g)$.
- 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 (74).

- 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 ℓ 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 ℓ^{n_ℓ} est majoré par l'ordre maximal d'un sous-groupe cyclique de $\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ i.e. $\ell^{n_\ell} \leq O(g)$.
- 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 (74).

Revêtements p-cycliques de la droite affine

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

- $f(X) \in Xk[X]$,$(\deg f = m, p) = 1$, unitaire
- $C_f : w^p - w = f(X)$, ∞ 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 affine

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

- $f(X) \in Xk[X]$,$(\deg f = m, p) = 1$, unitaire
- $C_f : w^p - w = f(X)$, ∞ 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.** $p > 0$

- $f(X) \in Xk[X]$,$(\deg f = m, p) = 1$, unitaire
- $C_f : w^p - w = f(X)$, ∞ 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.** $p > 0$

- $f(X) \in Xk[X]$,$(\deg f = m, p) = 1$, unitaire
- $C_f : w^p - w = f(X)$, ∞ 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.** $p > 0$

- $f(X) \in Xk[X]$,$(\deg f = m, p) = 1$, unitaire
- $C_f : w^p - w = f(X)$, ∞ 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.** $p > 0$

- $f(X) \in Xk[X]$,$(\deg f = m, p) = 1$, unitaire
- $C_f : w^p - w = f(X)$, ∞ 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 $m|1+p$.

Structure de $G_{\infty,1}(f)$

- 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 $V = \{\tau_y |\ \tau_y(X) = X + y,\ y \in k\}$.
  $f(X + y) = f(X) + f(y) + (F - \mathrm{Id})(P(X, y))$
  $P(X, y) \in Xk[X]$
  $V \simeq (\mathbb{Z}/p\mathbb{Z})^v$ en tant que sous-groupe de k.
- $[\tau_y, \tau_z] = \rho^{\epsilon(y,z)}$ où $\epsilon : V \times V \to \mathbb{F}_p$ est une forme alternée.
- ϵ est non dégénérée ssi $< \rho >= Z(G_{\infty,1})$.

Structure de $G_{\infty,1}(f)$

- 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
  $V = \{\tau_y | \, \tau_y(X) = X + y, \; y \in k\}$.
  $f(X + y) = f(X) + f(y) + (F - \mathrm{Id})(P(X, y))$
  $P(X, y) \in Xk[X]$
  $V \simeq (\mathbb{Z}/p\mathbb{Z})^v$ en tant que sous-groupe de k.
- $[\tau_y, \tau_z] = \rho^{\epsilon(y,z)}$ où $\epsilon : V \times V \to \mathbb{F}_p$ est une forme alternée.
- ϵ est non dégénérée ssi $< \rho >= Z(G_{\infty,1})$.

Structure de $G_{\infty,1}(f)$

- 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
  $V = \{\tau_y | \ \tau_y(X) = X + y, \ y \in k\}$.
  $f(X+y) = f(X) + f(y) + (F - \mathrm{Id})(P(X,y))$
  $P(X,y) \in Xk[X]$
  $V \simeq (\mathbb{Z}/p\mathbb{Z})^v$ en tant que sous-groupe de k.
- $[\tau_y, \tau_z] = \rho^{\epsilon(y,z)}$ où $\epsilon : V \times V \to \mathbb{F}_p$ est une forme alternée.
- ϵ est non dégénérée ssi $< \rho >= Z(G_{\infty,1})$.

Structure de $G_{\infty,1}(f)$

- 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
  $V = \{\tau_y |\ \tau_y(X) = X + y,\ y \in k\}$.
  $f(X+y) = f(X) + f(y) + (F - \mathrm{Id})(P(X,y))$
  $P(X,y) \in Xk[X]$
  $V \simeq (\mathbb{Z}/p\mathbb{Z})^v$ en tant que sous-groupe de k.
- $[\tau_y, \tau_z] = \rho^{\epsilon(y,z)}$ où $\epsilon : V \times V \to \mathbb{F}_p$ est une forme alternée.
- ϵ est non dégénérée ssi $< \rho >= Z(G_{\infty,1})$.

Bornes sur $|G_{\infty,1}(f)|$

Lemme: Si $f(X)=\sum_{1\leq i\leq m} t_i X^i \in k[X]$, unitaire, alors

- $\Delta(f)(X,Y) := f(X+Y)-f(X)-f(Y) = R(X,Y)+(F-\mathrm{Id})(P_f(X,Y))$ avec $R \in \bigoplus_{\lfloor \frac{m}{p}\rfloor \leq ip^{n(i)}<m,\ (i,p)=1} k[Y]X^{ip^{n(i)}}$ et $P_f \in Xk[X,Y]$.
- $P_f = (\mathrm{Id}+F+\ldots+F^{n-1})(\Delta(f)) \mod X^{[\frac{m-1}{p}]+1}$
- On note $\mathrm{Ad}_f(Y)$ le contenu du polynôme $R(X,Y)\in k[Y][X]$.
- $\mathrm{Ad}_f(Y)$ est un polynôme additif séparable
- $Z(\mathrm{Ad}_f(Y)) \simeq V$.

Bornes sur $|G_{\infty,1}(f)|$

Lemme: Si $f(X) = \sum_{1\leq i\leq m} t_i X^i \in k[X]$, unitaire, alors

- $\Delta(f)(X,Y) := f(X+Y) - f(X) - f(Y) = R(X,Y) + (F - \mathrm{Id})(P_f(X,Y))$ avec $R \in \bigoplus_{\lfloor \frac{m}{p} \rfloor \leq ip^{n(i)} < m,\ (i,p)=1} k[Y]X^{ip^{n(i)}}$ et $P_f \in Xk[X,Y]$.
- $P_f = (\mathrm{Id} + F + \ldots + F^{n-1})(\Delta(f)) \mod X^{[\frac{m-1}{p}]+1}$
- On note $\mathrm{Ad}_f(Y)$ le contenu du polynôme $R(X,Y) \in k[Y][X]$.
- $\mathrm{Ad}_f(Y)$ est un polynôme additif séparable
- $Z(\mathrm{Ad}_f(Y)) \simeq V$.

Bornes sur $|G_{\infty,1}(f)|$

Lemme: Si $f(X) = \sum_{1\leq i\leq m} t_i X^i \in k[X]$, unitaire, alors

- $\Delta(f)(X,Y) := f(X+Y) - f(X) - f(Y) = R(X,Y) + (F - \mathrm{Id})(P_f(X,Y))$ avec $R \in \bigoplus_{\lfloor \frac{m}{p} \rfloor \leq ip^{n(i)} < m,\ (i,p)=1} k[Y]X^{ip^{n(i)}}$ et $P_f \in Xk[X,Y]$.
- $P_f = (\mathrm{Id} + F + ... + F^{n-1})(\Delta(f)) \mod X^{[\frac{m-1}{p}]+1}$
- On note $\mathrm{Ad}_f(Y)$ le contenu du polynôme $R(X,Y) \in k[Y][X]$.
- $\mathrm{Ad}_f(Y)$ est un polynôme additif séparable
- $Z(\mathrm{Ad}_f(Y)) \simeq V$.

Bornes sur $|G_{\infty,1}(f)|$

Lemme: Si $f(X) = \sum_{1\leq i\leq m} t_i X^i \in k[X]$, unitaire, alors

- $\Delta(f)(X,Y) := f(X+Y) - f(X) - f(Y) = R(X,Y) + (F - \mathrm{Id})(P_f(X,Y))$ avec $R \in \bigoplus_{\lfloor \frac{m}{p} \rfloor \leq ip^{n(i)} < m,\ (i,p)=1} k[Y] X^{ip^{n(i)}}$ et $P_f \in Xk[X,Y]$.
- $P_f = (\mathrm{Id} + F + \ldots + F^{n-1})(\Delta(f)) \mod X^{[\frac{m-1}{p}]+1}$
- On note $\mathrm{Ad}_f(Y)$ le contenu du polynôme $R(X,Y) \in k[Y][X]$.
- $\mathrm{Ad}_f(Y)$ est un polynôme additif séparable
- $Z(\mathrm{Ad}_f(Y)) \simeq V$.

Bornes sur $|G_{\infty,1}(f)|$

Lemme: Si $f(X) = \sum_{1\le i\le m} t_i X^i \in k[X]$, unitaire, alors

- $\Delta(f)(X,Y) := f(X+Y) - f(X) - f(Y) = R(X,Y) + (F - \mathrm{Id})(P_f(X,Y))$ avec $R \in \bigoplus_{\lfloor \frac{m}{p} \rfloor \le ip^{n(i)} < m,\ (i,p)=1} k[Y]X^{ip^{n(i)}}$ et $P_f \in Xk[X,Y]$.
- $P_f = (\mathrm{Id} + F + \dots + F^{n-1})(\Delta(f)) \mod X^{[\frac{m-1}{p}]+1}$
- On note $\mathrm{Ad}_f(Y)$ le contenu du polynôme $R(X,Y) \in k[Y][X]$.
- $\mathrm{Ad}_f(Y)$ est un polynôme additif séparable
- $Z(\mathrm{Ad}_f(Y)) \simeq V$.

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. $\frac{|G_{\infty,1}|}{g^2} \leq \frac{4p}{(p-1)^2}$
- ([St] 73) $s=0$, i.e. $(m-1,p)=1$, alors $|G_{\infty,1}|=p$
- $s>0$
  - $\ell>1$, $p=2$, alors $\frac{|G_{\infty,1}|}{g} \leq \frac{2}{3}$
  - $\ell>1$, $p>2$, alors $\frac{|G_{\infty,1}|}{g} \leq \frac{p}{p-1}$
  - ([St]) $\ell=1$, $m=1+p^s$ alors $\frac{|G_{\infty,1}|}{g} \leq 2p^s\frac{p}{p-1}$ (égalité pour $f(X)=X^{1+p^s}$)

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. $\frac{|G_{\infty,1}|}{g^2} \leq \frac{4p}{(p-1)^2}$
- ([St] 73) $s = 0$, i.e. $(m-1, p) = 1$, alors $|G_{\infty,1}| = p$
- $s > 0$
  - $\ell > 1$, $p = 2$, alors $\frac{|G_{\infty,1}|}{g} \leq \frac{2}{3}$
  - $\ell > 1$, $p > 2$, alors $\frac{|G_{\infty,1}|}{g} \leq \frac{p}{p-1}$
  - ([St]) $\ell = 1$, $m = 1 + p^s$ alors $\frac{|G_{\infty,1}|}{g} \leq 2p^s \frac{p}{p-1}$ (égalité pour $f(X) = X^{1+p^s}$)

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. $\frac{|G_{\infty,1}|}{g^2} \leq \frac{4p}{(p-1)^2}$
- ([St] 73) $s=0$, i.e. $(m-1,p)=1$, alors $|G_{\infty,1}|=p$
- $s>0$
  - $\ell>1$, $p=2$, alors $\frac{|G_{\infty,1}|}{g} \leq \frac{2}{3}$
  - $\ell>1$, $p>2$, alors $\frac{|G_{\infty,1}|}{g} \leq \frac{p}{p-1}$
  - ([St]) $\ell=1$, $m=1+p^s$ alors $\frac{|G_{\infty,1}|}{g} \leq 2p^s\frac{p}{p-1}$ (égalité pour $f(X)=X^{1+p^s}$)

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. $\frac{|G_{\infty,1}|}{g^2}\leq\frac{4p}{(p-1)^2}$
- ([St] 73) $s=0$, i.e. $(m-1,p)=1$, alors $|G_{\infty,1}|=p$
- $s>0$
  - $\ell>1$, $p=2$, alors $\frac{|G_{\infty,1}|}{g}\leq\frac{2}{3}$
  - $\ell>1$, $p>2$, alors $\frac{|G_{\infty,1}|}{g}\leq\frac{p}{p-1}$
  - ([St]) $\ell=1$, $m=1+p^s$ alors $\frac{|G_{\infty,1}|}{g}\leq 2p^s\frac{p}{p-1}$ (égalité pour $f(X)=X^{1+p^s}$)

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. $\frac{|G_{\infty,1}|}{g^2}\leq\frac{4p}{(p-1)^2}$
- ([St] 73) $s=0$, i.e. $(m-1,p)=1$, alors $|G_{\infty,1}|=p$
- $s>0$
  - $\ell>1$, $p=2$, alors $\frac{|G_{\infty,1}|}{g}\leq\frac{2}{3}$
  - $\ell>1$, $p>2$, alors $\frac{|G_{\infty,1}|}{g}\leq\frac{p}{p-1}$
  - ([St]) $\ell=1$, $m=1+p^s$ alors $\frac{|G_{\infty,1}|}{g}\leq 2p^s\frac{p}{p-1}$ (égalité pour $f(X)=X^{1+p^s}$)

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. $\frac{|G_{\infty,1}|}{g^2} \leq \frac{4p}{(p-1)^2}$
- ([St] 73) $s=0$, i.e. $(m-1,p)=1$, alors $|G_{\infty,1}|=p$
- $s>0$
  - $\ell>1$, $p=2$, alors $\frac{|G_{\infty,1}|}{g} \leq \frac{2}{3}$
  - $\ell>1$, $p>2$, alors $\frac{|G_{\infty,1}|}{g} \leq \frac{p}{p-1}$
  - ([St]) $\ell=1$, $m=1+p^s$ alors $\frac{|G_{\infty,1}|}{g} \leq 2p^s\frac{p}{p-1}$ (égalité pour $f(X)=X^{1+p^s}$)

Caractérisation de $G_{\infty,1}(f)$

- Considérons les extensions de p-groupes du type $0 \to Z/p\mathbb{Z} \to G \to (\mathbb{Z}/p\mathbb{Z})^n \to 0$ (en particulier, $G_{\infty,1}(f)$ est de ce type). Alors $G' \subset Z(G)$.
- Si $G' = Z(G)$, on dit que G est extraspécial.
  - Alors $|G| = p^{2s+1}$. Il y a 2 classes d'isomorphisme pour s donné.
  - Si $p > 2$, on note $E(p^3)$ (resp. $M(p^3)$) le groupe non abélien d'ordre p^3 d'exposant p (resp. p^2). Alors $G \simeq E(p^3) * E(p^3) * \ldots * E(p^3)$ ou $M(p^3) * E(p^3) * \ldots * E(p^3)$ suivant que l'exposant est p ou p^2.
  - Si $p = 2$, alors $G \simeq D_8 * D_8 * \ldots * D_8$ ou bien $Q_8 * D_8 * \ldots * D_8$ (dans les 2 cas, l'exposant est 2^2)
- Si $G' \subset Z(G)$, G est sous-groupe d'un groupe extraspécial E avec $Z(E) \subset G$.

Caractérisation de $G_{\infty,1}(f)$

- Considérons les extensions de p-groupes du type $0 \to Z/p\mathbb{Z} \to G \to (\mathbb{Z}/p\mathbb{Z})^n \to 0$ (en particulier, $G_{\infty,1}(f)$ est de ce type). Alors $G' \subset Z(G)$.
- Si $G' = Z(G)$, on dit que G est extraspécial.
  - Alors $|G| = p^{2s+1}$. Il y a 2 classes d'isomorphisme pour s donné.
  - Si $p > 2$, on note $E(p^3)$ (resp. $M(p^3)$) le groupe non abélien d'ordre p^3 d'exposant p (resp. p^2). Alors $G \simeq E(p^3) * E(p^3) * \ldots * E(p^3)$ ou $M(p^3) * E(p^3) * \ldots * E(p^3)$ suivant que l'exposant est p ou p^2.
  - Si $p = 2$, alors $G \simeq D_8 * D_8 * \ldots * D_8$ ou bien $Q_8 * D_8 * \ldots * D_8$ (dans les 2 cas, l'exposant est 2^2)
- Si $G' \subset Z(G)$, G est sous-groupe d'un groupe extraspécial E avec $Z(E) \subset G$.

Caractérisation de $G_{\infty,1}(f)$

- Considérons les extensions de p-groupes du type $0 \to Z/p\mathbb{Z} \to G \to (\mathbb{Z}/p\mathbb{Z})^n \to 0$ (en particulier, $G_{\infty,1}(f)$ est de ce type). Alors $G' \subset Z(G)$.
- Si $G' = Z(G)$, on dit que G est extraspécial.
  - Alors $|G| = p^{2s+1}$. Il y a 2 classes d'isomorphisme pour s donné.
  - Si $p > 2$, on note $E(p^3)$ (resp. $M(p^3)$) le groupe non abélien d'ordre p^3 d'exposant p (resp. p^2). Alors $G \simeq E(p^3) * E(p^3) * \ldots * E(p^3)$ ou $M(p^3) * E(p^3) * \ldots * E(p^3)$ suivant que l'exposant est p ou p^2.
  - Si $p = 2$, alors $G \simeq D_8 * D_8 * \ldots * D_8$ ou bien $Q_8 * D_8 * \ldots * D_8$ (dans les 2 cas, l'exposant est 2^2)
- Si $G' \subset Z(G)$, G est sous-groupe d'un groupe extraspécial E avec $Z(E) \subset G$.

Caractérisation de $G_{\infty,1}(f)$

- Considérons les extensions de p-groupes du type $0 \to Z/p\mathbb{Z} \to G \to (\mathbb{Z}/p\mathbb{Z})^n \to 0$ (en particulier, $G_{\infty,1}(f)$ est de ce type). Alors $G' \subset Z(G)$.
- Si $G' = Z(G)$, on dit que G est extraspécial.
  - Alors $|G| = p^{2s+1}$. Il y a 2 classes d'isomorphisme pour s donné.
  - Si $p > 2$, on note $E(p^3)$ (resp. $M(p^3)$) le groupe non abélien d'ordre p^3 d'exposant p (resp. p^2). Alors $G \simeq E(p^3) * E(p^3) * ... * E(p^3)$ ou $M(p^3) * E(p^3) * ... * E(p^3)$ suivant que l'exposant est p ou p^2.
  - Si $p = 2$, alors $G \simeq D_8 * D_8 * ... * D_8$ ou bien $Q_8 * D_8 * ... * D_8$ (dans les 2 cas, l'exposant est 2^2)
- Si $G' \subset Z(G)$, G est sous-groupe d'un groupe extraspécial E avec $Z(E) \subset G$.

Caractérisation de $G_{\infty,1}(f)$

- Considérons les extensions de p-groupes du type $0 \to Z/p\mathbb{Z} \to G \to (\mathbb{Z}/p\mathbb{Z})^n \to 0$ (en particulier, $G_{\infty,1}(f)$ est de ce type). Alors $G' \subset Z(G)$.
- Si $G' = Z(G)$, on dit que G est extraspécial.
  - Alors $|G| = p^{2s+1}$. Il y a 2 classes d'isomorphisme pour s donné.
  - Si $p > 2$, on note $E(p^3)$ (resp. $M(p^3)$) le groupe non abélien d'ordre p^3 d'exposant p (resp. p^2). Alors $G \simeq E(p^3) * E(p^3) * \ldots * E(p^3)$ ou $M(p^3) * E(p^3) * \ldots * E(p^3)$ suivant que l'exposant est p ou p^2.
  - Si $p = 2$, alors $G \simeq D_8 * D_8 * \ldots * D_8$ ou bien $Q_8 * D_8 * \ldots * D_8$ (dans les 2 cas, l'exposant est 2^2)
- Si $G' \subset Z(G)$, G est sous-groupe d'un groupe extraspécial E avec $Z(E) \subset G$.

Caractérisation de $G_{\infty,1}(f)$

- Considérons les extensions de p-groupes du type $0 \to Z/p\mathbb{Z} \to G \to (\mathbb{Z}/p\mathbb{Z})^n \to 0$ (en particulier, $G_{\infty,1}(f)$ est de ce type). Alors $G' \subset Z(G)$.
- Si $G' = Z(G)$, on dit que G est extraspécial.
  - Alors $|G| = p^{2s+1}$. Il y a 2 classes d'isomorphisme pour s donné.
  - Si $p > 2$, on note $E(p^3)$ (resp. $M(p^3)$) le groupe non abélien d'ordre p^3 d'exposant p (resp. p^2). Alors $G \simeq E(p^3) * E(p^3) * \ldots * E(p^3)$ ou $M(p^3) * E(p^3) * \ldots * E(p^3)$ suivant que l'exposant est p ou p^2.
  - Si $p = 2$, alors $G \simeq D_8 * D_8 * \ldots * D_8$ ou bien $Q_8 * D_8 * \ldots * D_8$ (dans les 2 cas, l'exposant est 2^2)
- Si $G' \subset Z(G)$, G est sous-groupe d'un groupe extraspécial E avec $Z(E) \subset G$.

- Théorème. Si $f(X) = X\Sigma(F)(X) \in k[x]$, $\Sigma(F) = \sum_{0 \leq i \leq s} a_i F^i \in k\{F\}$ un polynôme additif avec $\deg f = 1 + p^s$, alors
  - $\mathrm{Ad}_f(Y) = F^s(\sum_{0 \leq i \leq s}(a_i F^i + F^{-i} a_i)(Y))$
  - $G_{\infty,1}(f)$ est un groupe extraspécial de cardinal p^{2s+1}, d'exposant p si $p > 2$ et du type $Q_8 * D_8 * \ldots * D_8$ si $p = 2$.
- Théorème. Si G est extension du type $0 \to \mathbb{Z}/p\mathbb{Z} \to G \to (\mathbb{Z}/p\mathbb{Z})^n \to 0$, il existe $f \in Xk[X]$ avec $G \simeq G_{\infty,1}(f)$.
- Idée:
  - Les groupes extraspéciaux d'exposant p^2 sont obtenus en modifiant le polynôme f du théorème précédent par un cocycle de Witt.
  - Si G est sous-groupe d'un groupe extraspécial E, on réalise E avec f_E comme dans le cas précédent et une modification convenable de f_E limite $G_{\infty,1}$ à G.

- Théorème. Si $f(X) = X\Sigma(F)(X) \in k[x]$, $\Sigma(F) = \sum_{0 \le i \le s} a_i F^i \in k\{F\}$ un polynôme additif avec $\deg f = 1 + p^s$, alors
  - $\mathrm{Ad}_f(Y) = F^s(\sum_{0 \le i \le s}(a_i F^i + F^{-i} a_i)(Y))$
  - $G_{\infty,1}(f)$ est un groupe extraspécial de cardinal p^{2s+1}, d'exposant p si $p > 2$ et du type $Q_8 * D_8 * \ldots * D_8$ si $p = 2$.
- Théorème. Si G est extension du type $0 \to \mathbb{Z}/p\mathbb{Z} \to G \to (\mathbb{Z}/p\mathbb{Z})^n \to 0$, il existe $f \in Xk[X]$ avec $G \simeq G_{\infty,1}(f)$.
- Idée:
  - Les groupes extraspéciaux d'exposant p sont obtenus en modifiant le polynôme f du théorème précédent par un cocycle de Witt.
  - Si G est sous-groupe d'un groupe extraspécial E, on réalise E avec f_E comme dans le cas précédent et une modification convenable de f_E limite $G_{\infty,1}$ à G.

- Théorème. Si $f(X) = X\Sigma(F)(X) \in k[x]$, $\Sigma(F) = \sum_{0 \leq i \leq s} a_i F^i \in k\{F\}$ un polynôme additif avec $\deg f = 1 + p^s$, alors
  - $\mathrm{Ad}_f(Y) = F^s(\sum_{0 \leq i \leq s}(a_i F^i + F^{-i} a_i)(Y))$
  - $G_{\infty,1}(f)$ est un groupe extraspécial de cardinal p^{2s+1}, d'exposant p si $p > 2$ et du type $Q_8 * D_8 * \ldots * D_8$ si $p = 2$.
- Théorème. Si G est extension du type $0 \to \mathbb{Z}/p\mathbb{Z} \to G \to (\mathbb{Z}/p\mathbb{Z})^n \to 0$, il existe $f \in Xk[X]$ avec $G \simeq G_{\infty,1}(f)$.
- Idée:
  - Les groupes extraspéciaux d'exposant p^2 sont obtenus en modifiant le polynôme f du théorème précédent par un cocycle de Witt.
  - Si G est sous-groupe d'un groupe extraspécial E, on réalise E avec f_E comme dans le cas précédent et une modification convenable de f_E limite $G_{\infty,1}$ à G.

- Théorème. Si $f(X) = X\Sigma(F)(X) \in k[x]$, $\Sigma(F) = \sum_{0\leq i\leq s} a_i F^i \in k\{F\}$ un polynôme additif avec $\deg f = 1 + p^s$, alors
  - $\mathrm{Ad}_f(Y) = F^s(\sum_{0\leq i\leq s}(a_i F^i + F^{-i} a_i)(Y))$
  - $G_{\infty,1}(f)$ est un groupe extraspécial de cardinal p^{2s+1}, d'exposant p si $p > 2$ et du type $Q_8 * D_8 * \dots * D_8$ si $p = 2$.
- Théorème. Si G est extension du type $0 \to \mathbb{Z}/p\mathbb{Z} \to G \to (\mathbb{Z}/p\mathbb{Z})^n \to 0$, il existe $f \in Xk[X]$ avec $G \simeq G_{\infty,1}(f)$.
- Idée:
  - Les groupes extraspéciaux d'exposant p^2 sont obtenus en modifi ant le polynôme f du théorème précédent par un cocycle de Witt.
  - Si G est sous-groupe d'un groupe extraspécial E, on réalise E avec f_E comme dans le cas précédent et une modifi cation convenable de f_E limite $G_{\infty,1}$ à G.

- Théorème. Si $f(X) = X\Sigma(F)(X) \in k[x]$, $\Sigma(F) = \sum_{0\leq i\leq s} a_i F^i \in k\{F\}$ un polynôme additif avec $\deg f = 1 + p^s$, alors
  - $\mathrm{Ad}_f(Y) = F^s(\sum_{0\leq i\leq s}(a_i F^i + F^{-i} a_i)(Y))$
  - $G_{\infty,1}(f)$ est un groupe extraspécial de cardinal p^{2s+1}, d'exposant p si $p > 2$ et du type $Q_8 * D_8 * \ldots * D_8$ si $p = 2$.
- Théorème. Si G est extension du type $0 \to \mathbb{Z}/p\mathbb{Z} \to G \to (\mathbb{Z}/p\mathbb{Z})^n \to 0$, il existe $f \in Xk[X]$ avec $G \simeq G_{\infty,1}(f)$.
- Idée:
  - Les groupes extraspéciaux d'exposant p^2 sont obtenus en modifi ant le polynôme f du théorème précédent par un cocycle de Witt.
  - Si G est sous-groupe d'un groupe extraspécial E, on réalise E avec f_E comme dans le cas précédent et une modifi cation convenable de f_E limite $G_{\infty,1}$ à G.

- Théorème. Si $f(X) = X\Sigma(F)(X) \in k[x]$, $\Sigma(F) = \sum_{0\leq i\leq s} a_i F^i \in k\{F\}$ un polynôme additif avec $\deg f = 1 + p^s$, alors
  - $\mathrm{Ad}_f(Y) = F^s(\sum_{0\leq i\leq s}(a_i F^i + F^{-i} a_i)(Y))$
  - $G_{\infty,1}(f)$ est un groupe extraspécial de cardinal p^{2s+1}, d'exposant p si $p > 2$ et du type $Q_8 * D_8 * \ldots * D_8$ si $p = 2$.
- Théorème. Si G est extension du type $0 \to \mathbb{Z}/p\mathbb{Z} \to G \to (\mathbb{Z}/p\mathbb{Z})^n \to 0$, il existe $f \in Xk[X]$ avec $G \simeq G_{\infty,1}(f)$.
- Idée:
  - Les groupes extraspéciaux d'exposant p^2 sont obtenus en modifi ant le polynôme f du théorème précédent par un cocycle de Witt.
  - Si G est sous-groupe d'un groupe extraspécial E, on réalise E avec f_E comme dans le cas précédent et une modifi cation convenable de f_E limite $G_{\infty,1}$ à G.

- Théorème. Si $f(X) = X\Sigma(F)(X) \in k[x]$, $\Sigma(F) = \sum_{0 \leq i \leq s} a_i F^i \in k\{F\}$ un polynôme additif avec $\deg f = 1 + p^s$, alors
  - $\mathrm{Ad}_f(Y) = F^s(\sum_{0 \leq i \leq s}(a_i F^i + F^{-i} a_i)(Y))$
  - $G_{\infty,1}(f)$ est un groupe extraspécial de cardinal p^{2s+1}, d'exposant p si $p > 2$ et du type $Q_8 * D_8 * \ldots * D_8$ si $p = 2$.
- Théorème. Si G est extension du type $0 \to \mathbb{Z}/p\mathbb{Z} \to G \to (\mathbb{Z}/p\mathbb{Z})^n \to 0$, il existe $f \in Xk[X]$ avec $G \simeq G_{\infty,1}(f)$.
- Idée:
  - Les groupes extraspéciaux d'exposant p^2 sont obtenus en modifi ant le polynôme f du théorème précédent par un cocycle de Witt.
  - Si G est sous-groupe d'un groupe extraspécial E, on réalise E avec f_E comme dans le cas précédent et une modifi cation convenable de f_E limite $G_{\infty,1}$ à G.

Grosses actions (I)

- **Théorème.** Soit $f(X) \in Xk[X]$ avec $(\deg f, p) = 1$. Si $\frac{|G_{\infty,1}|}{g} > \frac{p}{p-1}$ ($\frac{2}{3}$ si $p = 2$), alors $f(X) = cX + X\Sigma(F)(X) \in k[X]$.
- Idée: On montre par récurrence que la présence dans f d'un monôme de degré $\notin 1 + p^{\mathbb{N}}$ limite le degré de Ad_f.
- 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 il existe $\infty \in C$, avec
  - $C \to C/G \simeq \mathbb{P}^1_k - \infty$ est 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 $C/G_{\infty,2} - \{\infty\}$
- Passage aux sous-groupes 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).

Grosses actions (I)

- Théorème. Soit $f(X) \in Xk[X]$ avec $(\deg f, p) = 1$. Si $\frac{|G_{\infty,1}|}{g} > \frac{p}{p-1}$ ($\frac{2}{3}$ si $p = 2$), alors $f(X) = cX + X\Sigma(F)(X) \in k[X]$.
- Idée: On montre par récurrence que la présence dans f d'un monôme de degré $\notin 1 + p^{\mathbb{N}}$ limite le degré de Ad_f.
- 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 il existe $\infty \in C$, avec
  - $C \to C/G \simeq \mathbb{P}^1_k - \infty$ est 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 $C/G_{\infty,2} - \{\infty\}$
- Passage aux sous-groupes 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).

Grosses actions (I)

- Théorème. Soit $f(X) \in Xk[X]$ avec $(\deg f, p) = 1$. Si $\frac{|G_{\infty,1}|}{g} > \frac{p}{p-1}$ ($\frac{2}{3}$ si $p = 2$), alors $f(X) = cX + X\Sigma(F)(X) \in k[X]$.
- Idée: On montre par récurrence que la présence dans f d'un monôme de degré $\notin 1 + p^{\mathbb{N}}$ limite le degré de Ad_f.
- 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 il existe $\infty \in C$, avec
  - $C \to C/G \simeq \mathbb{P}^1_k - \infty$ est 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 $C/G_{\infty,2} - \{\infty\}$
- Passage aux sous-groupes 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).

Grosses actions (I)

- Théorème. Soit $f(X) \in Xk[X]$ avec $(\deg f, p) = 1$. Si $\frac{|G_{\infty,1}|}{g} > \frac{p}{p-1}$ ($\frac{2}{3}$ si $p = 2$), alors $f(X) = cX + X\Sigma(F)(X) \in k[X]$.
- Idée: On montre par récurrence que la présence dans f d'un monôme de degré $\notin 1 + p^{\mathbb{N}}$ limite le degré de Ad_f.
- 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 il existe $\infty \in C$, avec
  - $C \to C/G \simeq \mathbb{P}^1_k - \infty$ est 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 $C/G_{\infty,2} - \{\infty\}$
- Passage aux sous-groupes 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).

Grosses actions (I)

- Théorème. Soit $f(X) \in Xk[X]$ avec $(\deg f, p) = 1$. Si $\frac{|G_{\infty,1}|}{g} > \frac{p}{p-1}$ ($\frac{2}{3}$ si $p = 2$), alors $f(X) = cX + X\Sigma(F)(X) \in k[X]$.
- Idée: On montre par récurrence que la présence dans f d'un monôme de degré $\notin 1 + p^{\mathbb{N}}$ limite le degré de Ad_f.
- 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 il existe $\infty \in C$, avec
  - $C \to C/G \simeq \mathbb{P}^1_k - \infty$ est 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 $C/G_{\infty,2} - \{\infty\}$
- Passage aux sous-groupes 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).

Grosses actions (I)

- Théorème. Soit $f(X) \in Xk[X]$ avec $(\deg f, p) = 1$. Si $\frac{|G_{\infty,1}|}{g} > \frac{p}{p-1}$ ($\frac{2}{3}$ si $p = 2$), alors $f(X) = cX + X\Sigma(F)(X) \in k[X]$.
- Idée: On montre par récurrence que la présence dans f d'un monôme de degré $\notin 1 + p^{\mathbb{N}}$ limite le degré de Ad_f.
- 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 il existe $\infty \in C$, avec
  - $C \to C/G \simeq \mathbb{P}^1_k - \infty$ est 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 $C/G_{\infty,2} - \{\infty\}$
- Passage aux sous-groupes 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).

Grosses actions (I)

- Théorème. Soit $f(X) \in Xk[X]$ avec $(\deg f, p) = 1$. Si $\frac{|G_{\infty,1}|}{g} > \frac{p}{p-1}$ ($\frac{2}{3}$ si $p = 2$), alors $f(X) = cX + X\Sigma(F)(X) \in k[X]$.
- Idée: On montre par récurrence que la présence dans f d'un monôme de degré $\notin 1 + p^{\mathbb{N}}$ limite le degré de Ad_f.
- 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 il existe $\infty \in C$, avec
  - $C \to C/G \simeq \mathbb{P}^1_k - \infty$ est 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 $C/G_{\infty,2} - \{\infty\}$
- Passage aux sous-groupes 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).

Condition (N) et G_2

On suppose que (C, G) satisfait (N), on note G_i les groupes de ramifi cation.

- 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 existe $\Sigma(F) \in k\{F\}$, $f_1 = cX + X\Sigma(F)(X) \in k[X]$ avec $C/H \simeq C_{f_1}$.
- 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: $(v \in V) \times (f_1(X), f_2(X), ..., f_t(X)) \mod \wp(k[X])^t \to$ $\to (f_1(X+v), f_2(X+v), ..., f_t(X+v)) \mod \wp(k[X])^t$

Condition (N) et G_2

On suppose que (C, G) satisfait (N), on note G_i les groupes de ramifi cation.

- 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 existe $\Sigma(F) \in k\{F\}$, $f_1 = cX + X\Sigma(F)(X) \in k[X]$ avec $C/H \simeq C_{f_1}$.
- 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: $(v \in V) \times (f_1(X), f_2(X), ..., f_t(X)) \mod \wp(k[X])^t \to$ $\to (f_1(X+v), f_2(X+v), ..., f_t(X+v)) \mod \wp(k[X])^t$

Condition (N) et G_2

On suppose que (C, G) satisfait (N), on note G_i les groupes de ramifi cation.

- 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 existe $\Sigma(F) \in k\{F\}$, $f_1 = cX + X\Sigma(F)(X) \in k[X]$ avec $C/H \simeq C_{f_1}$.
- 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: $(v \in V) \times (f_1(X), f_2(X), ..., f_t(X)) \mod \wp(k[X])^t \to$ $\to (f_1(X+v), f_2(X+v), ..., f_t(X+v)) \mod \wp(k[X])^t$

Condition (N) et G_2

On suppose que (C, G) satisfait (N), on note G_i les groupes de ramifi cation.

- 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 existe $\Sigma(F) \in k\{F\}$, $f_1 = cX + X\Sigma(F)(X) \in k[X]$ avec $C/H \simeq C_{f_1}$.
- 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: $(v \in V) \times (f_1(X), f_2(X), ..., f_t(X)) \mod \wp(k[X])^t \to$ $\to (f_1(X+v), f_2(X+v), ..., f_t(X+v)) \mod \wp(k[X])^t$

Condition (N) et G_2

On suppose que (C, G) satisfait (N), on note G_i les groupes de ramifi cation.

- 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 existe $\Sigma(F) \in k\{F\}$, $f_1 = cX + X\Sigma(F)(X) \in k[X]$ avec $C/H \simeq C_{f_1}$.
- 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: $(v \in V) \times (f_1(X), f_2(X), ..., f_t(X)) \mod \wp(k[X])^t \to$ $\to (f_1(X+v), f_2(X+v), ..., f_t(X+v)) \mod \wp(k[X])^t$

Condition (N) et G_2

On suppose que (C, G) satisfait (N), on note G_i les groupes de ramifi cation.

- 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 existe $\Sigma(F) \in k\{F\}$, $f_1 = cX + X\Sigma(F)(X) \in k[X]$ avec $C/H \simeq C_{f_1}$.
- Si $G_2 \simeq (\mathbb{Z}/p\mathbb{Z})^t$, alors $k(C) = k(X, w_1, \dots, w_t)$ et $\wp(w_1, \dots, w_t) = (f_1(X), f_2(X), \dots, f_t(X)) \in (k[X])^t$
- $f_1(X), .., f_t(X)$ 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: $(v \in V) \times (f_1(X), f_2(X), \dots, f_t(X)) \mod \wp(k[X])^t \to$ $\to (f_1(X+v), f_2(X+v), \dots, f_t(X+v)) \mod \wp(k[X])^t$

Condition (N) et G_2

On suppose que (C, G) satisfait (N), on note G_i les groupes de ramifi cation.

- 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 existe $\Sigma(F) \in k\{F\}$, $f_1 = cX + X\Sigma(F)(X) \in k[X]$ avec $C/H \simeq C_{f_1}$.
- 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 $G_2 \subset Z(G)$. 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 $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.
- 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
- $f_2(X+Y) - f_2(X) - f_2(Y) = 2(Y^p - Y)X^{1+p} + (Y - Y^{p^2})X^{2p} + (Y^{2p^2} - Y^2 + 2Y^{1+p} - 2Y^{p+p^2})X^p \mod (F - \mathrm{Id})k[X, Y]$
- 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 $g = \frac{p-1}{2}(p + p * 2p)$.
- $\frac{|G|}{g} = \frac{2p}{p-1}\frac{p^2}{1+2p}$.
- $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2}\frac{p}{(1+2p)^2}$.

- $\mathrm{Im}\rho$ est un sous-groupe unipotent de $\mathrm{Gl}_t(\mathbb{F}_p)$ qui est réduit à l'identité ssi $G_2 \subset Z(G)$. Dans ce cas $f_i(X) = c_iX + X\Sigma_i(F)(X)$ où $\Sigma_i(F) \in k\{F\}$ et $v \in V$ est un zéro commun aux polynômes palindromiques $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.
- 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
- $f_2(X+Y) - f_2(X) - f_2(Y) = 2(Y^p - Y)X^{1+p} + (Y - Y^{p^2})X^{2p} + (Y^{2p^2} - Y^2 + 2Y^{1+p} - 2Y^{p+p^2})X^p$ mod $(F - \mathrm{Id})k[X, Y]$
- 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 $g = \frac{p-1}{2}(p + p * 2p)$.
- $\frac{|G|}{g} = \frac{2p}{p-1}\frac{p^2}{1+2p}$.
- $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2}\frac{p}{(1+2p)^2}$.

- $\mathrm{Im}\rho$ est un sous-groupe unipotent de $\mathrm{Gl}_t(\mathbb{F}_p)$ qui est réduit à l'identité ssi $G_2 \subset Z(G)$. Dans ce cas $f_i(X) = c_iX + X\Sigma_i(F)(X)$ où $\Sigma_i(F) \in k\{F\}$ et $v \in V$ est un zéro commun aux polynômes palindromiques $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.
- 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
- $f_2(X+Y) - f_2(X) - f_2(Y) = 2(Y^p - Y)X^{1+p} + (Y - Y^{p^2})X^{2p} + (Y^{2p^2} - Y^2 + 2Y^{1+p} - 2Y^{p+p^2})X^p$ mod $(F - \mathrm{Id})k[X, Y]$
- 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 $g = \frac{p-1}{2}(p + p * 2p)$.
- $\frac{|G|}{g} = \frac{2p}{p-1}\frac{p^2}{1+2p}$.
- $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2}\frac{p}{(1+2p)^2}$.

- $\mathrm{Im}\rho$ est un sous-groupe unipotent de $\mathrm{Gl}_t(\mathbb{F}_p)$ qui est réduit à l'identité ssi $G_2 \subset Z(G)$. 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 $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.
- 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
- $f_2(X+Y) - f_2(X) - f_2(Y) = 2(Y^p - Y)X^{1+p} + (Y - Y^{p^2})X^{2p} + (Y^{2p^2} - Y^2 + 2Y^{1+p} - 2Y^{p+p^2})X^p$ mod $(F - \mathrm{Id})k[X, Y]$
- 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 $g = \frac{p-1}{2}(p + p * 2p)$.
- $\frac{|G|}{g} = \frac{2p}{p-1} \frac{p^2}{1+2p}$.
- $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2} \frac{p}{(1+2p)^2}$.

- $\mathrm{Im}\rho$ est un sous-groupe unipotent de $\mathrm{Gl}_t(\mathbb{F}_p)$ qui est réduit à l'identité ssi $G_2 \subset Z(G)$. Dans ce cas $f_i(X) = c_iX + X\Sigma_i(F)(X)$ où $\Sigma_i(F) \in k\{F\}$ et $v \in V$ est un zéro commun aux polynômes palindromiques $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.
- 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
- $f_2(X+Y) - f_2(X) - f_2(Y) = 2(Y^p - Y)X^{1+p} + (Y - Y^{p^2})X^{2p} + (Y^{2p^2} - Y^2 + 2Y^{1+p} - 2Y^{p+p^2})X^p$ mod $(F - \mathrm{Id})k[X, Y]$
- 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 $g = \frac{p-1}{2}(p + p * 2p)$.
- $\frac{|G|}{g} = \frac{2p}{p-1}\frac{p^2}{1+2p}$.
- $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2}\frac{p}{(1+2p)^2}$.

- $\mathrm{Im}\rho$ est un sous-groupe unipotent de $\mathrm{Gl}_t(\mathbb{F}_p)$ qui est réduit à l'identité ssi $G_2 \subset Z(G)$. 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 $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.
- 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
- $f_2(X+Y) - f_2(X) - f_2(Y) = 2(Y^p - Y)X^{1+p} + (Y - Y^{p^2})X^{2p} + (Y^{2p^2} - Y^2 + 2Y^{1+p} - 2Y^{p+p^2})X^p$ mod $(F - \mathrm{Id})k[X, Y]$
- 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 $g = \frac{p-1}{2}(p + p * 2p)$.
- $\frac{|G|}{g} = \frac{2p}{p-1}\frac{p^2}{1+2p}$.
- $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2}\frac{p}{(1+2p)^2}$.

- $\mathrm{Im}\rho$ est un sous-groupe unipotent de $\mathrm{Gl}_t(\mathbb{F}_p)$ qui est réduit à l'identité ssi $G_2 \subset Z(G)$. 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 $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.
- 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
- $f_2(X+Y) - f_2(X) - f_2(Y) = 2(Y^p - Y)X^{1+p} + (Y - Y^{p^2})X^{2p} + (Y^{2p^2} - Y^2 + 2Y^{1+p} - 2Y^{p+p^2})X^p \mod (F - \mathrm{Id})k[X, Y]$
- 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 $g = \frac{p-1}{2}(p + p * 2p)$.
- $\frac{|G|}{g} = \frac{2p}{p-1}\frac{p^2}{1+2p}$.
- $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2}\frac{p}{(1+2p)^2}$.

- $\mathrm{Im}\rho$ est un sous-groupe unipotent de $\mathrm{Gl}_t(\mathbb{F}_p)$ qui est réduit à l'identité ssi $G_2 \subset Z(G)$. 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 $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.
- 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
- $f_2(X+Y) - f_2(X) - f_2(Y) = 2(Y^p - Y)X^{1+p} + (Y - Y^{p^2})X^{2p} + (Y^{2p^2} - Y^2 + 2Y^{1+p} - 2Y^{p+p^2})X^p \bmod (F - \mathrm{Id})k[X, Y]$
- 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 $g = \frac{p-1}{2}(p + p * 2p)$.
- $\frac{|G|}{g} = \frac{2p}{p-1}\frac{p^2}{1+2p}$.
- $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2}\frac{p}{(1+2p)^2}$.

- $\mathrm{Im}\rho$ est un sous-groupe unipotent de $\mathrm{Gl}_t(\mathbb{F}_p)$ qui est réduit à l'identité ssi $G_2 \subset Z(G)$. 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 $\mathrm{Ad}_{f_i} \in k\{F, F^{-1}\}$.
- 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
- $f_2(X+Y) - f_2(X) - f_2(Y) = 2(Y^p - Y)X^{1+p} + (Y - Y^{p^2})X^{2p} + (Y^{2p^2} - Y^2 + 2Y^{1+p} - 2Y^{p+p^2})X^p$ mod $(F - \mathrm{Id})k[X, Y]$
- 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 $g = \frac{p-1}{2}(p + p * 2p)$.
- $\frac{|G|}{g} = \frac{2p}{p-1} \frac{p^2}{1+2p}$.
- $\frac{|G|}{g^2} = \frac{4p}{(p-1)^2} \frac{p}{(1+2p)^2}$.

- Supposons que G_2 n'est pas abélien, alors $G_2 = G'$. Ainsi, si $|G_2| = p^3$, alors G_2 est abélien.
- 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 extraspecial 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.

- Supposons que G_2 n'est pas abélien, alors $G_2 = G'$. Ainsi, si $|G_2| = p^3$, alors G_2 est abélien.
- 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 extraspecial 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.

- Supposons que G_2 n'est pas abélien, alors $G_2 = G'$. Ainsi, si $|G_2| = p^3$, alors G_2 est abélien.
- 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 extraspecial 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.

- Supposons que G_2 n'est pas abélien, alors $G_2 = G'$. Ainsi, si $|G_2| = p^3$, alors G_2 est abélien.
- 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 extraspecial 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.

- Supposons que G_2 n'est pas abélien, alors $G_2 = G'$. Ainsi, si $|G_2| = p^3$, alors G_2 est abélien.
- 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 extraspecial 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.

- Supposons que G_2 n'est pas abélien, alors $G_2 = G'$. Ainsi, si $|G_2| = p^3$, alors G_2 est abélien.
- 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 extraspecial 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.

Surfaces de Riemann

- En caractéristique 0, un analogue des courbes maximales 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 courbes maximales 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 courbes maximales est donné par les actions d'un groupe fini 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 ramifié 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 courbes maximales est donné par les actions d'un groupe fini 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 ramifié 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 ∞ ; 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 $g_{C_m} = 1 + n_m(-1 + m/2) - (1/2)\sum_{0 \le j \le m-1} n_j \le n_m(-1 + m/2)$

- ([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 ∞ ; 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 ∞ ; 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 $g_{C_m} = 1 + n_m(-1+m/2) - (1/2)\sum_{0\le j\le m-1} n_j \le n_m(-1+m/2)$

- $\frac{|G_1(m)|}{g_{C_m}} \geq \frac{n_m q}{n_m(-1+m/2)} = \frac{q}{-1+m/2}$. 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 $n = 1$.
  - Idée: On peut supposer que $n = 2$ en considérant $(C/H, G/H)$ pour $H = G_2^{p^{n-2}}$. Alors $C \to C/G_2$ est défi ni par $\wp(w_0, w_1) = (f_0, f_1)$ avec $f_0 = X\Sigma(F)(X)$, $\deg f_0 = p^s$.
  - Soit $y \in V := Z(\mathrm{Ad}_{f_0}(Y))$ et $P \in k[X]$ avec $f_0(X+y) = f_0(X) + \wp(P)$ alors $f_1(X+y) - f_1(X) = \ell(y)f_0(X) + \frac{1}{p}(f_0(X)^p + P(X)^p - P(X)^{p^2} - (f_0(X) + P(X))^p - f_0(X+y)^p + (f_0(X+y) + P(X)^p)^p)$
  - $= \ell(y)f_0(X) + \sum_{1 \leq i \leq p-1} \frac{(-1)^{i-1}}{i} y^i X^{p-i+p^{s+1}}$ mod $X^{p^{s+1}}$ où $\ell : V \to \mathbb{F}_p$ est une forme linéaire.
- 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 $n = 1$.
  - Idée: On peut supposer que $n = 2$ en considérant $(C/H, G/H)$ pour $H = G_2^{p^{n-2}}$. Alors $C \to C/G_2$ est défini par $\wp(w_0, w_1) = (f_0, f_1)$ avec $f_0 = X\Sigma(F)(X)$, $\deg f_0 = p^s$.
  - Soit $y \in V := Z(\mathrm{Ad}_{f_0}(Y))$ et $P \in k[X]$ avec $f_0(X + y) = f_0(X) + \wp(P)$ alors $f_1(X + y) - f_1(X) = \ell(y)f_0(X) + \frac{1}{p}(f_0(X)^p + P(X)^p - P(X)^{p^2} - (f_0(X) + P(X))^p - f_0(X + y)^p + (f_0(X + y) + P(X)^p)^p)$
  - $= \ell(y)f_0(X) + \sum_{1 \leq i \leq p-1} \frac{(-1)^{i-1}}{i} y^i X^{p-i+p^{s+1}}$ mod $X^{p^{s+1}}$ où $\ell : V \to \mathbb{F}_p$ est une forme linéaire.
- 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 $n = 1$.
  - Idée: On peut supposer que $n = 2$ en considérant $(C/H, G/H)$ pour $H = G_2^{p^{n-2}}$. Alors $C \to C/G_2$ est défini par $\wp(w_0, w_1) = (f_0, f_1)$ avec $f_0 = X\Sigma(F)(X)$, $\deg f_0 = p^s$.
  - Soit $y \in V := Z(\mathrm{Ad}_{f_0}(Y))$ et $P \in k[X]$ avec $f_0(X+y) = f_0(X) + \wp(P)$ alors $f_1(X+y) - f_1(X) = \ell(y)f_0(X) + \frac{1}{p}(f_0(X)^p + P(X)^p - P(X)^{p^2} - (f_0(X) + P(X))^p - f_0(X+y)^p + (f_0(X+y) + P(X)^p)^p)$
  - $= \ell(y)f_0(X) + \sum_{1\le i\le p-1} \frac{(-1)^{i-1}}{i} y^i X^{p-i+p^{s+1}} \mod X^{p^{s+1}}$ où $\ell : V \to \mathbb{F}_p$ est une forme linéaire.
- 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 $n = 1$.
  - Idée: On peut supposer que $n = 2$ en considérant $(C/H, G/H)$ pour $H = G_2^{p^{n-2}}$. Alors $C \to C/G_2$ est défini par $\wp(w_0, w_1) = (f_0, f_1)$ avec $f_0 = X\Sigma(F)(X)$, $\deg f_0 = p^s$.
  - Soit $y \in V := Z(\mathrm{Ad}_{f_0}(Y))$ et $P \in k[X]$ avec $f_0(X+y) = f_0(X) + \wp(P)$ alors $f_1(X+y) - f_1(X) = \ell(y)f_0(X) + \frac{1}{p}(f_0(X)^p + P(X)^p - P(X)^{p^2} - (f_0(X) + P(X))^p - f_0(X+y)^p + (f_0(X+y) + P(X)^p)^p)$
  - $= \ell(y)f_0(X) + \sum_{1 \le i \le p-1} \frac{(-1)^{i-1}}{i} y^i X^{p-i+p^{s+1}}$ mod $X^{p^{s+1}}$ où $\ell : V \to \mathbb{F}_p$ est une forme linéaire.
- 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 $n = 1$.
  - Idée: On peut supposer que $n = 2$ en considérant $(C/H, G/H)$ pour $H = G_2^{p^{n-2}}$. Alors $C \to C/G_2$ est défini par $\wp(w_0, w_1) = (f_0, f_1)$ avec $f_0 = X\Sigma(F)(X)$, $\deg f_0 = p^s$.
  - Soit $y \in V := Z(\mathrm{Ad}_{f_0}(Y))$ et $P \in k[X]$ avec $f_0(X+y) = f_0(X) + \wp(P)$ alors $f_1(X+y) - f_1(X) = \ell(y)f_0(X) + \frac{1}{p}(f_0(X)^p + P(X)^p - P(X)^{p^2} - (f_0(X) + P(X))^p - f_0(X+y)^p + (f_0(X+y) + P(X)^p)^p)$
  - $= \ell(y)f_0(X) + \sum_{1\leq i\leq p-1} \frac{(-1)^{i-1}}{i} y^i X^{p-i+p^{s+1}}$ mod $X^{p^{s+1}}$ où $\ell : V \to \mathbb{F}_p$ est une forme linéaire.
- 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

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

- 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
  - $|G_{i_0+1}| \leq \frac{1}{M} \frac{|G/G_{i_0+1}|}{g_{C/G_{i_0+1}}^2} \leq \frac{1}{M} \frac{4|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2}$.
- 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.
- Il suffi t de remarquer que 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 $|G_2|$.

Courbes maximales I

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

- 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
  - $|G_{i_0+1}| \leq \frac{1}{M}\frac{|G/G_{i_0+1}|}{g^2_{C/G_{i_0+1}}} \leq \frac{1}{M}\frac{4|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2}$.
- 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.
- Il suffi t de remarquer que 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 $|G_2|$.

Courbes maximales I

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

- 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
  - $|G_{i_0+1}| \leq \frac{1}{M}\frac{|G/G_{i_0+1}|}{g^2_{C/G_{i_0+1}}} \leq \frac{1}{M}\frac{4|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2}$.
- 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.
- Il suffit de remarquer que 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 $|G_2|$.

Courbes maximales I

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

- 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
  - $|G_{i_0+1}| \leq \frac{1}{M}\frac{|G/G_{i_0+1}|}{g^2_{C/G_{i_0+1}}} \leq \frac{1}{M}\frac{4|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2}$.
- 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.
- Il suffi t de remarquer que 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 $|G_2|$.

Courbes maximales I

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

- 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
  - $|G_{i_0+1}| \leq \frac{1}{M}\frac{|G/G_{i_0+1}|}{g^2_{C/G_{i_0+1}}} \leq \frac{1}{M}\frac{4|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2}$.
- 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.
- Il suffi t de remarquer que 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 $|G_2|$.

Courbes maximales I

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

- Soit i_0 avec $G_2 = G_3 = ... = G_{i_0} \supsetneqq G_{i_0+1}$. 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
  - $|G_{i_0+1}| \leq \frac{1}{M} \frac{|G/G_{i_0+1}|}{g^2_{C/G_{i_0+1}}} \leq \frac{1}{M} \frac{4|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2}$.
- 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.
- Il suffi t de remarquer que 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 $|G_2|$.

Courbes maximales I

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

- 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
  - $|G_{i_0+1}| \leq \frac{1}{M}\frac{|G/G_{i_0+1}|}{g^2_{C/G_{i_0+1}}} \leq \frac{1}{M}\frac{4|G_2/G_{i_0+1}|}{(|G_2/G_{i_0+1}|-1)^2}$.
- 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.
- Il suffi t de remarquer que 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 $|G_2|$.

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 $G_2 = \mathbb{Z}/p\mathbb{Z}$).
- 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.

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 $G_2 = \mathbb{Z}/p\mathbb{Z}$).
- 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.

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 $G_2 = \mathbb{Z}/p\mathbb{Z}$).
- 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.

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 $G_2 = \mathbb{Z}/p\mathbb{Z}$).
- 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.

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 $G_2 = \mathbb{Z}/p\mathbb{Z}$).
- 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.

- Idée: On a vu que $|G_2|$ et donc t sont majorés. Soit $m_i := \deg f_i$. On peut supposer que $m_1 \leq m_2 \leq ... \leq m_t$.
- Si l'image de ρ est triviale.
  - Alors $m_i - 1 = p^{\nu_i}$ et $\nu_1 \leq ... \leq \nu_t$
  - $|G| = p^t|V| \leq p^{t+2\nu_1}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i})$
  - $M \leq \frac{p^t|V|}{g_C^2} \leq \frac{4p^t}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$
  - $\nu_i - \nu_1$ est majoré.
  - $\frac{p^{2\nu_1}}{|V|} \leq \frac{4p^t}{M(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$ et donc $\{\frac{p^{2\nu_1}}{|V|}\}$ est fini.
  - $\{\frac{|G|}{g_C^2} = \frac{4p^t|V|p^{-2\nu_1}}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}\}$ est fini.

- Idée: On a vu que $|G_2|$ et donc t sont majorés. Soit $m_i := \deg f_i$. On peut supposer que $m_1 \leq m_2 \leq ... \leq m_t$.
- Si l'image de ρ est triviale.
  - Alors $m_i - 1 = p^{\nu_i}$ et $\nu_1 \leq ... \leq \nu_t$
  - $|G| = p^t|V| \leq p^{t+2\nu_1}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i})$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$
  - $\nu_i - \nu_1$ est majoré.
  - $\frac{p^{2\nu_1}}{|V|} \leq \frac{4p^t}{M(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$ et donc $\{\frac{p^{2\nu_1}}{|V|}\}$ est fini.
  - $\{\frac{|G|}{g_C^2} = \frac{4p^t|V|p^{-2\nu_1}}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}\}$ est fini.

- Idée: On a vu que $|G_2|$ et donc t sont majorés. Soit $m_i := \deg f_i$. On peut supposer que $m_1 \le m_2 \le \ldots \le m_t$.
- Si l'image de ρ est triviale.
  - Alors $m_i - 1 = p^{\nu_i}$ et $\nu_1 \le \ldots \le \nu_t$
  - $|G| = p^t|V| \le p^{t+2\nu_1}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1 \le i \le t} p^{i-1}p^{\nu_i})$
  - $M \le \frac{p^t|V|}{g^2} \le \frac{4p^t}{(p-1)^2(\sum_{1 \le i \le t} p^{i-1}p^{\nu_i-\nu_1})^2}$
  - $\nu_i - \nu_1$ est majoré.
  - $\frac{p^{2\nu_1}}{|V|} \le \frac{4p^t}{M(p-1)^2(\sum_{1 \le i \le t} p^{i-1}p^{\nu_i-\nu_1})^2}$ et donc $\{\frac{p^{2\nu_1}}{|V|}\}$ est fini.
  - $\{\frac{|G|}{g_C^2} = \frac{4p^t|V|p^{-2\nu_1}}{(p-1)^2(\sum_{1 \le i \le t} p^{i-1}p^{\nu_i-\nu_1})^2}\}$ est fini.

- Idée: On a vu que $|G_2|$ et donc t sont majorés. Soit $m_i := \deg f_i$. On peut supposer que $m_1 \leq m_2 \leq \ldots \leq m_t$.
- Si l'image de ρ est triviale.
  - Alors $m_i - 1 = p^{\nu_i}$ et $\nu_1 \leq \ldots \leq \nu_t$
  - $|G| = p^t|V| \leq p^{t+2\nu_1}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i})$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$
  - $\nu_i - \nu_1$ est majoré.
  - $\frac{p^{2\nu_1}}{|V|} \leq \frac{4p^t}{M(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$ et donc $\{\frac{p^{2\nu_1}}{|V|}\}$ est fini.
  - $\{\frac{|G|}{g_C^2} = \frac{4p^t|V|p^{-2\nu_1}}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}\}$ est fini.

- Idée: On a vu que $|G_2|$ et donc t sont majorés. Soit $m_i := \deg f_i$. On peut supposer que $m_1 \leq m_2 \leq \ldots \leq m_t$.
- Si l'image de ρ est triviale.
  - Alors $m_i - 1 = p^{\nu_i}$ et $\nu_1 \leq \ldots \leq \nu_t$
  - $|G| = p^t|V| \leq p^{t+2\nu_1}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1 \leq i \leq t} p^{i-1}p^{\nu_i})$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t}{(p-1)^2(\sum_{1\leq i \leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$
  - $\nu_i - \nu_1$ est majoré.
  - $\frac{p^{2\nu_1}}{|V|} \leq \frac{4p^t}{M(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$ et donc $\{\frac{p^{2\nu_1}}{|V|}\}$ est fini.
  - $\{\frac{|G|}{g_C^2} = \frac{4p^t|V|p^{-2\nu_1}}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}\}$ est fini.

- Idée: On a vu que $|G_2|$ et donc t sont majorés. Soit $m_i := \deg f_i$. On peut supposer que $m_1 \leq m_2 \leq \ldots \leq m_t$.
- Si l'image de ρ est triviale.
  - Alors $m_i - 1 = p^{\nu_i}$ et $\nu_1 \leq \ldots \leq \nu_t$
  - $|G| = p^t |V| \leq p^{t+2\nu_1}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i})$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$
  - $\nu_i - \nu_1$ est majoré.
  - $\frac{p^{2\nu_1}}{|V|} \leq \frac{4p^t}{M(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$ et donc $\{\frac{p^{2\nu_1}}{|V|}\}$ est fini.
  - $\{\frac{|G|}{g_C^2} = \frac{4p^t|V|p^{-2\nu_1}}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}\}$ est fini.

- Idée: On a vu que $|G_2|$ et donc t sont majorés. Soit $m_i := \deg f_i$. On peut supposer que $m_1 \leq m_2 \leq ... \leq m_t$.
- Si l'image de ρ est triviale.
  - Alors $m_i - 1 = p^{\nu_i}$ et $\nu_1 \leq ... \leq \nu_t$
  - $|G| = p^t|V| \leq p^{t+2\nu_1}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i})$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$
  - $\nu_i - \nu_1$ est majoré.
  - $\frac{p^{2\nu_1}}{|V|} \leq \frac{4p^t}{M(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$ et donc $\{\frac{p^{2\nu_1}}{|V|}\}$ est fini.
  - $\{\frac{|G|}{g_C^2} = \frac{4p^t|V|p^{-2\nu_1}}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}\}$ est fini.

- Idée: On a vu que $|G_2|$ et donc t sont majorés. Soit $m_i := \deg f_i$. On peut supposer que $m_1 \leq m_2 \leq ... \leq m_t$.
- Si l'image de ρ est triviale.
  - Alors $m_i - 1 = p^{\nu_i}$ et $\nu_1 \leq ... \leq \nu_t$
  - $|G| = p^t|V| \leq p^{t+2\nu_1}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i})$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$
  - $\nu_i - \nu_1$ est majoré.
  - $\frac{p^{2\nu_1}}{|V|} \leq \frac{4p^t}{M(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$ et donc $\{\frac{p^{2\nu_1}}{|V|}\}$ est fi ni.
  - $\{\frac{|G|}{g_C^2} = \frac{4p^t|V|p^{-2\nu_1}}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}\}$ est fi ni.

- Idée: On a vu que $|G_2|$ et donc t sont majorés. Soit $m_i := \deg f_i$. On peut supposer que $m_1 \leq m_2 \leq ... \leq m_t$.
- Si l'image de ρ est triviale.
  - Alors $m_i - 1 = p^{\nu_i}$ et $\nu_1 \leq ... \leq \nu_t$
  - $|G| = p^t |V| \leq p^{t+2\nu_1}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i})$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$
  - $\nu_i - \nu_1$ est majoré.
  - $\frac{p^{2\nu_1}}{|V|} \leq \frac{4p^t}{M(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}$ et donc $\{\frac{p^{2\nu_1}}{|V|}\}$ est fi ni.
  - $\{\frac{|G|}{g_C^2} = \frac{4p^t|V|p^{-2\nu_1}}{(p-1)^2(\sum_{1\leq i\leq t} p^{i-1}p^{\nu_i-\nu_1})^2}\}$ est fi ni.

- Si l'image de ρ n'est pas triviale.
  - Il existe un plus petit i_0 tel que $f_{i_0+1}(X) \neq X\Sigma(F)(X)$.
  - Pour $v \in V$ $f_{i_0+1}(X+v) = f_{i_0+1}(X) + \sum_{1\leq i\leq i_0} \ell_i(v) f_i(X) \mod \wp(k[X])$
  - ℓ_i est une forme linéaire non nulle sur le $\mathbb{F}_p$-espace vectoriel V.
  - Soit $W := \cap_{1\leq i\leq i_0} \ker \ell_i$; $|W| \geq \frac{|V|}{p^{i_0}}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}(m_i-1)) \geq \frac{(p-1)}{2}(p^{i_0}(m_{i_0+1}-1))$.
  - $\frac{2p|W|}{(p-1)(m_{i_0+1}-1)} \leq \frac{2p}{p-1}$
  - $g_C \geq \frac{p-1}{2}p^{i_0}(m_{i_0+1}-1) \geq \frac{p-1}{2}|V|$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t|V|}{(p-1)^2|V|^2}$
  - $|V|$ est majoré et $g_C^2 \leq \frac{p^t|V|}{M}$ est majoré.
  - $\{\frac{|G|}{g_C^2} = \frac{|G_2||V|}{g_C^2}\}$ est fi ni. ///

- Si l'image de ρ n'est pas triviale.
  - Il existe un plus petit i_0 tel que $f_{i_0+1}(X) \neq X\Sigma(F)(X)$.
  - Pour $v \in V$ $f_{i_0+1}(X+v) = f_{i_0+1}(X) + \sum_{1\leq i\leq i_0} \ell_i(v) f_i(X)$ mod $\wp(k[X])$
  - ℓ_i est une forme linéaire non nulle sur le $\mathbb{F}_p$-espace vectoriel V.
  - Soit $W := \cap_{1\leq i\leq i_0} \ker \ell_i$; $|W| \geq \frac{|V|}{p^{i_0}}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}(m_i-1)) \geq \frac{(p-1)}{2}(p^{i_0}(m_{i_0+1}-1))$.
  - $\frac{2p|W|}{(p-1)(m_{i_0+1}-1)} \leq \frac{2p}{p-1}$
  - $g_C \geq \frac{p-1}{2}p^{i_0}(m_{i_0+1}-1) \geq \frac{p-1}{2}|V|$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t|V|}{(p-1)^2|V|^2}$
  - $|V|$ est majoré et $g_C^2 \leq \frac{p^t|V|}{M}$ est majoré.
  - $\{\frac{|G|}{g_C^2} = \frac{|G_2||V|}{g_C^2}\}$ est fi ni. ///

- Si l'image de ρ n'est pas triviale.
  - Il existe un plus petit i_0 tel que $f_{i_0+1}(X) \neq X\Sigma(F)(X)$.
  - Pour $v \in V$ $f_{i_0+1}(X+v) = f_{i_0+1}(X) + \sum_{1\leq i\leq i_0} \ell_i(v) f_i(X)$ mod $\wp(k[X])$
  - ℓ_i est une forme linéaire non nulle sur le $\mathbb{F}_p$-espace vectoriel V.
  - Soit $W := \cap_{1\leq i\leq i_0} \ker \ell_i$; $|W| \geq \frac{|V|}{p^{i_0}}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}(m_i - 1)) \geq \frac{(p-1)}{2}(p^{i_0}(m_{i_0+1} - 1))$.
  - $\frac{2p|W|}{(p-1)(m_{i_0+1}-1)} \leq \frac{2p}{p-1}$
  - $g_C \geq \frac{p-1}{2} p^{i_0}(m_{i_0+1} - 1) \geq \frac{p-1}{2}|V|$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t|V|}{(p-1)^2|V|^2}$
  - $|V|$ est majoré et $g_C^2 \leq \frac{p^t|V|}{M}$ est majoré.
  - $\{\frac{|G|}{g_C^2} = \frac{|G_2||V|}{g_C^2}\}$ est fi ni. ///

- Si l'image de ρ n'est pas triviale.
  - Il existe un plus petit i_0 tel que $f_{i_0+1}(X) \neq X\Sigma(F)(X)$.
  - Pour $v \in V$ $f_{i_0+1}(X+v) = f_{i_0+1}(X) + \sum_{1\leq i\leq i_0} \ell_i(v) f_i(X) \mod \wp(k[X])$
  - ℓ_i est une forme linéaire non nulle sur le $\mathbb{F}_p$-espace vectoriel V.
  - Soit $W := \cap_{1\leq i\leq i_0} \ker \ell_i$; $|W| \geq \frac{|V|}{p^{i_0}}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}(m_i - 1)) \geq \frac{(p-1)}{2}(p^{i_0}(m_{i_0+1} - 1))$.
  - $\frac{2p|W|}{(p-1)(m_{i_0+1}-1)} \leq \frac{2p}{p-1}$
  - $g_C \geq \frac{p-1}{2} p^{i_0}(m_{i_0+1} - 1) \geq \frac{p-1}{2}|V|$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t|V|}{(p-1)^2|V|^2}$
  - $|V|$ est majoré et $g_C^2 \leq \frac{p^t|V|}{M}$ est majoré.
  - $\{\frac{|G|}{g_C^2} = \frac{|G_2||V|}{g_C^2}\}$ est fi ni. ///

- Si l'image de ρ n'est pas triviale.
  - Il existe un plus petit i_0 tel que $f_{i_0+1}(X) \neq X\Sigma(F)(X)$.
  - Pour $v \in V$ $f_{i_0+1}(X+v) = f_{i_0+1}(X) + \sum_{1 \leq i \leq i_0} \ell_i(v) f_i(X) \mod \wp(k[X])$
  - ℓ_i est une forme linéaire non nulle sur le $\mathbb{F}_p$-espace vectoriel V.
  - Soit $W := \cap_{1 \leq i \leq i_0} \ker \ell_i$; $|W| \geq \frac{|V|}{p^{i_0}}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1 \leq i \leq t} p^{i-1}(m_i - 1)) \geq \frac{(p-1)}{2}(p^{i_0}(m_{i_0+1} - 1))$.
  - $\frac{2p|W|}{(p-1)(m_{i_0+1}-1)} \leq \frac{2p}{p-1}$
  - $g_C \geq \frac{p-1}{2} p^{i_0}(m_{i_0+1} - 1) \geq \frac{p-1}{2}|V|$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t|V|}{(p-1)^2|V|^2}$
  - $|V|$ est majoré et $g_C^2 \leq \frac{p^t|V|}{M}$ est majoré.
  - $\{\frac{|G|}{g_C^2} = \frac{|G_2||V|}{g_C^2}\}$ est fi ni. ///

- Si l'image de ρ n'est pas triviale.
  - Il existe un plus petit i_0 tel que $f_{i_0+1}(X) \neq X\Sigma(F)(X)$.
  - Pour $v \in V$ $f_{i_0+1}(X+v) = f_{i_0+1}(X) + \sum_{1\leq i\leq i_0} \ell_i(v) f_i(X) \mod \wp(k[X])$
  - ℓ_i est une forme linéaire non nulle sur le $\mathbb{F}_p$-espace vectoriel V.
  - Soit $W := \cap_{1\leq i\leq i_0} \ker \ell_i$; $|W| \geq \frac{|V|}{p^{i_0}}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}(m_i - 1)) \geq \frac{(p-1)}{2}(p^{i_0}(m_{i_0+1} - 1))$.
  - $\frac{2p|W|}{(p-1)(m_{i_0+1}-1)} \leq \frac{2p}{p-1}$
  - $g_C \geq \frac{p-1}{2} p^{i_0}(m_{i_0+1} - 1) \geq \frac{p-1}{2}|V|$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t|V|}{(p-1)^2|V|^2}$
  - $|V|$ est majoré et $g_C^2 \leq \frac{p^t|V|}{M}$ est majoré.
  - $\{\frac{|G|}{g_C^2} = \frac{|G_2||V|}{g_C^2}\}$ est fi ni. ///

- Si l'image de ρ n'est pas triviale.
  - Il existe un plus petit i_0 tel que $f_{i_0+1}(X) \neq X\Sigma(F)(X)$.
  - Pour $v \in V$ $f_{i_0+1}(X+v) = f_{i_0+1}(X) + \sum_{1\leq i\leq i_0} \ell_i(v) f_i(X) \mod \wp(k[X])$
  - ℓ_i est une forme linéaire non nulle sur le $\mathbb{F}_p$-espace vectoriel V.
  - Soit $W := \cap_{1\leq i\leq i_0} \ker \ell_i$; $|W| \geq \frac{|V|}{p^{i_0}}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}(m_i - 1)) \geq \frac{(p-1)}{2}(p^{i_0}(m_{i_0+1} - 1))$.
  - $\frac{2p|W|}{(p-1)(m_{i_0+1}-1)} \leq \frac{2p}{p-1}$
  - $g_C \geq \frac{p-1}{2} p^{i_0}(m_{i_0+1} - 1) \geq \frac{p-1}{2}|V|$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t|V|}{(p-1)^2|V|^2}$
  - $|V|$ est majoré et $g_C^2 \leq \frac{p^t|V|}{M}$ est majoré.
  - $\{\frac{|G|}{g_C^2} = \frac{|G_2||V|}{g_C^2}\}$ est fi ni. ///

- Si l'image de ρ n'est pas triviale.
  - Il existe un plus petit i_0 tel que $f_{i_0+1}(X) \neq X\Sigma(F)(X)$.
  - Pour $v \in V$ $f_{i_0+1}(X+v) = f_{i_0+1}(X) + \sum_{1\leq i\leq i_0} \ell_i(v) f_i(X) \mod \wp(k[X])$
  - ℓ_i est une forme linéaire non nulle sur le $\mathbb{F}_p$-espace vectoriel V.
  - Soit $W := \cap_{1\leq i\leq i_0} \ker \ell_i$; $|W| \geq \frac{|V|}{p^{i_0}}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}(m_i - 1)) \geq \frac{(p-1)}{2}(p^{i_0}(m_{i_0+1} - 1))$.
  - $\frac{2p|W|}{(p-1)(m_{i_0+1}-1)} \leq \frac{2p}{p-1}$
  - $g_C \geq \frac{p-1}{2} p^{i_0}(m_{i_0+1} - 1) \geq \frac{p-1}{2}|V|$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t|V|}{(p-1)^2|V|^2}$
  - $|V|$ est majoré et $g_C^2 \leq \frac{p^t|V|}{M}$ est majoré.
  - $\{\frac{|G|}{g_C^2} = \frac{|G_2||V|}{g_C^2}\}$ est fi ni. ///

- Si l'image de ρ n'est pas triviale.
  - Il existe un plus petit i_0 tel que $f_{i_0+1}(X) \neq X\Sigma(F)(X)$.
  - Pour $v \in V$ $f_{i_0+1}(X+v) = f_{i_0+1}(X) + \sum_{1\leq i\leq i_0} \ell_i(v) f_i(X) \mod \wp(k[X])$
  - ℓ_i est une forme linéaire non nulle sur le $\mathbb{F}_p$-espace vectoriel V.
  - Soit $W := \cap_{1\leq i\leq i_0} \ker \ell_i$; $|W| \geq \frac{|V|}{p^{i_0}}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}(m_i - 1)) \geq \frac{(p-1)}{2}(p^{i_0}(m_{i_0+1} - 1))$.
  - $\frac{2p|W|}{(p-1)(m_{i_0+1}-1)} \leq \frac{2p}{p-1}$
  - $g_C \geq \frac{p-1}{2} p^{i_0}(m_{i_0+1} - 1) \geq \frac{p-1}{2}|V|$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t|V|}{(p-1)^2|V|^2}$
  - $|V|$ est majoré et $g_C^2 \leq \frac{p^t|V|}{M}$ est majoré.
  - $\{\frac{|G|}{g_C^2} = \frac{|G_2||V|}{g_C^2}\}$ est fi ni. ///

- Si l'image de ρ n'est pas triviale.
  - Il existe un plus petit i_0 tel que $f_{i_0+1}(X) \neq X\Sigma(F)(X)$.
  - Pour $v \in V$ $f_{i_0+1}(X+v) = f_{i_0+1}(X) + \sum_{1\leq i\leq i_0} \ell_i(v) f_i(X) \mod \wp(k[X])$
  - ℓ_i est une forme linéaire non nulle sur le $\mathbb{F}_p$-espace vectoriel V.
  - Soit $W := \cap_{1\leq i\leq i_0} \ker \ell_i$; $|W| \geq \frac{|V|}{p^{i_0}}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}(m_i - 1)) \geq \frac{(p-1)}{2}(p^{i_0}(m_{i_0+1} - 1))$.
  - $\frac{2p|W|}{(p-1)(m_{i_0+1}-1)} \leq \frac{2p}{p-1}$
  - $g_C \geq \frac{p-1}{2} p^{i_0}(m_{i_0+1} - 1) \geq \frac{p-1}{2}|V|$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t|V|}{(p-1)^2|V|^2}$
  - $|V|$ est majoré et $g_C^2 \leq \frac{p^t|V|}{M}$ est majoré.
  - $\{\frac{|G|}{g_C^2} = \frac{|G_2||V|}{g_C^2}\}$ est fi ni. ///

- Si l'image de ρ n'est pas triviale.
  - Il existe un plus petit i_0 tel que $f_{i_0+1}(X) \neq X\Sigma(F)(X)$.
  - Pour $v \in V$ $f_{i_0+1}(X+v) = f_{i_0+1}(X) + \sum_{1\leq i\leq i_0} \ell_i(v) f_i(X) \mod \wp(k[X])$
  - ℓ_i est une forme linéaire non nulle sur le $\mathbb{F}_p$-espace vectoriel V.
  - Soit $W := \cap_{1\leq i\leq i_0} \ker \ell_i$; $|W| \geq \frac{|V|}{p^{i_0}}$.
  - $g_C = \frac{(p-1)}{2}(\sum_{1\leq i\leq t} p^{i-1}(m_i - 1)) \geq \frac{(p-1)}{2}(p^{i_0}(m_{i_0+1} - 1))$.
  - $\frac{2p|W|}{(p-1)(m_{i_0+1}-1)} \leq \frac{2p}{p-1}$
  - $g_C \geq \frac{p-1}{2} p^{i_0}(m_{i_0+1} - 1) \geq \frac{p-1}{2}|V|$
  - $M \leq \frac{p^t|V|}{g^2} \leq \frac{4p^t|V|}{(p-1)^2|V|^2}$
  - $|V|$ est majoré et $g_C^2 \leq \frac{p^t|V|}{M}$ est majoré.
  - $\{\frac{|G|}{g_C^2} = \frac{|G_2||V|}{g_C^2}\}$ est fi ni. ///

Références 1

- M. Matignon: *Automorphism groups for p-cyclic covers of the affine line* (with C. Lehr), **Compos. Math.** 141 (2005), no. 5, 1213–1237.
- M. Matignon, (avec C. Lehr): *Wild monodromy and automorphisms of curves* , **Duke math. J.** à paraître, voir math.AG/0412294
- M. Matignon, (avec C. Lehr): *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.
- M. Matignon, (avec C. Lehr): *Curves with a big p-group action.* En préparation.

Références 2

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

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

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

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