

COURS DE JEAN-PIERRE SERRE

JEAN-PIERRE SERRE

E. BAYER (réd.)

C. GOLDSTEIN (réd.)

Problèmes Galoisien – I

Cours de Jean-Pierre Serre, tome 9 (1989)

http://www.numdam.org/item?id=CJPS_1989__9_

© Bibliothèque de l'IHP, 2015, tous droits réservés.

L'accès aux archives de la collection « Cours de Jean-Pierre Serre » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Notes numérisées par l'IHP et diffusées par le programme
Numérisation de documents anciens mathématiques*

<http://www.numdam.org/>

- 4 FEV. 2000

Jean - Pierre SERRE

Problèmes Galoisien - I

(Cours au Collège de France, janvier - mars 1989)

Notes de E. Bayer et C. Goldstein

N° Cote : PB 929 gal I-II
Institut Henri Poincaré BIBLIOTHÈQUE 11, rue P.-et-M.-Curie 75231 PARIS CEDEX 05
N° Inventaire : 28656B + 28657B

Algèbre et géométrie

M. Jean-Pierre SERRE, membre de l'Institut
(Académie des Sciences), professeur

ANNUAIRE

DU

COLLÈGE DE FRANCE
1988 - 1989

RÉSUMÉ
DES COURS ET TRAVAUX



89^e année

PARIS

11, place Marcelin-Berthelot (V^e)

Algèbre et géométrie

M. Jean-Pierre SERRE, membre de l'Institut
(Académie des Sciences), professeur

Le cours a été consacré au problème suivant : peut-on construire des extensions galoisiennes de \mathbf{Q} de groupe de Galois un groupe fini donné ?

1. La construction de Scholz-Reichardt (1936)

Cette construction s'applique aux p -groupes, $p \neq 2$.

Soit G un tel groupe. Choisissons un entier $n \geq 1$ tel que tout élément de G soit d'ordre $\leq p^n$.

SCHOLZ et REICHARDT prouvent l'existence d'extensions galoisiennes L/\mathbf{Q} , avec $\text{Gal}(L/\mathbf{Q}) = G$, satisfaisant à la condition suivante :

(S_n) – Pour tout nombre premier $q \in \text{ram}(L/\mathbf{Q})$, on a $q \equiv 1 \pmod{p^n}$, et le groupe d'inertie en q est égal au groupe de décomposition.

La démonstration procède par récurrence sur l'ordre de G . Si C est un sous-groupe central de G d'ordre p , l'hypothèse de récurrence montre qu'il existe une extension galoisienne K/\mathbf{Q} , avec $\text{Gal}(K/\mathbf{Q}) = G/C$, qui satisfait à (S_n). On prouve alors (en utilisant par exemple des arguments cohomologiques) qu'il existe une extension L/K , cyclique de degré p , qui est galoisienne sur \mathbf{Q} de groupe de Galois G et satisfait à (S_n). On peut même construire L de telle sorte que $\text{ram}(L/\mathbf{Q}) = \text{ram}(K/\mathbf{Q}) \cup \{q\}$, où q est un nombre premier aussi grand que l'on veut. D'où, si $|G| = p^m$, l'existence d'extensions galoisiennes de \mathbf{Q} du groupe de Galois G , qui ne sont ramifiées qu'en m nombres premiers.

Le théorème de Scholz-Reichardt a été étendu par SHAFAREVICH (1954) à tous les groupes résolubles finis. La démonstration de Shafarevich n'a pas été exposée dans le cours. Elle contient d'ailleurs une erreur relative au nombre premier $p = 2$, erreur qu'il serait souhaitable de corriger (dans les notes de ses « Collected Mathematical Papers », Shafarevich esquisse une méthode possible).

2. Le théorème d'irréductibilité de Hilbert et la propriété Gal_T

La plupart des méthodes de construction d'extensions galoisiennes à groupe de Galois donné utilisent le *théorème d'irréductibilité* de HILBERT (1892).

Grosso modo, ce théorème affirme ceci : si $L/\mathbf{Q}(T)$ est une extension galoisienne finie de groupe de Galois G , il existe une infinité de t appartenant à \mathbf{Q} tels que l'extension « spécialisée » L_t/\mathbf{Q} soit galoisienne de groupe G . Si de plus L est une extension *régulière* de $\mathbf{Q}(T)$ (i.e. ne contient aucune extension algébrique de \mathbf{Q} , à part \mathbf{Q}), on peut exiger que les L_t soient linéairement disjointes d'une extension donnée de \mathbf{Q} . (Le même énoncé vaut pour les extensions galoisiennes d'un corps de fonctions rationnelles $\mathbf{Q}(T_1, \dots, T_n)$, $n \geq 1$.)

On peut prouver que les « mauvaises » valeurs de t ne sont pas très nombreuses. Cela se fait par un argument de « crible », qui avait été exposé dans le cours de 1980-1981.

Disons qu'un groupe fini G possède la propriété Gal_T s'il satisfait aux conditions équivalentes suivantes :

(i) Il existe une extension galoisienne régulière de $\mathbf{Q}(T)$ de groupe de Galois G .

(ii) Il existe un entier $n \geq 1$ et une extension galoisienne régulière de $\mathbf{Q}(T_1, \dots, T_n)$ de groupe de Galois G .

(Le fait que (ii) \implies (i) est une conséquence du théorème de Bertini.)

D'après le théorème de Hilbert ci-dessus, Gal_T entraîne que G est groupe de Galois d'une infinité d'extensions de \mathbf{Q} , deux à deux disjointes ; en particulier, pour tout corps de nombres K il existe une extension galoisienne L/K telle que $\text{Gal}(L/K) = G$. Il est donc intéressant de donner des exemples de groupes G ayant la propriété Gal_T :

— G abélien ;

— $G = S_n$ ou A_n , d'après HILBERT (1892) ;

— $G = \text{PSL}_2(\mathbf{F}_p)$, où p est un nombre premier tel que $\left(\frac{2}{p}\right) = -1$, ou

$\left(\frac{3}{p}\right) = -1$, ou $\left(\frac{7}{p}\right) = -1$, d'après K.-y. SHIH (1974).

D'autres exemples seront traités dans le cours de 1989-1990, par la méthode de « rigidité ».

3. La méthode d'E. Noether (1918)

On réalise le groupe donné G comme sous-groupe du groupe de permutations S_n , ce qui permet de le faire opérer sur le corps $L = \mathbf{Q}(X_1, \dots, X_n)$. Si

$K = L^G$ désigne le corps des invariants de L on obtient ainsi une extension galoisienne régulière L/K de groupe de Galois G . Supposons que la condition suivante soit satisfaite :

(N) – Le corps K est une extension stablement rationnelle de \mathbf{Q} , i.e. $K(T_1, \dots, T_m)$ est isomorphe à $\mathbf{Q}(T_1, \dots, T_{n+m})$ pour m assez grand.

(On peut prouver que cette condition ne dépend pas du plongement choisi de G dans un groupe symétrique.)

On a alors Gal_T , ce qui montre que G est groupe de Galois d'une extension de \mathbf{Q} . C'est la méthode proposée par E. NOETHER.

Cette méthode est rarement applicable. La condition (N) est trop forte. Elle n'est pas satisfaite lorsque G est cyclique d'ordre 47 (SWAN, VOSKRESENSKII, 1969) ou d'ordre 8 (LENSTRA, 1974). En fait, même l'analogie de (N) sur \mathbf{C} peut être en défaut : le corps K_C des invariants de G dans $\mathbf{C}(X_1, \dots, X_n)$ n'est pas toujours stablement rationnel sur \mathbf{C} . De façon plus précise, SALTMAN (1984) a montré que, s'il existe un élément non nul de $H^2(G, \mathbf{Q}/\mathbf{Z})$ qui induit 0 sur tous les sous-groupes abéliens à deux générateurs de G , alors K_C n'est pas stablement rationnel sur \mathbf{C} (on construit des exemples de tels groupes G en prenant des extensions centrales convenables de groupes abéliens élémentaires). La démonstration repose sur l'étude du « groupe de Brauer non ramifié » du corps K_C . (Les résultats de Swan, Voskresenskii, Lenstra et Saltman ont été exposés dans le Séminaire par J.-L. COLLIOT-THÉLÈNE.)

4. Une variante de la méthode d'E. Noether

Cette variante, due à EKEDAHL et COLLIOT-THÉLÈNE (1987), vise à remplacer la condition (N) par une condition plus faible, susceptible d'être vérifiée pour tout groupe fini G .

Soit K une extension régulière de type fini de \mathbf{Q} , et soit V une \mathbf{Q} -variété intègre lisse de corps des fonctions K . Disons que K satisfait à la condition d'*approximation faible affaiblie* si :

(AFA) – Il existe un ensemble fini T de nombres premiers tel que, pour tout ensemble fini S de nombres premiers disjoint de T , l'image de $V(\mathbf{Q})$ dans le produit des $V(\mathbf{Q}_p)$, $p \in S$, est dense. (Cette propriété ne dépend pas du choix de V .)

La condition (AFA) est plus faible que « K est stablement rationnel ». Elle est cependant suffisante (Ekedahl et Colliot-Thélène) pour entraîner un théorème d'irréductibilité à la Hilbert :

Si L/K est une extension galoisienne de groupe de Galois G , et si K satisfait à (AFA), on peut en déduire par spécialisation des extensions galoisiennes de \mathbf{Q} à groupe de Galois G . Si de plus L est \mathbf{Q} -régulière, on peut

obtenir des extensions linéairement disjointes de toute extension finie de \mathbf{Q} donnée.

Ainsi, la méthode d'E. Noether pourrait s'appliquer à tout groupe fini G , pourvu que l'on puisse montrer que les corps $K = L^G$ correspondants satisfont à (AFA), ce qui est vrai dans tous les cas connus. On peut même espérer (Colliot-Thélène) que (AFA) est vraie pour tout corps K qui est « unirationnel », i.e. sous-corps d'un corps $\mathbf{Q}(X_1, \dots, X_n)$.

SÉMINAIRE

Jean-Louis COLLIOT-THÉLÈNE, *Exemples de variétés non rationnelles* (2 exposés).

PUBLICATIONS

J.-P. SERRE, *Abelian ℓ -adic representations and elliptic curves* (McGill University Lecture Notes, written with the collaboration of Willem KUYK and John LABUTE), 2^e édition révisée, Addison-Wesley, 1989.

— *Lectures on the Mordell-Weil Theorem* (translated and edited by Martin BROWN from notes by Michel WALDSCHMIDT), Vieweg, 1989.

MISSIONS

Cours

— *Topics in Galois Theory*, Harvard, septembre-décembre 1988.

Exposés

— *Abelian varieties and their division points* (3 exposés), Schloss Ringberg, juillet 1988.

— *Galois groups and modular forms*, Stockholm, septembre 1988 ;

— *Homotopy groups : why and why not ?*, Harvard, octobre 1988 ;

— *Root systems*, Harvard, novembre 1988 ;

- *Galois groups over \mathbf{Q}* , McGill University, novembre 1988 ; M.I.T., novembre 1988 ; State College, décembre 1988 ;
- *Modular forms mod p , and quaternions*, Columbia, novembre 1988 ;
- *La forme $\text{Tr}(x^2)$: suite*, Bordeaux, mars 1989 ; Zurich, mai 1989 ;
- *Some examples of modular Galois representations mod p* , Texel, avril 1989 ;
- *Problèmes énumératifs sur les coniques, d'après CHASLES*, E.N.S., mai 1989 ;
- *Sommes de trois carrés dans $\mathbf{F}_q[T]$* , Zurich, mai 1989 ;
- *La moyenne arithmético-géométrique*, Académie des Sciences, juin 1989 ;
- *Réductions supersingulières d'une courbe elliptique, d'après N. ELKIES*, Séminaire de Théorie des Nombres, Paris, juin 1989 ;
- *Automorphic forms mod p on quaternion groups*, Durham, juillet 1989 ;
- *Points rationnels et cribles*, Luminy, juillet 1989 ;
- *Motifs*, Luminy, juillet 1989.

Problèmes Galoisiens I (1989)

Introduction	...	1
Méthode d'E. Noether	...	10
Exemples de bas degrés	...	13
Théorème de Scholz - Reichardt	...	21
Sous-groupes de Frattini	...	41
Ishanov - Safarovič	...	45
Variétés rationnelles	...	49
Lemme sans nom	...	51
Gal _T	...	56
Bitangentes réelles	...	59
Construction de Saltman	...	65
Th. d'inv'd. de Hilbert	...	70
Ensembles minis	...	71
Propriété de Hilbert	...	72
Lien entre Hilbert et appr. faible	...	83
Conjecture de Colliot-Thélène	...	87
Le théorème du grand crible	...	91
Groupes de Galois S_n et A_n	...	101
Fonctions de Mordell	...	106
La construction de Shih	...	113

Problèmes galoisiens

Construction d'extension à groupe de Galois
donné de \mathbb{Q}
de $\mathbb{Q}(T)$

G groupe fini.

Conjecture : Il existe une extension galoisienne
de \mathbb{Q} de groupe de Galois G .

G groupe simple non abélien

ordre croissant :

A_5	60	}	connus pour être groupes de Galois d'ext. de $\mathbb{Q}(T)$
$SL_3(\mathbb{F}_2)$	168		
A_6	360		
$SL_2(\mathbb{F}_8)$	504		
⋮			

10^{ème} : $SL_2(\mathbb{F}_{16})$ ← exemples sur
 \mathbb{Q} , mais
pas sur $\mathbb{Q}(T)$.

Les petits groupes sont souvent des PSL_2
et la conjecture est connue dans ce cas.
 M_{23} ?

Conjecture de $\mathbb{Q}(T)$, irrégulière
de groupe G .

$$\begin{array}{c} E \\ | \\ \mathbb{Q}(T) \end{array}$$
 régulière si disjointe de $\bar{\mathbb{Q}}/\mathbb{Q}$

Si $E/\mathbb{Q}(T)$ galoisienne, elle est régulière $\Leftrightarrow \mathbb{Q}$ fermé dans l'extension

$E/\mathbb{Q}(T)$ régulière $\Leftrightarrow E$ est corps de fct d'une courbe absolument irréductible sur \mathbb{Q} .

Hilbert 1890, théorème d'irréductibilité $\Rightarrow S_n, A_n$ sont groupes de Galois sur $\mathbb{Q}, \mathbb{Q}(T)$.

Equation

$$P = X^n + a_1(T)X^{n-1} + \dots + a_n(T) = 0$$

K corps de caractéristique 0. Supposons l'équation irréductible sur $K(T)$.

$$a_i(T) \in K(T)$$

$t \in K \neq$ pôles de a_i

$$P_t(x) = 0$$

Hilbert Si K est un corps de nombres il existe une infinité de $t \in K$ tels que

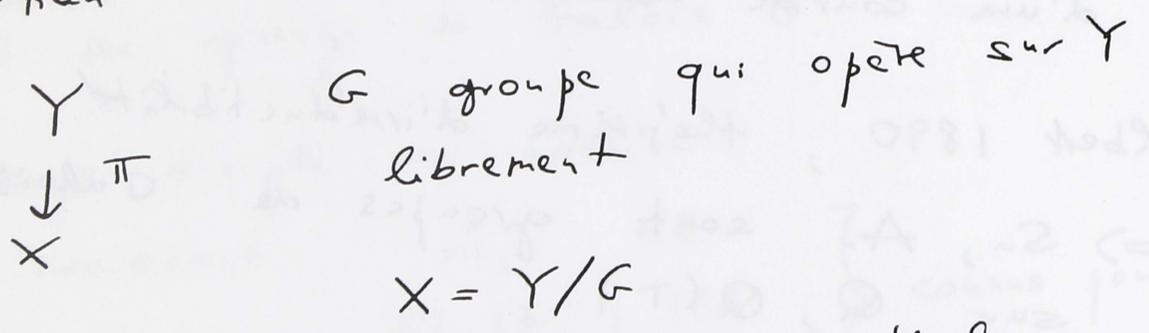
1.) $P_t(x)$ irréductible

G groupe de Galois de $P \subset S_n$

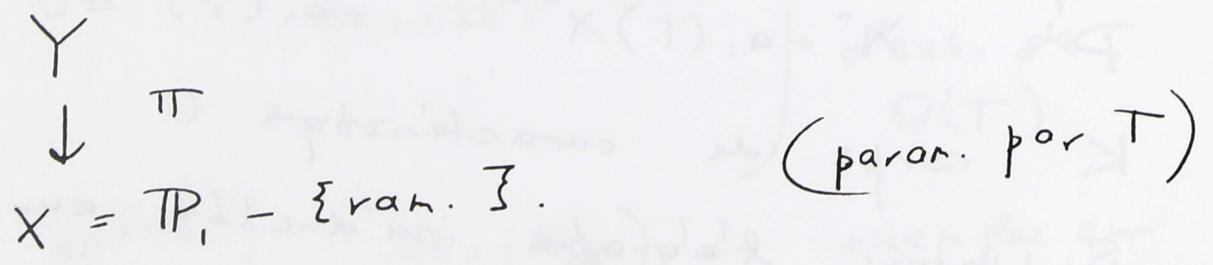
2.) le groupe de Galois de P_t soit égal à celui de P .

Vrai pour plusieurs variables. Presque tous les $t \in K$ conviennent (par ex. si $K = \mathbb{Q}$, $|t| \leq N$, $t \in \mathbb{Z}$, ceux qui ne conviennent pas sont en nombre $O(N^{1/2})$).

Si k est un corps quelconque, $k(t)$ est hilbertien.



k revêtement galoisien étale.



$x \in X(k) \quad \pi^{-1}(x) = ?$

Sur \bar{k} , $\pi^{-1}(x)$ ds $Y(\bar{k})$

G opère librement. Pas des pts de $Y(k)$ en général.

Irr Si les points $y \in \pi^{-1}(x)$ sont conjugués entre eux par $\text{Gal}(\bar{k}/k)$

\Rightarrow extension galoisienne de k à \bar{k}
groupe de Galois G .

Cas général (i.e. si Irr n'est pas vraie).

$y \in \pi^{-1}(x)$. Orbite de y par $Gal(F/k)$

$$s \in Gal(F/k) \longrightarrow G$$

$$s(y) = g(s)^{-1}y$$

$$s \longrightarrow g(s)$$

Autre façon de faire :

$\pi^{-1}(x)$ schéma fini étale sur k avec action de G

Λ_x = algèbre affine de $\pi^{-1}(x)$

G -algèbre galoisienne

produit de corps.

Cas Irr : celui où Λ_x est un corps

$$\begin{array}{c}
K(x)^{gal} \\
| \\
K(x) \\
| \\
K(t)
\end{array}$$

$$\begin{array}{c}
Y \\
\downarrow \\
X_n \text{ de deg } n \\
\downarrow \\
X = \mathbb{P}^1 - \{\Delta = 0\}
\end{array}$$

$$\begin{array}{c}
Y \\
\downarrow G \\
X
\end{array}$$

K corps de nombres
 X variété K -rationnelle
($K(x)$ ext. transcendant pure de K).

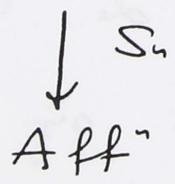
Alors le théorème d'irréductibilité de Hilbert marche

Ekedahl } conjecturent ?? (ou
Colliot-Thélène } verra plus tard :
quelque chose d'un
peu plus faible que
l'approximation faible)

?? de E-CT =>
conjecture

S_n

S_n agissant sur Affⁿ par perm. des coord.



$K[x_1, \dots, x_n]$

|
 $K[\sigma_1, \dots, \sigma_n]$

E. Noether (~ 1918)

Méthode de Hilbert s'applique à tout slg
G de S_n pourvu que le corps des
invariants dans $\mathbb{Q}(x_1, \dots, x_n)$ soit une
extension transcendante pure de \mathbb{Q} .

Vrai pour slg de S₄.

Construction directe (arithmétique) (6)
pour G un p -groupe par Scholz
et Reichardt (~ 1938).

Démonstration la semaine prochaine

G d'ordre p^m

On peut choisir E/\mathbb{Q} , $\text{Gal} = G$
 E ramifiée en seulement m nombres
premiers.

$m=1$ groupe cyclique d'ordre p

$$l \equiv 1 \pmod{p}$$

$$(\mathbb{Z}/l\mathbb{Z})^* \longrightarrow C_p$$

$$\mathbb{Q}(\zeta_p) \supset E \supset \mathbb{Q}$$

Scholz - Reichardt marche pour groupes
nilpotents d'ordre impair.

Thm de Šafarevič : groupes résolubles (~ 1954)
contient une erreur pour $p=2$
Ishanov, Faddeev et ? ont écrit un
livre sur cette démonstration qui paraîtra
bientôt.

G résoluble d'ordre impair : démonstration
de Neukirch (1977)

R. Swan (1969)

le corps des invariants de G n'est pas toujours pur (sur \mathbb{Q}).

e.g. G cyclique d'ordre 47.

(Exposé de Colliot-Thélène sur ce résultat, ainsi que sur un thm de Saltman (~1984) pas vrai sur \mathbb{C} p -groupes, p^2 ou mieux).

Lenstra (G abélien) a donné critère nécessaire et suffisant. 47 peut être remplacé par 8.

Aussi résultats de Voskresenskiï.

Remarque de Saltman: résultat de non-pureté pour 8 était évident:

Wang (~1949)

"thm" de Grünwald. On donne des caractères locaux

$$\begin{array}{l}
 i=1, \dots, k \\
 p_i \text{ distinct} \\
 G_{\mathbb{Q}_{p_i}} \xrightarrow{\chi_i} C_n \text{ cyclique d'ordre } n \\
 \mathbb{Q}_{p_i}^* \rightarrow C_n
 \end{array}$$

Il existe un homomorphisme global

$$\chi: G_{\mathbb{Q}} \rightarrow C_n$$

qui, localement en p_i , donne χ_i .

On cherche
$$\begin{array}{c} E \\ | \\ \mathbb{Q} \end{array} C_n$$

algèbre galoisienne, donnée localement.

Publiée par Grünwald ~ 1938.

Contre-exemple de Wang: $n=8$

$k=1, p_i=2$

$G_{\mathbb{Q}_2} \rightarrow C_8$ homomorphisme surjectif non ramifié.

Il s'agit de montrer qu'il n'y a pas d'extension cyclique de $d^{\circ} 8$ de \mathbb{Q} qui soit non ramifiée en \mathbb{Q}_2 et donc une extension cyclique de $d^{\circ} 8$ de \mathbb{Q}_2 .

Une telle extension E est associée à un caractère

$$\chi: (\mathbb{Z}/n\mathbb{Z})^* \xrightarrow{\text{sur}} C_8$$

$z \mapsto z^n, \chi(z)$ engendre C_8 .

$n = \prod l^{\alpha}$. On voit facilement que $\alpha=1$

$n = \prod_{l \neq 2} l$ $\chi = \prod \chi_l$

$$\chi_l: (\mathbb{Z}/l\mathbb{Z})^* \rightarrow C_8$$

Il existe un l tel que $\chi_l(z)$

engendre C_8 .

$$8 \mid l-1 \Rightarrow l \equiv 1 \pmod{8} \Rightarrow \left(\frac{2}{l}\right) = 1 \Rightarrow$$

$$2 = x^2 \quad x \in (\mathbb{Z}/l\mathbb{Z})^*$$

$\Rightarrow \chi(z) = \chi(x)^2 \Rightarrow \chi(z)$ n'est pas un g n rateur !

Dans Artin - Tate il y a "liste" des contre-exemples. Par exemple le thm est tjs vrai si n est impair.

Si "Noether" marche :

$$\mathbb{Q}(x_1, \dots, x_n)^G \text{ pur,}$$

on obtient une extension g n rique (universelle) elle donne par sp cialisation

toutes les extensions a groupe de Galois G .

$$\begin{array}{c} E \\ |^G \\ K \end{array}$$

$$\begin{array}{c} Y \\ \downarrow^G \\ X \\ p \in X \end{array}$$

$$\text{Gal}(E/K) \xrightarrow{\psi_E} G$$

On "brd" :

$$\begin{array}{c} Y_p \\ \downarrow \\ X \end{array}$$

points rat de $Y_p \rightarrow \text{ext.}$

v rifier que Y_p a des points rat.

Hilbert 90.

$\text{pure } k' \Rightarrow \text{Grünwald}$
 C_n

$X: \mapsto \text{pts } P_i \in X(\mathbb{Q}_{p_i})$

approximation faible pour X : on

approche P_i par $P \in X(\mathbb{Q})$.

La fibre est la même. $\} \text{ donne l'extension voulue.}$

—
Méthode d'E. Noether

Si elle fonctionne, donc ext. géométriques.

Autre méthode: méthode de "rigidité":

K-y. Shih, M. Fried, V. Belyi, J. Thomson, B. Mazur

Thomson: $M = F$, "Mouste" est groupe de Galois sur $\mathbb{Q}(T)$

(modulo thm de classification des groupes simples).

C_1, C_2, C_3 classes de conjugaison de G

- 1.) C_i rationnelles
- 2.) (C_1, C_2, C_3) rigide :

a.) il existe $x_i \in C_i$ avec $x_1 x_2 x_3 = 1$
 et $G = \langle x_1, x_2 \rangle$

b.) un tel (x_1, x_2, x_3) est unique
 à G -conj. près

$$y_1, y_2, y_3 \quad \exists g \in G \quad y_i = g x_i g^{-1}$$

Théorème (Shih --- Thomson)

Tout groupe G de centre trivial ayant
 une famille (C_1, C_2, C_3) rigide et rat.
 est groupe de Galois sur $\mathbb{Q}(T)$ (ram.
 seulement en $0, 1$ et ∞).

$$\text{Nombre des } x_i = \frac{|C_1| |C_2| |C_3|}{|G|} \sum \dots$$

voir exposé Bourbaki.

Pour Mestre: prendre $C_1 = 2A, C_2 = 3B,$
 $C_3 = 29A$

engendrent s/g $H \subsetneq G$

↓
 quotients simples. Voir atlas

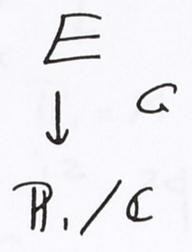
Sur \mathbb{C}

$\mathbb{C}(T)$

$\mathbb{P}^1 / \mathbb{C}$



Groupe fondamental libre de $a \geq 2$ g'enerateurs



unique, α isomorphisme unique pres.

Variantes (Matzart).

Cette methode ne marche pas pour tous les groupes, par ex. A_5 .

Matzart fait intervenir le groupe des tresses.

Groupes sporadiques: connus, sauf M_{23} .

Groupes non sporadiques

- $PSL_2(\mathbb{F}_p)$ $p \equiv ?$
- $G_2(\mathbb{F}_p)$ (Thomson)

Industrie des $Tr(x^2)$:

groupes de centre d'ordre 2.

E.g. \tilde{A}_n V, ρ_a $n \equiv ? \pmod{8}$
 Mestre en general.

Exemples d'extensions de bas degre'

$n = 2$
 $K \text{ car } \neq 2$

\mathbb{P}^1	x	$\{0, \infty\}$ ram.
\downarrow	\downarrow	
\mathbb{P}^1	$x^2 = T$	

$K(\sqrt{T})$ corps si T non carré

G_m	x
\downarrow	\downarrow
G_m	x^2

Cyclique d'ordre 3 C_3

$C_3 \hookrightarrow GL_2$

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

C_3 agit sur \mathbb{P}^1

\downarrow

$\mathbb{P}^1 = \mathbb{P}^1 / C_3$

$$\sigma : X \mapsto \frac{1}{1-X}$$

$$T = X + \sigma X + \sigma^2 X = \frac{X^3 - 3X + 1}{X^2 - X}$$

$$X^3 - 3X + 1 = T(X^2 - X)$$

$$X^3 - TX^2 + (T-3)X + 1 = 0.$$

Donne toutes les extensions cubiques de K .
 Marche en toute caractéristique.

Comment monte-t-on que c'est g  n  rique?

C_3 agit sur $\mathbb{P}_1 = Y$

\downarrow
 $\mathbb{P}_1 = X$

E
| cubique
 K cyclique

$C_K \xrightarrow{\psi_E} C_3$

On prend $Y = \mathbb{P}_1$ par ψ_E .

Est-ce que Y^ψ a des points rationnels?

$\psi_E \in H^1(G_K, GL_2) = 0$ (Herbert 90.)

\downarrow
 $H^1(G_K, PGL_2)$

Donc $Y_{\psi_E} \cong \mathbb{P}_1$.

Autre d  monstration: Y_{ψ_E} a des points rationnels sur une extension de degr   impair. Par Springer,

Y_{ψ_E} a des points rationnels.

Extensions cycliques de degr   4.

K $K_2 = K(\sqrt{\varepsilon})$, $\varepsilon \in K^*$
non carr  !

car $\neq 2$

Existe-t-il K_4 tel que

$$C_4 \begin{pmatrix} K_4 \\ | \\ K_2 \\ | \\ K \end{pmatrix} ?$$

Decrire les K_4 possibles.

$$K_4 = K_2(\sqrt{a+b\sqrt{\epsilon}}) \quad a, b ?$$

Théorème K_4 est cyclique de $d^{\circ}4$ sur K

$$\Leftrightarrow \exists c \in K^* \text{ avec } a^2 - \epsilon b^2 = \epsilon c^2.$$

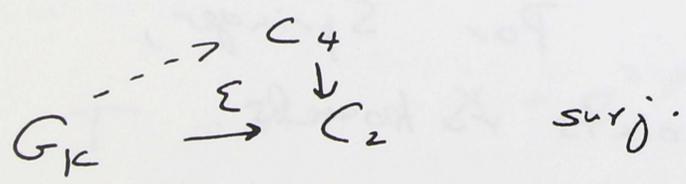
Corollaire: K_4 existe $\Leftrightarrow a^2 - \epsilon b^2 - \epsilon c^2 = 0$ a solutions

$$\Leftrightarrow (\epsilon, \epsilon) = 0 \text{ dans } Br_2(K).$$

$$\parallel$$

$$(-1, \epsilon)$$

$\Leftrightarrow \epsilon$ est somme de 2 carrés



$$0 \rightarrow C_2 \rightarrow C_4 \rightarrow C_2 \rightarrow 0$$

$$\quad \quad \quad \mathbb{Z}/2\mathbb{Z} \quad \quad \mathbb{Z}/4\mathbb{Z}$$

$$H^1(G_K, \mathbb{Z}/4\mathbb{Z}) \rightarrow H^1(G_K, \mathbb{Z}/2\mathbb{Z}) \xrightarrow{\delta} H^2(G_K, \mathbb{Z}/2\mathbb{Z})$$

$\begin{matrix} \psi \\ \varepsilon \end{matrix}$ $\begin{matrix} \text{"} \\ \text{Br}_2(K) \end{matrix}$

$$\delta \varepsilon = 0 ? \quad \in \text{Br}_2(K)$$

Pour tout groupe G , on a $\delta x = xx \quad x \in H^1$.

(cas particulier de formules sur les carrés de Steenrod)

$$G = \mathbb{Z}/2\mathbb{Z} \quad \begin{matrix} H^1(G) = \mathbb{Z}/2\mathbb{Z} \\ H^2(G) = \mathbb{Z}/2\mathbb{Z} \end{matrix} \quad \begin{matrix} x \\ \downarrow \delta \\ xx \end{matrix}$$

$\delta x = xx$ est vraie pour $G = \mathbb{Z}/2\mathbb{Z}$.

Entraîne que c'est vrai pour tout G
 $x \in H^1(G)$

$$x : G \rightarrow \mathbb{Z}/2\mathbb{Z}$$

"Méthode de l'exemple universel".

Si $\mu_4 \subset K$, pas de problème.
 -1 carré, donc $(-1, \varepsilon) = 0$.

Autre démonstration: marche si $\mu_4 \subset K$, descente.

Soit G un groupe et $\varepsilon: G \rightarrow C_2$ surjectif
Soit H le noyau, $(G:H)=2$.

$$G = G_K, \quad H = G_{K_2}$$

Soit $\chi: H \rightarrow C_2$. Soit $H_\chi = \text{Ker } \chi$.

Théorème: Pour que H_χ soit invariant
dans G à quotient $\cong C_4$ il faut et
il suffit que $\text{Cor}_H^G \chi = \varepsilon$ dans $H'(G)$

$$\varepsilon \in H'(G) = \text{Hom}(G, \mathbb{Z}/2\mathbb{Z})$$

$$\chi \in H'(H) = \text{Hom}(H, -)$$

$$\text{Cor}_H^G : H'(H) \rightarrow H'(G)$$

$$\text{Cor}_H^G(\chi) : G^{ab} \xrightarrow{\text{Ver}_H^G} H^{ab} \xrightarrow{\chi} C_2$$

$\text{Ver}_H^G = \text{transfer}$

Application: $G = G_K, \quad H'(G) = K^*/K^{*2}$
 $H = G_{K_2}, \quad H'(H) = K_2^*/K_2^{*2}$

$$\text{Cor}_H^G : K_2^*/K_2^{*2} \rightarrow K^*/K^{*2}$$

norme $N_{K_2/K}$.

$$\chi \in H'(H) \text{ corr. à } a + b\sqrt{\varepsilon}$$

$$\varepsilon \in H'(G) \iff \varepsilon \in K^*/K^{*2}$$

$$N(a+b\sqrt{\epsilon}) = \epsilon c^2$$

Même genre de question en car 2 :

$$K_2 = K(x) \quad \begin{aligned} \wp x &= x^2 + x \\ \wp x &= \epsilon \end{aligned} \quad \epsilon \in K$$

$$K_4 = K(y) \quad \wp y = a + b$$

K_4 cyclique de $d^o 4$?

$$H^1(G) = K / \wp K$$

$$H^1(H) = K_2 / \wp K_2$$

Cor = trace

$$\text{Tr}(a+bx) \equiv \epsilon \pmod{\wp K}$$

$$b = \epsilon + z^2 + z, \quad z \in K.$$

$$H^i(G_K) = 0, \quad i \geq 2.$$

Pos gènerique s: $\forall \epsilon \in K, \exists x^2 + x = \epsilon$ (conjugue)

Exercice : Si $\epsilon \in K, \exists x^2 + x = \epsilon$,
 il n'existe pas d'extension gènerique
 à 1 paramètre de groupe C_4 .

Compléments sur les extensions cycliques
de degré 4

$$K_4 = K_2(\sqrt{a+b\sqrt{\varepsilon}})$$

$$\begin{array}{c} | \\ K_2 = K(\sqrt{\varepsilon}) \end{array}$$

$$\begin{array}{c} | \\ K \end{array}$$

cyclique de degré 4



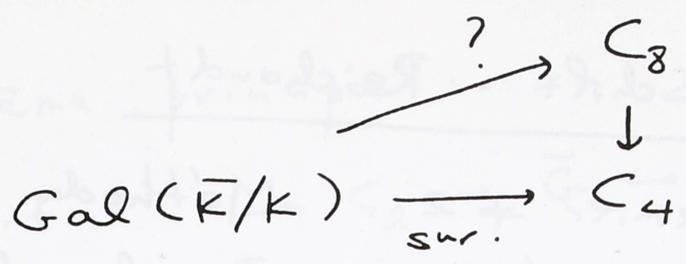
il existe $c \in K^\times$ t. q. $a^2 - \varepsilon b^2 = c^2 \varepsilon$.

$\varepsilon \neq 0$
 $c \neq 0$ e.v. alg. gal.

$$\begin{array}{cc} \sigma & c \\ \sigma^{-1} & -c \end{array}$$

Peut-on plonger dans ext. cyclique
de degré 8 ?

$$C_8 \left\{ \begin{array}{c} K_8 \\ | \\ K_4 \\ | \\ K \end{array} \right.$$



Obstr. $\in H^2(\text{Gal}(\bar{K}/K), C_2) = \text{Br}_2(K)$.

Formule : $\text{Obstr.} = (2, \varepsilon) + (-1, a) \quad a \neq 0$
 $= (2, \varepsilon) \quad a = 0$

On le voit par $\text{Tr}(x^2)$.

Autre méthode pour obtenir une famille d'extensions cycliques de degré 4 :

$$C_4 \subset \text{PGL}_2(\mathbb{Q})$$

$$\begin{array}{c}
 \mathbb{P}^1 \\
 | \\
 C_4
 \end{array}$$

$$\mathbb{P}^1 / C_4 = \mathbb{P}^1$$

Famille d'extensions cycliques de degré 4 de $\mathbb{Q}(T)$, donnée par l'équation :

$$X^4 - TX^3 + 6X^2 + TX + 1 = 0$$

Pas générique si $\sqrt{-1} \notin K$ (correspond à $(-1, a) = 0$).

Exercice : Si $\sqrt{-1} \notin K$, car $K \neq \mathbb{2}$, il n'existe pas d'extension générique à 1 paramètre de groupe C_4 .

Théorème de Scholz - Reichardt

l nombre premier $\neq 2$. Méthode de Scholz, complétée par Reichardt :

Soit L/\mathbb{Q} une extension galoisienne de groupe de Galois G , où G est un l -groupe d'ordre l^m ($m \geq 1$).
 $\text{ram}(L/\mathbb{Q}) = \text{ens. des } p \text{ ramifiés dans } L/\mathbb{Q}$.

Soit N un entier.

On dit que L/\mathbb{Q} a la propriété (S_N) si, pour tout $p \in \text{ram}(L/\mathbb{Q})$, on a :

① $p \equiv 1 \pmod{l^N}$

② Le groupe d'inertie I_p rel. à p coïncide avec le groupe de déc. D_p , plus précisément :

choisissons $v|p$, v place de L
 $I_v \subset D_v \subset G$ inertie et déc.

② : $I_v = D_v$

$$D_v / I_v = \text{Gal}(L(v) / \mathbb{F}_p) \stackrel{②}{=} 1$$



$$L(v) = \mathbb{F}_p$$



$$\text{Frob}_v = 1.$$

Théorème principal :

Soit $1 \rightarrow C_\ell \rightarrow \tilde{G} \rightarrow G \rightarrow 1$
 suite exacte de ℓ -groupes, C_ℓ cyclique
 d'ordre ℓ , $C_\ell \subset$ centre de \tilde{G} .

On suppose que l'exposant de \tilde{G} divise ℓ^N
 i.e. $x^{\ell^N} = 1$ pour tout $x \in \tilde{G}$.

Théorème :

Soit L/\mathbb{Q} une extension galoisienne de
 groupe G satisfaisant $\bar{\alpha}(S_N)$.
 Il existe alors une extension galoisienne
 \tilde{L}/\mathbb{Q} de groupe \tilde{G} , contenant L ,
 satisfaisant $\bar{\alpha}(S_N)$ et telle que

$$\text{ram}(\tilde{L}/\mathbb{Q}) = \text{ram}(L/\mathbb{Q}) \cup \{q\}.$$

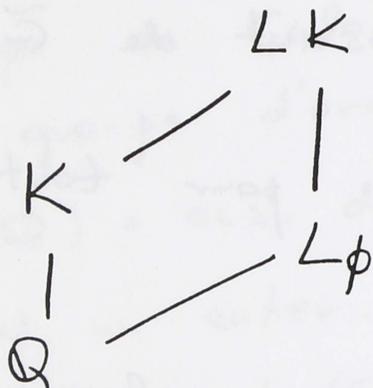
Corollaire :

Pour tout ℓ -groupe ϕ d'ordre ℓ^α ,
 il existe une extension galoisienne
 L_ϕ de \mathbb{Q} , de groupe ϕ , avec
 $|\text{ram}(L_\phi/\mathbb{Q})| = \alpha$.

Démonstration par récurrence sur α .

On applique le théorème avec $\phi = \tilde{G}$,
 N tel que $\exp(\phi)$ divise ℓ^N .

On obtient ramification disjointe d'un ensemble fini donné. Ceci permet de réaliser ϕ sur n'importe quel corps de nombres K :



On demande $\text{ram}(L\phi/\mathbb{Q}) \cap \text{ram}(K/\mathbb{Q}) = \emptyset$.

Le cas d'un groupe profini ϕ

Soit ϕ un groupe profini. On dit que ϕ est un groupe "séparable", ou "de type dénombrable", s'il satisfait aux conditions équivalentes suivantes:

- 1.) La topologie de ϕ est métrisable
- 2.) Il y a un sous-ensemble dénombrable dense
- 3.) Les s/g ouverts forment un ensemble dénombrable
- 4.) $\phi = \varprojlim (\rightarrow \phi_m \rightarrow \phi_{m-1} \rightarrow)$, (dénombrable)
 \leftarrow
 ϕ_i finis, flèches surjectives.

Si $\phi = \text{Gal}(L/K)$, ces propriétés
sont équivalentes à $[L:K] \leq \aleph_0$;
si ϕ est un pro- ℓ -groupe, elles
sont équivalentes à $\dim H^1(G, \mathbb{Z}/\ell\mathbb{Z}) \leq \aleph_0$.

Remarquons que $\text{Gal}(\overline{\mathbb{C}(T)}/\mathbb{C}(T))$
n'est pas séparable.

Théorème :

Si ϕ est un pro- ℓ -groupe séparable
d'exposant fini, alors il existe une
extension galoisienne de \mathbb{Q} de groupe
de Galois ϕ .

Exposant fini $\Leftrightarrow \exists N$ t.q. $x^{\ell^N} = 1$
pour tout $x \in \phi$.

C'est un cas particulier du théorème
de Neukirch.

On utilise la condition 4.

$$\phi = \varprojlim \phi_n$$

On peut supposer que

$$1 \rightarrow C_\ell \rightarrow \phi_n \rightarrow \phi_{n-1} \rightarrow 1$$

$\underbrace{\hspace{1.5cm}}$
cyclique d'ordre ℓ ,

l^N : exponent des ϕ_n

$$\phi_n \begin{pmatrix} L_{n+1} \\ | \\ L_n \end{pmatrix} \quad (S_N)$$

Contre-exemples si on enlève la condition "exposant borne" :

$\mathbb{Z}_l \times \mathbb{Z}_l$ n'est pas groupe de Galois / \mathbb{Q} .

Démonstration du théorème de Scholz - Reichardt :

$$1 \rightarrow C_l \rightarrow \tilde{G} \rightarrow G \rightarrow 1$$

N t.q. $\exp(\tilde{G})$ divise l^N .

L/\mathbb{Q} de groupe G , avec (S_N) .

Construire \tilde{L} ?

1^{er} cas

$$\tilde{G} = G \times C_l$$

$\tilde{L} = LE$, E/\mathbb{Q} cyclique de degré l linéairement disjointe de L .

\tilde{L} satisfait à la condition (S_N)

$$\text{ram}(E/\mathbb{Q}) = \{q\},$$

$$q \notin \text{ram}(L/\mathbb{Q}).$$

Conditions sur q :

$$q \equiv 1 \pmod{\ell^N}$$

q totalement décomposé dans L/\mathbb{Q}

pour tout $p \in \text{ram}(L/\mathbb{Q})$, l'image de p dans \mathbb{F}_q est une puissance ℓ -ième.



q est totalement décomposé dans

$$\mathbb{Q}(\sqrt[\ell^N]{1}),$$

L ,

$$\mathbb{Q}(\sqrt[\ell]{1}, \sqrt[\ell]{p_1}, \dots, \sqrt[\ell]{p_k})$$

$$\text{ou } \text{ram}(L/\mathbb{Q}) = \{p_1, \dots, p_k\}$$

$$\text{degré: } (\ell-1)(\ell^N-1)(\ell^{2k})$$

$$\text{ou } \ell^n = |G|.$$

Lemme standard:

Si F/\mathbb{Q} est une extension finie,

il existe une infinité de nombres

premiers totalement décomposés dans F .

(Tout sous-ensemble de densité 1 contient un tel nombre premier)

Si F/\mathbb{Q} Galoisienne: densité de tels $q = \frac{1}{[F:\mathbb{Q}]}$.

Se déduit du théorème de Chebotarev.

Démonstration plus élémentaire:

Supposons F/\mathbb{Q} Galoisienne.

Soit $F = \mathbb{Q}(x)$, et soit f le polynôme minimal de x . On peut supposer que

$f \in \mathbb{Z}[x]$. Soit Δ le discriminant

de f . Si $q \nmid \Delta$ et si f a

une racine dans \mathbb{F}_q , alors q est

totalement décomposé. S'il n'y avait

qu'un nombre fini de tels q (i.e.

ramifié ou totalement décomposé), disons

$\{p_1, \dots, p_n\}$, alors on aurait

$$f(\alpha) = \pm p_1^{m_1} \dots p_n^{m_n} \quad \text{pour tout } \alpha \in \mathbb{Z}.$$

Le nombre des valeurs distinctes de

f sur $\{1, \dots, N\}$ est au moins $\frac{1}{\deg f} N$.

On aurait donc

$$\frac{1}{d} N \leq (\log N)^*$$

contradiction.

Remarquons que l'on obtient ainsi

(pour $X^n - 1$) une preuve élémentaire

du thm de la progression arithmétique

de Dirichlet, pour les $p \equiv 1 \pmod{n}$.

Soit q un nombre premier totalement décomposé dans $L(\sqrt[q]{p_1}, \sqrt[q]{p_2}, \dots, \sqrt[q]{p_k})$.

Alors il existe un homomorphisme surjectif

$$\chi: (\mathbb{Z}/q\mathbb{Z})^\times \rightarrow C_q$$

(car $q \equiv 1 \pmod{q}$)

Mais $(\mathbb{Z}/q\mathbb{Z})^\times \cong \text{Gal}(\mathbb{Q}(\sqrt[q]{1})/\mathbb{Q})$.

Donc χ définit une extension E/\mathbb{Q} , unique extension cyclique de \mathbb{Q} de degré q ramifiée seulement en q .

Soit $\tilde{L} = LE$. Alors

$$\text{Gal}(\tilde{L}/\mathbb{Q}) = \tilde{G} = G \times C_q.$$

$$\text{ram}(\tilde{L}/\mathbb{Q}) = \text{ram}(L/\mathbb{Q}) \cup \{q\}.$$

Vérifions (S_N) pour \tilde{L} :

Si $p \in \text{ram}(L/\mathbb{Q})$, on a $p \equiv 1 \pmod{q}$.

$$\tilde{D}_p = D_p \times 1 \quad \text{car } p \text{ est décomposé}$$

$$\tilde{I}_p = I_p \times 1 \quad \text{dans } E/\mathbb{Q}.$$

Frob_p dans $E = \chi(p) \in C_q$

$\chi(p) = 1$ par construction (image de p dans \mathbb{F}_q puissance q ième).

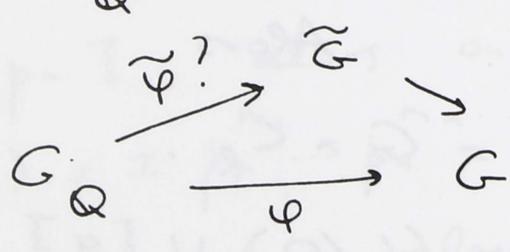
- Condition pour q : $q \equiv 1 \pmod{l^N}$
 $\tilde{D}_q = 1 \times C_l$ car q est tot. de/c. dans L/\mathbb{Q} .
 $\tilde{I}_q = 1 \times C_l$

2ème cas :

L'extension
 $1 \rightarrow C_l \rightarrow \tilde{G} \rightarrow G \rightarrow 1$ (*)
 est non triviale.

Problème de plougement. (*)
 définit $e \in H^2(G, C_l)$.

Soit $G_{\mathbb{Q}} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.



$\tilde{\varphi}$ existe \iff nullité de $\varphi^*(e) \in H^2(G_{\mathbb{Q}}, C_l)$

$$\varphi^*: H^2(G, C_l) \rightarrow H^2(G_{\mathbb{Q}}, C_l)$$

S: $\varphi^* e = 0$, $\tilde{\varphi}$ existe et est surjectif
 (car l'extension est non scindée)

$$H^i(G_K, \mathbb{C}) =: H^i(K, \mathbb{C})$$

(K corps, $G_K = \text{Gal}(\bar{K}/K)$)
 car $K = \mathbb{C}$

Théorème :

Soit K un corps de nombres, et soit C un groupe cyclique d'ordre premier l .

Alors l'homomorphisme

$$H^2(K, C) \rightarrow \prod_{\substack{v \text{ place} \\ \text{de } K}} H^2(K_v, C)$$

est injectif.

Idee de la démonstration:

Soit $K' = K(\sqrt[l]{1})$

\downarrow
 K

ext. de degré
premier à l

$H^2(K, C) \rightarrow H^2(K', C)$ est injectif.

Il suffit donc de démontrer le théorème pour K' , i.e. on peut supposer $\mu_l \subset K$.

$C = \mu_l$. $H^2(K, \mu_l) = \text{Br}_l(K)$.

Mais on sait que

$$\text{Br}_l(K) \rightarrow \prod_v \text{Br}_l(K_v)$$

est injective.

En fait, $\text{Br}(K) \rightarrow \prod_v \text{Br}(K_v)$

est injective.

Theorème de Brauer - Hasse - Noether (?)

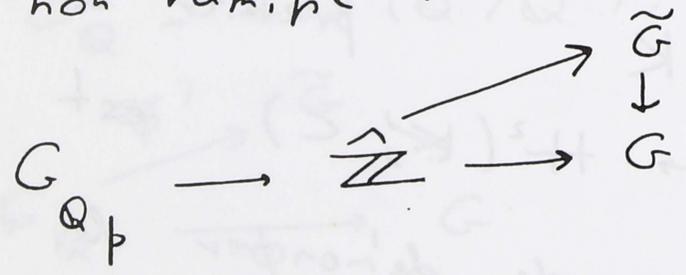
Il en existe plusieurs démonstrations.

(voir par ex. Weil : dem. analytique, utilise fct zeta).

L'énoncé est faux pour C_8 !
mais vrai pour C_4 , et C_N , N impair.

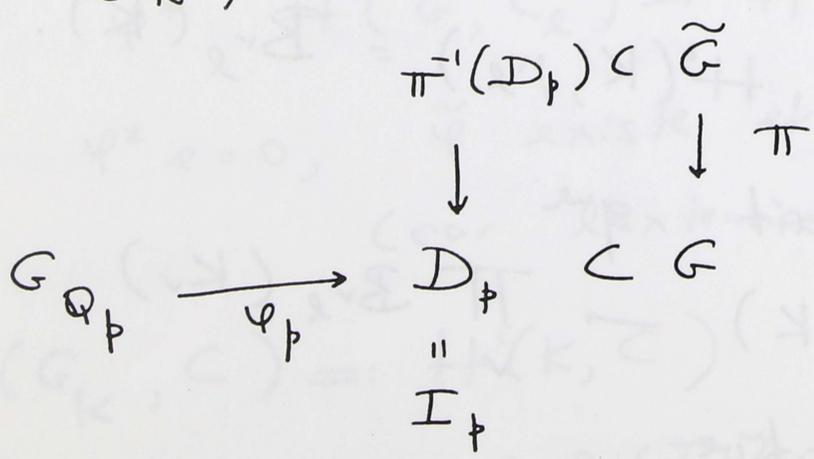
A vérifier: l'obstruction cohomologique $\psi^* e$ est nulle en toute place p de \mathbb{Q}

a) p non ramifiée: évident



b.) p ramifiée:

$(S_N) \Rightarrow$ obstruction nulle.



ramification modérée car $(p, l) = 1$

puisque $p = 1 \ (l^N)$, $N \geq 1$.

Donc $I_p = D_p$ est cyclique.

$\pi^{-1}(D_p)$ est une extension centrale d'un groupe cyclique. Donc $\pi^{-1}(D_p)$ est abélien. Son exposant divise 2^N .

\mathbb{Q}_p contient μ_{2^N} (car $f \equiv 1 \pmod{2^N}$).

Lemme :

Soit K un corps, $\mu^n \subset K$, $(n, \text{car } K) = 1$.

Soit $1 \rightarrow C \rightarrow A \rightarrow B \rightarrow 1$

une suite exacte de groupes abéliens d'exposants divisant n . Alors tout homomorphisme $G_K \rightarrow B$ se relève en $G_K \rightarrow A$.

Kummer :

$$\text{Hom}(G_K, \mathbb{Z}/n\mathbb{Z}) \cong K^*/K^{*n}$$

$$\text{Hom}(G_K, A) = (K^*/K^{*n}) \otimes A$$

2.1 Problème de plongement est résoluble. Une extension \tilde{L}/\mathbb{Q} à groupe de Galois \tilde{G} existe.

2.2. Modifier \tilde{L} pour que $\text{ram}(\tilde{L}/\mathbb{Q}) = \text{ram}(L/\mathbb{Q})$

2.3. ——— $\text{ram}(\tilde{L}/\mathbb{Q}) = \text{ram}(L/\mathbb{Q}) \cup \{q\}$
avec propriété (SN).

Lemme:

Pour tout p premier, soit

$$\varepsilon_p : G_{\mathbb{Q}_p} \rightarrow C \quad (\text{abélien fini})$$

Supposons que $\varepsilon_p(\text{inerte en } p) = 1$ pour

presque tout p . Alors il existe

$$\varepsilon : G_{\mathbb{Q}} \rightarrow C \quad \text{tel que pour tout } p,$$

$$\varepsilon|_{G_{\mathbb{Q}_p}} = \varepsilon_p \quad \text{sur le groupe}$$

d'inertie en p . Un tel ε est

unique.

C cyclique d'ordre n .

$$(\mathbb{Z}/N\mathbb{Z})^* \xrightarrow{\varepsilon} C$$

N bien choisi

$$p_1, \dots, p_k \neq q. \quad \varepsilon(\text{inerte en } p) \neq 1$$

$$p_i^{n_i} \text{ conducteur de } \varepsilon(\text{---})$$

$$N = \prod p_i^{n_i}, \quad \prod (\mathbb{Z}/p_i^{n_i}\mathbb{Z})^*$$

$$I_{\mathbb{Q}} = \mathbb{Q}^* \times \left(\prod \mathbb{Z}_p^* \times \mathbb{R}_+^* \right)$$

Proposition:

Soit $1 \rightarrow C \rightarrow \tilde{\Phi} \rightarrow \Phi \rightarrow 1$
 une suite exacte de groupes finis,
 $C \subset$ centre de $\tilde{\Phi}$.

Soit $\psi: G_{\mathbb{Q}} \rightarrow \Phi$ un homomorphisme
 relevable en un homomorphisme dans $\tilde{\Phi}$.

Soit $\tilde{\psi}_p: G_{\mathbb{Q}_p} \rightarrow \tilde{\Phi}$ relevant ψ_p .

Supposons $\tilde{\psi}_p$ non ramifié pour presque
 tout p . Alors il existe un relèvement
 $\tilde{\psi}: G_{\mathbb{Q}} \rightarrow \tilde{\Phi}$ qui coïncide avec les $\tilde{\psi}_p$
 sur l'inverse en p .

On choisit un relèvement $\Psi: G_{\mathbb{Q}} \rightarrow \tilde{\Phi}$.

Soit Ψ_p la restriction de Ψ à $G_{\mathbb{Q}_p}$.

Donc il existe un caractère $\varepsilon_p: G_{\mathbb{Q}_p} \rightarrow C$

t.q. $\Psi_p = \varepsilon_p \tilde{\psi}_p$. Par le lemme on

obtient un ε global. Alors $\tilde{\psi} = \varepsilon^{-1} \Psi$
 convient.

Conclusion de la 2^{ème} étape:

$$\begin{array}{ccc}
 & & \tilde{G} \\
 & \nearrow & \downarrow \\
 G_{\mathbb{Q}} & \longrightarrow & G
 \end{array}$$

Si $p \notin \text{ram}(L/\mathbb{Q})$, on peut relever
 $G_{\mathbb{Q}_p} \rightarrow G$ par un homomorphisme non
 ramifié. D'où relèvement global
 $\tilde{\varphi}: G_{\mathbb{Q}} \rightarrow \tilde{G}$ non ramifié si
 $p \notin \text{ram}(L/\mathbb{Q})$.

Condition de Scholz:

p ramifié, $p \equiv 1 \pmod{l^N}$ ok.

$D_p = I_p$? pas nécessairement.

$$\tilde{I}_p \subset \tilde{D}_p \subset \tilde{G}$$

$$I_p = D_p \subset G$$

Il se peut que $\tilde{I}_p = I_p$, mais

$$\tilde{I}_p \subsetneq \tilde{D}_p.$$

Il faut modifier l'extension.

La 3^{ème} étape utilisera cebotarev
 dans $L\left(\sqrt[l^N]{1}, \sqrt[l]{p_i}\right)$.

$l, N \geq 1, l \neq 2.$

$$1 \rightarrow C_l \rightarrow \tilde{G} \rightarrow G \rightarrow 1$$

G l -groupe, C_l cyclique d'ordre l

$$\tilde{G} \begin{pmatrix} \tilde{L} \\ L^{C_l} \\ G \\ K \end{pmatrix} \text{ condition } (SN)$$

On veut (SN) pour \tilde{L} , et $\text{ram}(\tilde{L}/\mathbb{Q}) = \text{ram}(L/\mathbb{Q}) \cup \{q\}$.

On peut construire un \tilde{L} avec $\text{ram}(\tilde{L}/\mathbb{Q}) = \text{ram}(L/\mathbb{Q})$

(qui ne satisfait pas a priori à la condition (SN))

3^{ème} étape: Modifier un tel \tilde{L} pour qu'il satisfasse à (SN) , et $\text{ram}(\tilde{L}/\mathbb{Q}) - \text{ram}(L/\mathbb{Q}) = \{q\}$

$$p \in \text{ram}(L/\mathbb{Q}) \quad I_p = D_p \subset G \quad \text{pour } L/\mathbb{Q}$$

Soit $S = \{p \in \text{ram}(L/\mathbb{Q}) \mid \pi^{-1}(I_p) \text{ n'est pas cyclique}\}$

$$l^{\alpha+1} \quad \pi^{-1}(I_p) \subset \tilde{G}$$

$$\begin{array}{ccc} & & \downarrow \pi \\ \text{d'ordre } l^\alpha & & I_p = D_p \subset G \end{array}$$

S: $p \in \text{ram}(L/\mathbb{Q}), p \notin S$, alors

$$\tilde{I}_p \subset \tilde{D}_p \subset \pi^{-1}(I_p) \subset \tilde{G}$$

$$\downarrow \\ I_p$$

puis que $\pi^{-1}(I_p)$ est cyclique, on doit avoir $\tilde{I}_p = \tilde{D}_p = \pi^{-1}(I_p)$.

Supposons S non vide (sinon, il n'y a rien à faire).

$$p \in S \quad \tilde{I}_p \subset \tilde{D}_p \subset \pi^{-1}(\tilde{I}_p) \subset \tilde{G}$$

$$\searrow \quad \swarrow \quad \downarrow$$

$$\quad \quad \quad I_p$$

\tilde{I}_p est cyclique (car ext. nodée)

$$\tilde{I}_p \cong I_p \quad \pi^{-1}(I_p) = C_l \times \tilde{I}_p$$

$$\text{Frob}_p \in \tilde{D}_p / \tilde{I}_p \hookrightarrow C_l$$

$$p \in S \longmapsto c_p \in C_l$$

$$c_p = 1 \iff \tilde{D}_p = \tilde{I}_p$$

$$S = \{p_1, \dots, p_k\} \quad c_{p_i} = c_i$$

On peut supposer $c_i \neq 1 \in C_l$

$$\text{Soit } c_i = c_1^{v_i} \quad 0 \leq v_i \leq l-1$$

On va prouver l'existence d'un nombre premier q ayant les propriétés suivantes:
 $q \notin \text{ram}(L/\mathbb{Q})$, $q \in \text{ens. de densité } 1$ donc'

- ① $q \equiv 1 \pmod{l^N}$
- ② q totalement décomposé dans L
- ③ q pas totalement décomposé dans $\mathbb{Q}(\sqrt[l]{1}, \sqrt[l]{p_i})$.

(4) q totalement décomposé dans
 $\mathbb{Q}(\sqrt[l]{1}, \sqrt[l]{p_i/p_i^{v_i}})$.

C'est ici que $l \neq 2$ est important !

$$\mathbb{Q}(\sqrt[l^N]{1}) = \mathbb{Q}(\sqrt[l]{1}) \cdot F$$

F cyclique de degré l^{N-1} .

On demande donc décomposition totale de q de

$$\mathbb{Q}(\sqrt[l^N]{1}) = \mathbb{Q}(\sqrt[l]{1}) \cdot F$$

et dans L

comportement prescrit dans

$$\mathbb{Q}(\sqrt[l]{1}, \sqrt[l]{p_1}, \dots, \sqrt[l]{p_k})$$

Lemme: Les corps F, L et $\mathbb{Q}(\sqrt[l]{1}, \sqrt[l]{p_i}, p_i \in S)$
sont linéairement disjoints.

(a) F et L sont disjoints (F ramifié
seulement en l , L pas ram. en l)

$F.L$ ext. gal. de groupe de Galois
en l -groupe.

(b) $F.L$ est lin. disj. de $\mathbb{Q}(\sqrt[l]{1}, \sqrt[l]{p}, p \in S)$, car
Toute extension galoisienne de \mathbb{Q} de
degré une puissance de l est lin.
disjointe de $\mathbb{Q}(\sqrt[l]{1}, \sqrt[l]{p}, p \in S)$

(b) \Leftrightarrow (c) :

(c) Le groupe de Galois de $H = \mathbb{Q}(\sqrt[l]{1}, \sqrt[l]{p}, p \in S)$ n'a aucun quotient d'ordre une puissance de l , à part $l^0 = 1$ (ceci est faux si $l = 2$)

Gal(H)
 \downarrow groupe de Galois (l, \dots, l)
 $\mathbb{Q}(\sqrt[l]{1})$ l fois
 $\downarrow \mathbb{F}_l^*$
 \mathbb{Q}

Gal(H/\mathbb{Q}) est produit direct de \mathbb{F}_l^*

et de Gal($H/\mathbb{Q}(\sqrt[l]{1})$): type (l, \dots, l)

action de \mathbb{F}_l^* sur Gal($H/\mathbb{Q}(\sqrt[l]{1})$)
 est par homothétie.

$\mathbb{F}_l^* \neq \{1\}$ si $l \neq 2$.

Donc Gal(H/\mathbb{Q}) n'a aucun quotient d'ordre l . D'où (c).

Indép. des corps $F, L, H = \mathbb{Q}(\sqrt[l]{1}, \sqrt[l]{p}, p \in S)$

q totalement décomposé dans F et L

q totalement décomposé dans $\mathbb{Q}(\sqrt[l]{1})$.

$H/\mathbb{Q}(\sqrt[l]{1}) =$ composé de $\mathbb{Q}(\sqrt[l]{1}, \sqrt[l]{p_i})$

et de $\mathbb{Q}(\sqrt[l]{1}, \sqrt[l]{p_i/p_i^{v_i}})$ $i \geq 2$

Les q ainsi obtenus forment un ensemble de densité > 0 .

Soit q satisfaisant aux 4 conditions (1), ..., (4).

Il existe un caractère surjectif

$$\varepsilon: G_{\mathbb{Q}} \rightarrow C_{\ell}$$

ramifié seulement en q .

correspond à $\mathbb{Q}(\sqrt[\ell]{1})$
 \downarrow
 \vdots
 \downarrow cyclique de degré ℓ
 \mathbb{Q}

On peut parler de $\varepsilon(\text{Frob } p_i)$, notés

$$\varepsilon(p_1), \dots, \varepsilon(p_k) \in C_{\ell}.$$

$$\text{On a } \begin{cases} \varepsilon(p_i) = \varepsilon(p_i)^{\nu_i} & i = 1, \dots, k \\ \varepsilon(p_1) \neq 1 \end{cases}$$

(4) $\Leftrightarrow p_i / p_i^{\nu_i}$ est une puissance ℓ -ième mod q .

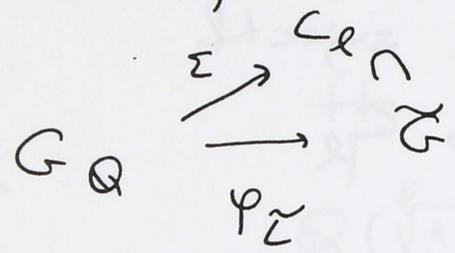
D'où la 1^{ère} formule

(3) $\Leftrightarrow p_1$ n'est pas puissance ℓ -ième mod q

$$\begin{array}{c} \uparrow \downarrow \\ \varepsilon(p_1) \neq 1 \end{array}$$

On peut remplacer ε par une puissance (d'ordre premier à l) on peut supposer $\varepsilon(p_i) = c_i \in \mathbb{C}_l \Rightarrow \varepsilon(p_i) = c_i$ pour tout i

On "tord" par ε^{-1}



$$\varphi_{\tilde{Z}} \varepsilon^{-1} : G_{\mathbb{Q}} \rightarrow \tilde{G}$$

Condition (S_N) est satisfaite

Intermède sur groupes finis

Sous-groupe de Frattini d'un groupe

fini :

G groupe fini, le slg de Frattini de G est $\phi(G) = \bigcap_{\substack{H \\ \text{maximal}}} H$ (maximal ds G : parmi les slg propres de G)

Si H est un slg de G tel que

$$H \cdot \phi(G) = G, \text{ alors } H = G.$$

Sinon, il existerait $M \subset G$, maximal, avec $H \subset M$, d'où $H \cdot \phi(G) \subset M$ - contradiction



Pour qu'une partie S de G engendre G il suffit qu'elle engendre $G/\phi(G)$.

S: G est un p -groupe, les H max. sont les s/g (normaux) d'indice p et $G/\phi(G)$ = plus grand quotient de G qui soit abélien élémentaire de type (p, \dots, p) .

(dual de $H^1(G, \mathbb{Z}/p\mathbb{Z})$)

$$\phi(G) = (G, G) G^p.$$

Exemple: Si G est un groupe simple, $\phi(G) = 1$.

On s'intéressera à un cas intermédiaire: groupes résolubles.

Théorème (Ore, cf. livre de Huppert, p 68 vol I)

Soit G un groupe fini, et soit H un s/g distingué de G , avec

$$G > H > \phi(G)$$

et $H/\phi(G)$ nilpotent.

Alors H est nilpotent.

Corollaire: $\phi(G)$ est nilpotent.

C'est un exercice sur les groupes de Sylow.

G nilpotent (\Leftrightarrow) pour tout p , G a la qu'un seul p s/g de Sylow. (i.e. tout p -groupe de Sylow de G est distingué).



(\Leftarrow) G est un produit direct de p -groupes.

S_p p -Sylow de G , distingué
 $p_1 \neq p_2$, S_{p_1}, S_{p_2} s/g distingués
 $S_{p_1} \cap S_{p_2} = \{1\}$.

\Downarrow
 commutent entre eux.

$\prod_p S_p \rightarrow G$ ou compare les ordres
 d'où \cong .

Il faut prouver que, si $S \subset H$ est un p -Sylow de H , alors S est distingué dans H .

L'image de S dans $H/\phi(G)$ est un p -Sylow de $H/\phi(G)$, donc est l'unique s/g de Sylow de $H/\phi(G)$.

On en conclut que $S \cdot \phi(G)$ est distingué dans G .

Si $g \in G$, $g S g^{-1}$ est contenu dans $S \phi(G) \subset H$
 c'est un p -Sylow de $S \phi(G)$.

Par le thm de Sylow, il existe $t \in S \phi(G)$ avec $t g S g^{-1} t^{-1} = S$. Autrement dit,
 $t g \in N_G(S)$. D'où $G = S \phi(G) N_G(S)$
 $g = t^{-1} t g = \phi(G) N_G(S)$

$\Rightarrow N_G(S) = G$

Théorème (Ore) : Soit G un groupe
résoluble d'ordre $|G| > 1$. Alors G est
isomorphe à un quotient d'un produit
semi-direct $N \rtimes R$ d'un groupe résoluble
 R avec $|R| < |G|$, et N nilpotent.
(N distingué sur lequel R opère)

$G > \phi(G)$, $G/\phi(G)$ résoluble $\neq \{1\}$

S: $|G| > 1$, alors $G \neq \phi(G)$.

Donc contient un slg abélien A normal,
caractéristique, $\neq \{1\}$. (prendre l'avant-
dernier dérivé).

Soit $N \subset G$ avec $N > \phi(G)$,

$N/\phi(G) = A$. Par le thm précédent
 N est nilpotent et distingué de G .

N n'est pas contenu dans $\phi(G)$.

Il existe un slg maximal R de G
tel que $N \not\subset R$.

On a un homomorphisme

$$N \rtimes R \longrightarrow G$$

il est surjectif, car son image $N \cdot R$
est soit R , soit G . R est exclu
car $N \not\subset R$.

E'noncé (Isharov) :

Soit L/K une extension galoisienne finie de corps de nombres de groupe de Galois G , et soit N un groupe nilpotent sur lequel opère G .

Soit $\tilde{G} = N \rtimes G$

$$(*) \quad 1 \rightarrow N \rightarrow \tilde{G} \rightarrow G \rightarrow 1 \quad \text{scindée}$$

Alors le problème de plongement pour $(*)$ est résoluble. Autrement dit,

il existe $\tilde{L} \supset L$, \tilde{L} Galoisienne sur K ,

$$\text{Gal}(\tilde{L}/K) = \tilde{G}.$$

$$\tilde{L}$$

$$| \text{nilpotent } N$$

$$L$$

$$K$$

Théorème (Shafarevitch)

L'énoncé précédent entraîne que tout groupe fini résoluble G est groupe de Galois d'une extension L/K , où K est un corps de nombres fixé.

Démonstration par récurrence sur $|G|$.

Si $|G| = 1$, par le théorème précédent

$G \cong \text{qtr de } N \rtimes \mathbb{Z}$, \mathbb{Z} résoluble d'ordre $< |G|$.

D'où L_0/K Galoisienne de groupe
de Galois R .

E'noncé \Rightarrow il existe $L_1 \supset L_0 \supset K$
avec $\text{Gal}(L_1/K) \cong N \rtimes R$

Par th. de Galois, G est groupe de
Galois de L/K , avec $L \subset L_1$.

Preuve de l'énoncé dans le cas N abélien.

Si N est quotient d'un N' "réalisable"
alors N est réalisable. (car
$$\begin{array}{c} N' \rtimes G \\ \downarrow \text{sur} \\ N \rtimes G \end{array}$$
).

$$G' \begin{array}{c} L' \\ | \\ L \\ | \\ K \end{array} \quad \begin{array}{l} N \text{ n.potent} \\ G' \xrightarrow{\text{sur}} G \\ N \rtimes G' \xrightarrow{\text{sur}} N \rtimes G \end{array}$$

On peut supposer $N \cong$ somme directe de
modules induits $\mathbb{Z}/n\mathbb{Z}[G]$, pour un
 n fixe! (le copies)

On peut supposer que $L \supset \mathbb{F}_n$

$$\begin{array}{c} \tilde{L} \\ | \\ \mathbb{Z} \end{array} \begin{array}{l} \text{le copies de } \mathbb{Z}/n\mathbb{Z}[G] \end{array}$$

$$\begin{array}{c} L \\ | \\ K \end{array} \quad \begin{array}{l} \text{Soit } p \text{ totalement décomposé} \\ \text{dans } L/\mathbb{Q}, \text{ premier à } n. \end{array}$$

p_1, \dots, p_k tot. de'c. ...

Soient v_1, \dots, v_k places de L au-dessus de p_1, \dots, p_k .

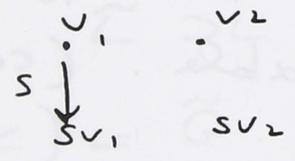
$sv_i, s \in G, i \in [1, k]$ sont distinctes.

On choisit $x_1, \dots, x_k \in L^* \text{ t.q.}$

$$(sv_i)(x_j) = 0$$

sauf si $s = 1$ et $i = j$, auquel cas

$$sv_i(x_j) = 1.$$



$$\tilde{L} = L(\sqrt[n]{sx_1}, \dots, \sqrt[n]{sx_k}, s \in G)$$

répond à la question.

$k |G|$ éléments, donnant extensions disjointes. \tilde{L} est Galoisienne sur K .

$$\text{Gal}(\tilde{L}/L) = k \text{ copies de } \mathbb{Z}/n\mathbb{Z}[G].$$

$$1 \rightarrow N \rightarrow \text{Gal}(\tilde{L}/K) \rightarrow G \rightarrow 1$$

Donc produit semi-direct.

Remarque: dans le cas non abélien
 on suppose N p -groupe, avec action de G
 $N/\phi(N)$ de type (p, \dots, p) avec action de G
 quotient d'une somme de $\mathbb{Z}/p\mathbb{Z}[G]$

On choisit les $x_i \in N$ engendrant N

$$y_{i,s} = s x_i, \quad s \in G, \quad 1 \leq i \leq k.$$

L : groupe libre de base $Y_{i,s}$.

Action de G sur L par permutation des indices s .

On choisit un exposant p^M et un indice r , on divise L par le r ième terme de la suite centrale descendante, et par les puissances p^M ièmes : $L_{r,M}$.

G opère sur $L_{r,M}$.

N est un quotient de $L_{r,M}$ si r, M assez grands.

Il suffit donc de démontrer l'énoncé pour $L_{r,M}$.

Suite du cours :

30/1 rationalité de certaines variétés

6/2 Colliot-Thélène : non rationalité de certaines variétés

13/2 — Théorème d'irréductibilité de Hébert.

Exemple :

Variété stablement rationnelle mais pas rationnelle

30/1/89

K corps, $\text{car}(K) = 0$, \bar{K} clôture alg.

V var. alg. / K irréductible, réduite

$K(V)$: corps de fonctions

S : K est algébriquement fermée dans $K(V)$



V absolument irréductible



V/\bar{K} irréductible

$\cancel{V(K)} K(V)/K$ est dite régulière

L' gal

L'

L' finie

L régulière

K

L' gal : clôture alg. de L'/K

\sum

régulière

L' gal / K n'est pas en général une extension régulière.

Par exemple:

$$\mathbb{Q}(\mu_3, \sqrt[3]{T})$$

$$\uparrow$$
$$\mathbb{Q}(\sqrt[3]{T})$$

$$\uparrow$$
$$\mathbb{Q}(T)$$

$$\uparrow$$
$$\mathbb{Q}$$

V est dite K -rationnelle si $K(V)$ est une extension transcendante pure de K .

$$\dim V = n \quad K(V) \cong K(T_1, \dots, T_n)$$

V birat. isom. / $K \cong \mathbb{P}^n$, ou \mathbb{A}^n .

\bar{K} -rationnelle : V/\bar{K} est rationnelle.
(on dit aussi "rationnelle").

Une conique sans point rationnel est rationnelle / \bar{K} mais pas sur K .

K -unirationnelle si $K(V)$ est contenu dans une extension transcendante pure de K (qui peut être choisie finie sur $K(V)$)

\mathbb{P}^n appl. rat.



quitte à se restreindre à des ouverts, c'est un isom.

$\mathbb{P}^n \rightarrow$ géométriquement surjectif

quitte à se restreindre à ouverts conv., morphisme fini

\bar{K} -unirationnelle est aussi dite "unirationnelle"

V est stablement K -rationnelle \Leftrightarrow

$\exists n$ t.q. $\mathbb{P}^n \times V$ soit K -rationnelle

Exemple : $y^2 + z^2 = x^3 - 2$ sur \mathbb{Q}

variété stablement rationnelle mais pas rationnelle.

E. Noether

G fini $\hookrightarrow S_n$ opère sur $K[x_1, \dots, x_n]$,
 $K(x_1, \dots, x_n)$. Soit $L = K(x_1, \dots, x_n)^G$.

$Y = \mathbb{A}^n$ G opère sur Y

\downarrow
 $Y/G = X$ sur des ouverts convenables
c'est un rev. gal. étale

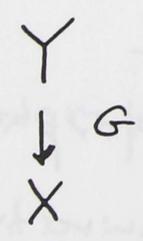
$K(X) = L$.

Y est K -rationnelle

X est K -unirationnelle.

Est-ce que X est K -rationnelle?
(stabilité K -rationnelle suffirait pour
entraîner l'existence d'ext. gal. de \mathbb{Q}
de groupe de Galois G).

"Lemme sans nom" :



$X = Y/G$.

K Y
 G opère sur Y

on peut supposer que
 G opère librement, car
on peut se restreindre à
un ouvert.

Revêtement étale, galoisienne

$\rho : G \rightarrow GL(V)$

V espace vect. / K
de dim finie n

On obtient fibre vectoriel \mathcal{V} sur X :

$$(V \times Y)/G = \mathcal{V}$$

$$\downarrow$$

$$X$$

est un fibré vectoriel localement trivial
Descente des faisceaux.

$$\sigma_Y \otimes V$$

$$\downarrow$$

$$Y$$

donne faisceau localement
trivial sur X .

(On supposera les variétés quasi-projectives
pour que les quotients par groupes finis
existent).

\mathcal{V} est birationnellement isomorphe à $V \times X$.

Lemme:

Le quotient de $V \times Y$ par G est birat.
isom. à $V \times (Y/G)$.

Proposition:

Soient V_1, V_2 deux G -modules ($K[G]$ -modules)
de dimension finie sur K , avec V_2 fidèle.

Alors $(V_1 \times V_2)/G$ birat. isom. à $V_1 \times (V_2/G)$

$$Y = V_2 - \bigcup_{\substack{g \in G \\ g \neq 1}} \text{Ker}(g^{-1})$$

Corollaire 1 :

S: V_2/G est K -rationnelle, il en est de même de V/G , où $V_3 = V_1 \oplus V_2$.

Corollaire 2 :

S: V/G est stablement K -rationnelle pour un G -module fidèle V , il en est de même pour les autres modules fidèles.

Exemples

$G = \mathbb{H}_8$: groupe des quaternions (d'ordre 8).

A montrer: rationalité du corps des invariants.

Ici $K = \mathbb{Q}$ (mais certainement vrai sur $\mathbb{H} K$)

$$1 \rightarrow (2) \rightarrow G \rightarrow (2,2) \rightarrow 1$$

$$\mathbb{Q}[G] = \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{H}$$

\mathbb{H} : corps des quaternions usuels / \mathbb{Q}

S: l'on veut une repr. fidèle, il faut qu'il y ait au moins une copie de \mathbb{H} .

Représentation de d^{ox} de G donnée par $\mathbb{H} \otimes \mathbb{Q}$

$$G \hookrightarrow \mathbb{H}_{\mathbb{Q}}^* \quad V = \mathbb{H} \otimes \mathbb{Q}, \quad V/G$$

On remplace V par un ouvert: $\mathbb{H}_{\mathbb{Q}}^*$.

Dans \mathbb{H} (vu comme variété alg. / \mathbb{Q})

on regarde l'ouvert U défini par $Nrd \neq 0$.

$$U \simeq G_m / \mathbb{H} \otimes \mathbb{Q} \quad \mathbb{H}_{\mathbb{Q}}^*, \text{ vu comme groupe algébrique / } \mathbb{Q}.$$

Espace homogène $\mathbb{H}^*_\mathbb{Q}/G = X$

variété \mathbb{Q} -rationnelle ??

$-1 \in G. \quad \mathbb{H}^*_\mathbb{Q} / \{\pm 1\} = ?$

$\cong SO_3 \times \mathbb{G}_m \quad x^2 + y^2 + z^2$

$q \in \mathbb{H}^*_\mathbb{Q} \mapsto (r_q, \text{Nrd}(q))$
 $\in SO_3 \quad \in \mathbb{G}_m$

quat. purs $(xi + yj + zk) = \zeta$, $\zeta \mapsto q \zeta q^{-1}$
est une rotation $r_q \in SO_3$.

Noyau est $\{\pm 1\}$: $\text{Nrd}(q) = 1$

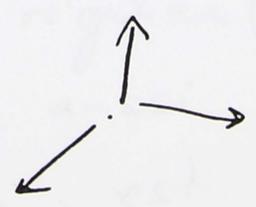
$r_q = 1 \Rightarrow q \in \text{centre}$

$\Rightarrow \lambda^2 = 1 \Rightarrow \lambda = \pm 1$.

$D = \mathbb{Q} / \{\pm 1\} \quad (2, 2)$

$X \cong \mathbb{A}^1 \times (SO_3 / D)$

birat.



D : s/g de SO_3 préservant Ox, Oy et Oz .

$(x, y, z) \mapsto (\pm x, \pm y, \pm z)$
avec 0 ou 2 signes -.

Drapeau: $(0_x, 0_{xy})$

(ou drapeau complet: $(0, 0_x, 0_{xy}, 0_{xyz})$)

Fixateur de ce drapeau dans SO_3 est D .

Drap: variété des drapeaux

$$SO_3/D \rightarrow \underline{\text{Drap}} \quad \dim 3$$

birat. isom.

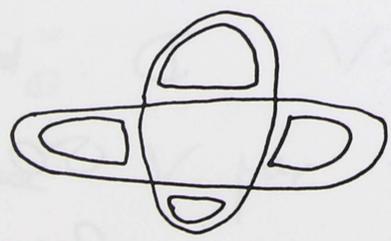
$(T$ lisse, convexe, $\dim n$

G de $\dim n$ opère sur T , $t \in T$

$$\text{Fix}_G t = D \quad G/D \rightarrow T \quad \text{isom. birat} \\ (\text{car} = 0!)$$

Drap est rationnelle.

Ref: Quaternion extensions, C. Jensen, N. Yui
Alg. Geom. and Comm. Alg. 1987, 155-182



$$(2x^2 + y^2 - 3)(2y^2 + x^2 - 3) + \epsilon = 0$$

$$0 < \epsilon < 0,72$$

G

K

G a la propr. $\text{Gal}_{K(T)}$

s'il existe une ext. gal. $L/K(T)$,

de groupe G, qui soit régulière sur K

L

Y

courbe abs. irréd.

|

↓

lisse, projective,

K(T)

 \mathbb{P}^1

avec action fidèle
de G,

$Y/G \simeq \mathbb{P}^1$.

Théorème d'irréductibilité de Hilbert

⇓

$\text{Gal}_{K(T)}$, où K est un corps de
nombres, entraîne l'existence d'une infinité
d'extensions galoisiennes de K à groupe G,
deux à deux disjointes.

Théorème: s'il existe une extension galoisienne

de groupe G, régulière de $K(x_1, \dots, x_n)$, $n \geq 1$,

il en existe aussi une de $K(T)$

(i.e. $\text{Gal}_{K(T)}$ est vraie)

Y

 $Y/G \simeq \mathbb{P}^n$

↓

rev. (ramifiée)

 \mathbb{P}^n

On applique le thm de Bertini:

G = grassmannienne des droites de \mathbb{P}^n

Il existe un ouvert non vide U de G tel que si $u \in U$, D_u la droite correspondante de \mathbb{P}^n , la restriction de $Y \bar{\cup} D_u$ est absolument irréductible.

On choisit ensuite $u \in U(K)$.

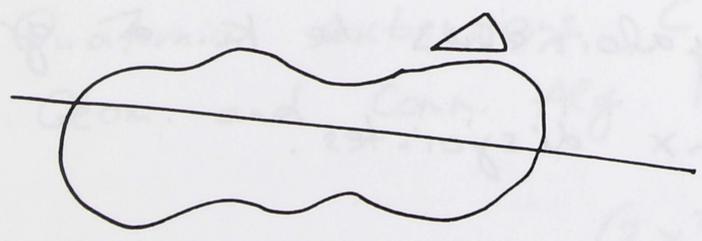
(Hartshorne, p. 179

$Y \rightarrow \mathbb{P}^n$, image de $\dim \geq 2$)
abs. irréductible.

Construction explicite de U :



Δ hypersurface de \mathbb{P}^n , lieu de ramification (réduite).



Les droites coupant transversalement Δ en des points lisses forment un ouvert U de G , dense.

U convient.

$$\pi_1(\mathbb{P}^2 - \Delta, \dots) \xrightarrow{\text{sur}} G$$

$$\uparrow$$

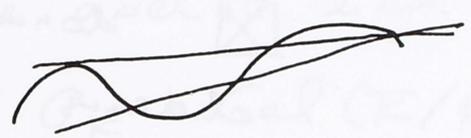
$$\pi_1(\mathbb{P}^2 - \Delta \cap \mathbb{P}^1)$$

sur ?

vrai pour
dte g n rique

aussi pour droites
voisines

Exemple :



Δ : quartique non sing
 $\subset \mathbb{P}^2$

Plan double ramifi 
le long de Δ .

$$t^2 = \phi(x, y, z)$$

ϕ :  quation de Δ .

ϕ : section du faisceau $\mathcal{O}(4)$

$$\mathcal{O}(4) = \mathcal{L} = M \otimes 2$$

$$M = \mathcal{O}(2)$$

ψ sect. de \mathcal{L} . On d crit rev.

ramifi  le long de ψ comme suit:

$$t^2 = \psi$$

/ \ sect. de \mathcal{L}

sect. de M

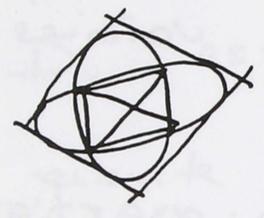
4 pts distincts \rightarrow courbe elliptique

3 " " de genre 0

28 bitangentes \rightarrow  2 coniques.

Exemple où les 28 bitangentes sont réelles:

$$(2x^2 + y^2 - 3)(2y^2 + x^2 - 3) + \varepsilon = 0$$
$$0 < \varepsilon < 0,72$$



— 4 bitangentes évidentes

⊠ donne chacune 4 bitangentes !

$$4 + 6 \cdot 4 = 28$$

(S: $\varepsilon > \frac{9}{8}$ pas de points réels)
= 2 coniques imag.

$\varepsilon = 0,72$: 2 pts de tg confondus.

Problème :

Démontrer ceci.

Exercice :

Pas de courbe de 4^e degré à au moins 5 branches.

Théorème : Un groupe abélien fini a la propriété Gal.

Utilisation des tores :

Un tore S est un K -groupe algébrique qui est \bar{K} -isom. à un produit de G_m .

Groupe des caractères de S :

$$X(S) = \hat{S} = \text{Hom}_{\bar{K}}(S, G_m)$$

Groupe abélien libre muni d'une action de $G_K = \text{Gal}(\bar{K}/K)$.

Groupe $Y(S) = \mathbb{Z}$ -dual de $X(S)$

$$= \text{Hom}_{\bar{K}}(G_m, S)$$

("slog" à un paramètre)
de S

Certains sont K -rationnels :

Tore déployé : isom. à un produit de G_m

$\iff G_K$ agit trivialement sur $X(S)$.

Tore "quasitrivial"

(de permutation,
induit)

s'il existe une \mathbb{Z} -base
de $X(S)$ stable par
l'action de G .

$\exists I$ ens. fin. où opère G

$$X(S) \simeq \mathbb{Z}^I.$$

Décomposons I en orbites de G_K

\Rightarrow décomposition de S_I en produit

Regarder le cas où G_K agit transitivement sur I , $I \neq \emptyset$.

$I \cong G_K/H$, H slg ouvert de G_K

H correspond à ext.

$L = \text{sl corps de } \bar{K} \text{ fixe par } H$
 $|$
 K

$S_I = \underline{L}^*$ un com groupe $\text{alg.}/K$

$= R_{L/K} G_m$ (Weil)

$= \prod_{L/K} G_m$ (Grothendieck)

S_I est K -rationnelle.

On a aussi: $H^1(K, S_I) = 0$

Lemme de Shapiro :

$H^1(K, S_I) = H^1(L, G_m) = 0$ (Hilbert 90)

Si S est un tore, et si A est un groupe abélien fini, et si:

$A \hookrightarrow S(K)$, le tore $S' = S/A$ est défini, et on a une suite exacte

$$0 \rightarrow A \rightarrow S \rightarrow S' \rightarrow 0$$

$$\begin{array}{c} S \\ \downarrow A \\ S' \end{array}$$

Théorème :

Pour tout groupe abélien A , on peut trouver un tore S sur \mathbb{Q} avec $A \subset S(\mathbb{Q})$ et S/A quasi-trivial.

(On pourrait aussi demander S quasi-trivial, mais peut-être pas les deux à la fois).

Corollaire :

A a la propriété Gal $_{\mathbb{T}}$.

(car S/A est une variété K -rationnelle)

Démonstration :

Suite exacte de tores \rightarrow suite exacte des caractères -

$$0 \rightarrow M \rightarrow S \rightarrow S' \rightarrow 0$$

M un G_K -module fini, $M \subset S$

$$0 \rightarrow X(S') \rightarrow X(S) \rightarrow M^\vee \rightarrow 0$$

M^\vee : dual de carrier de M

$$= \text{Hom}_{\overline{K}}(M, \overline{K}).$$

$$0 \rightarrow Y(S) \rightarrow Y(S') \rightarrow \widetilde{M} \rightarrow 0$$

$$\widetilde{M} = \text{Hom}(M^\vee, \mathbb{Q}/\mathbb{Z})$$

$$\widetilde{A} = \text{Hom}(A^\vee, \mathbb{Q}/\mathbb{Z})$$

$$H \subset G_K$$

opère triv.

$$\bigoplus \mathbb{Z}[G_K/H] \rightarrow \widetilde{A}$$

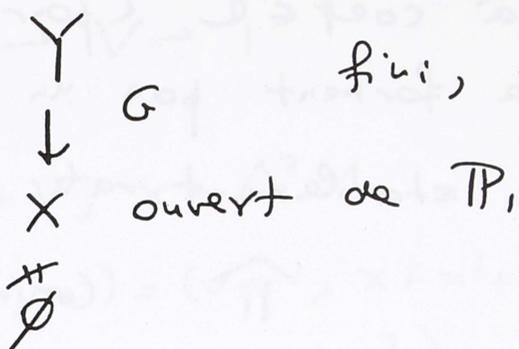
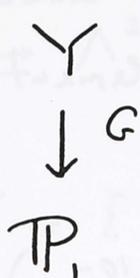
Sous-lemme: tout G_K -module de type fini est quotient d'un G_K -module de permutation.

Théorème:

Soit G un groupe fini, soit A un G -module fini, et soit $\widetilde{A} = A \rtimes G$.

S: G a la propriété $\text{Gal}_K(\tau)$, il en est de même de \widetilde{A} .

Principe de la construction :



fini, étale

/K

Si le théorème est démontré pour A, il l'est pour tout quotient de A.

On peut supposer A induit, i.e.

$$A = \bigoplus_{g \in G} gB, \quad B \text{ s/g de } A.$$

$$A = B \times \dots \times B$$



\tilde{G} : produit "en carrousel" (wreath product) de B et de G.

On choisit un tore S contenant \mathbb{R} :

$$0 \rightarrow B \rightarrow S \rightarrow S' \rightarrow 0$$

S, S' tores
S' quasi-trivial

$$A = B \times \dots \times B \subset S \times \dots \times S = \Sigma$$

(= $S^{(G)}$??)

$$\Sigma' = S' \times \dots \times S'$$

$$0 \rightarrow A \rightarrow \Sigma \rightarrow \Sigma' \rightarrow 0$$

G opère

$Y \times \Sigma$, action de $\tilde{G} = A \rtimes G$. On vérifie gén. libre et que le quotient $Y \times \Sigma / \tilde{G}$ est variété rationnelle.

G fini

fct. rat. à coef $\in \mathbb{C}$ (pour une action linéaire fidèle) ne forment pas un corps stablement pur.

V/G non stablement rat.

\Uparrow (voir Colliot-Thélène)

(Hyp) Il existe $\alpha \in H^2(G, \mathbb{Q}/\mathbb{Z})$, $\alpha \neq 0$,
qui induit 0 dans chacun des $H^2(B, \mathbb{Q}/\mathbb{Z})$
 B slg abélien bicyclique.

$Br_{nr}(V/G) \simeq \{ \text{groupe des } \alpha \text{ tués par les } \text{slg} \text{ bicycliques} \}$

Exemple (Saltman)

$$p \neq 2 \quad 1 \rightarrow U \rightarrow G \rightarrow V \rightarrow 1$$

U, V abéliens élém. de type (p, \dots, p)

extension centrale

inv. évidents:

$$1.) \quad x \in V \mapsto \tilde{x} \in G \mapsto \tilde{x}^p \in U$$

$$\text{hom.} \quad \psi_G : V \rightarrow U$$

$$\psi_G = 0 \iff x^p = 1 \text{ pour } \forall x \in G$$

$$2.) \quad x \in V, y \in V \mapsto (\tilde{x}, \tilde{y}) \in U$$

$$\tilde{x}, \tilde{y} \in G$$

$$\psi_G : \Lambda^2 V \rightarrow U$$

$$H^2(V, U) = \text{Hom}(V, U) \oplus \text{Hom}(\Lambda^2 V, U)$$

$$1 \rightarrow \Lambda^2 V \rightarrow \tilde{G} \rightarrow V \rightarrow 1 \quad \begin{cases} \varphi = 0 \\ \gamma = \text{id} \end{cases}$$

$$\tilde{G} = \left\{ (v, x) \mid v \in V, x \in \Lambda^2 V \right. \\ \left. (v, x)(v', x') = (v+v', x+x' + \frac{1}{2}v \wedge v') \right\} \\ (\text{signe ?})$$

On choisit $X \subset \Lambda^2 V$, X cyclique d'ordre p
indecomposable : il n'existe pas de $v_1, v_2 \in V$
avec $0 \neq v_1 \wedge v_2 \in X$
Il en existe si $\dim V \geq 4$ (i.e. $|V| \geq p^4$).

Posons $G = \tilde{G}/X$

$$\begin{array}{ccccccc} 1 & \rightarrow & \Lambda^2 V & \rightarrow & \tilde{G} & \rightarrow & V \rightarrow 1 \\ & & & & \downarrow & & \\ 1 & \rightarrow & \Lambda^2 V/X & \rightarrow & G = \tilde{G}/X & \rightarrow & V \rightarrow 1 \end{array}$$

$$1 \rightarrow X \rightarrow \tilde{G} \rightarrow G \rightarrow 1$$

définit $\alpha \in H^2(G, \mathbb{Z}/p\mathbb{Z}) \rightarrow H^2(G, \mathbb{Q}/\mathbb{Z})$

A voir : image de α dans $H^1(G, \mathbb{Q}/\mathbb{Z})$ est $\neq 0$.

$$0 \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Q}/\mathbb{Z} \xrightarrow{p} \mathbb{Q}/\mathbb{Z} \rightarrow 0$$

$$H^1(\quad, \mathbb{Q}/\mathbb{Z}) \rightarrow H^2(\quad) \rightarrow H^2(\quad) \rightarrow H^2(\quad) \\ \alpha \mapsto 0$$

alors $\exists \theta : G \rightarrow \mathbb{Q}/\mathbb{Z}$ dont α est l'image

extensions obtenues:

$$\begin{array}{ccccccc}
0 & \rightarrow & \mathbb{Z}/p\mathbb{Z} & \rightarrow & \mathbb{Z}/p^2\mathbb{Z} & \rightarrow & \mathbb{Z}/p\mathbb{Z} \rightarrow 0 \\
& & & & \searrow & \swarrow & \\
& & & & & & \mathbb{Q}/\mathbb{Z}
\end{array}$$

On aurait des éléments d'ordre p^2 .

α restr. aux slg bicycliques abéliens de G est 0.

Soit B bicyclique abélien dans G .

Soit B_V l'image de B dans V .

On a $\text{rg}(B_V) \leq 1$.

$x, y \in B_V$ ind. sur \mathbb{F}_p , $\chi_G(x \wedge y) = 0$

$\text{Ker } \chi_G = X$.

Mais X n'a pas d'éléments indécomposables - contradiction.

\tilde{B} = image réciproque de B dans \tilde{B} .

L'image de \tilde{B} dans V est de $\dim \leq 1$

(donc cyclique).

$\Rightarrow \tilde{B}/\text{centre}$ est cyclique $\Rightarrow \tilde{B}$ abélien.

$\Rightarrow \tilde{B}$ est de type (p, \dots, p) .

$0 \rightarrow X \rightarrow \tilde{B} \rightarrow B \rightarrow 0$ est décomposable

Donc \tilde{B} est extension scindée de B

$\Leftrightarrow \alpha|_B = 0$.

Exemple minimal obtenu ainsi:

$$|V| = p^4, \quad |V/\chi| = p^5, \quad |G| = p^9$$

($p \neq 2$ n'est pas une restriction sérieuse :
 χ_G est quadratique et non linéaire,
 mais on peut adapter la démonstration).

Fin d'une démonstration

$$K \text{ corps}, \quad \begin{array}{c} Y \\ \downarrow G \\ \mathbb{P}^1 / K \end{array}$$

A groupe abélien fini ou opère G ,

$$\tilde{G} = A \rtimes G.$$

Théorème : Si G a la propriété
 $\text{Gal}_K(\tau)$, il en est de même de \tilde{G} .

$$0 \rightarrow A \rightarrow S \rightarrow S' \rightarrow 0$$

S, S' tores / \mathbb{Q}

$S(\mathbb{Q}) \supset A$, S' quasi-trivial ("de permutation").

On a vu que l'on pouvait supposer $A = \bigoplus_{g \in G} B$
 B groupe abélien:

on écrit $A = B \oplus \dots \oplus B$ indexé par G

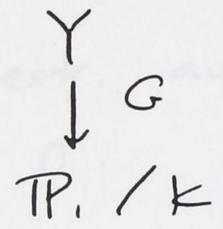
changement de notation:

$$0 \rightarrow B \rightarrow S \rightarrow S' \rightarrow 0, \quad B \subset S(\mathbb{Q})$$

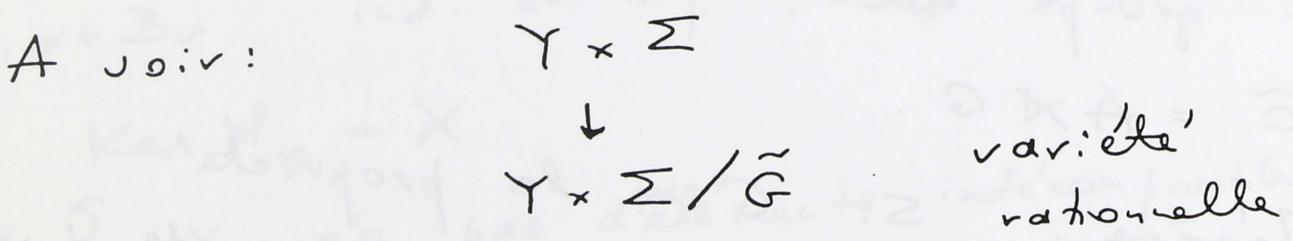
S' quasi-trivial

$$0 \rightarrow A \rightarrow \Sigma \rightarrow \Sigma' \rightarrow 0$$

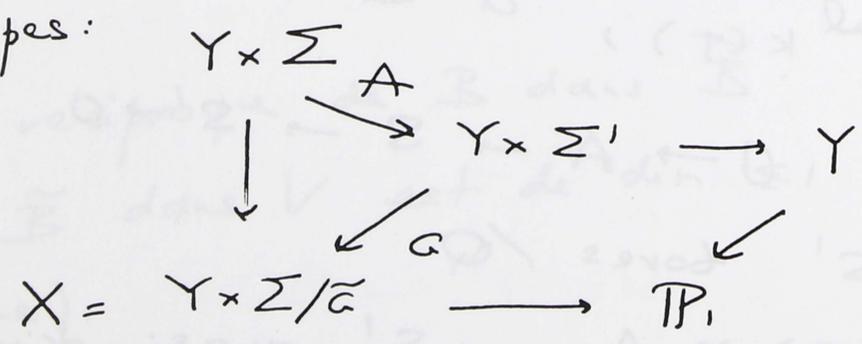
$\Sigma = S \times \dots \times S$
 $\Sigma' = S' \times \dots \times S'$



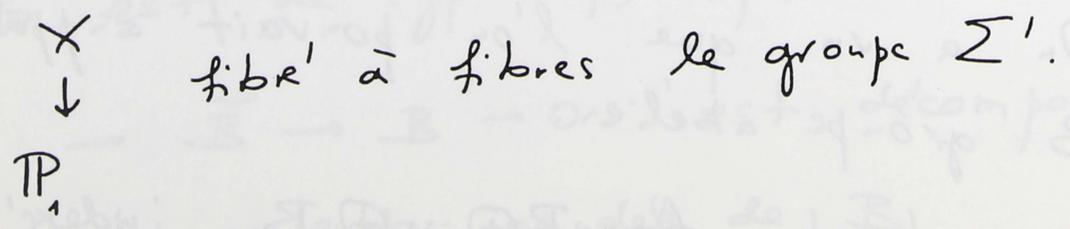
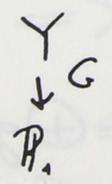
$Y \times \Sigma$ action de \tilde{G} : sur Y par $\tilde{G} \rightarrow G$
sur Σ : A agit par translations
 G en permutant les facteurs.



Plusieurs étapes :



G agit sur $\Sigma' = S' \times \dots \times S'$.



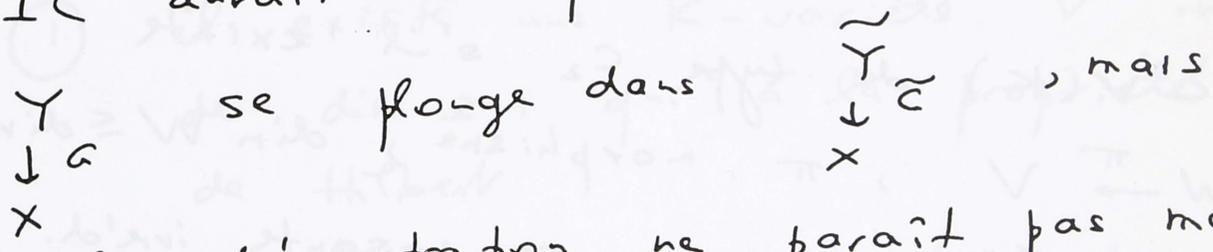
Ce fibre' X est birationnellement un produit.

Fibre a- pt. gé'n. $\rightarrow \alpha \in H^1(K(T), \Sigma')$

Σ' est quasi-trivial $\Rightarrow H^1(K(T), \Sigma') = 0$
par Hilbert 90.

Σ' est rat., $X \underset{\text{birat}}{\simeq} \mathbb{P}^1 \times \Sigma'$.

$\mathbb{C} \subset \mathbb{R}$ aurait été plus naturel de montrer que



la démonstration ne paraît pas marcher.

Théorème d'irréductibilité de Hilbert



Par exemple, $K = \mathbb{F}_q$ Y quadratique
 Y, X (courbes) abs. irréd.

$$|Y(\mathbb{F}_q)| = q + \varepsilon_Y, \quad \varepsilon_Y \leq 1 + 2g_Y(\sqrt{q}) \sim q \quad (\text{Weil})$$

$$|X(\mathbb{F}_q)| = q + \varepsilon_X \sim q$$

On a une involution de Y , $y \mapsto y'$
 y, y' ont $\tilde{\alpha}$ image ds X . Donc $|\pi Y(\mathbb{F}_q)| \sim \frac{1}{2} q$.

Définitions :

K corps de caract. 0

V var. irré'd. / K . $V(K)$: pts rat. de V

$A \subset V(K)$, A est de "type C_1 " s'il existe une sous-variété $W \subset V$, $W \text{ fermé } \neq V$ ($\dim W < \dim V$), avec $A \subset W(K)$.

Type C_1 : A non Zariski-dense.

$A \subset V(K)$ de type C_2 s'il existe $W \xrightarrow{\pi} V$, π morphisme, $\dim W \leq \dim V$

$A \subset \pi W(K)$, aucune composante irré'd.

de W ne s'applique birat. sur V (pas de section générique)

Définition :

$A \subset V(K)$ est dit mince s'il est contenu dans un ensemble de type C_2 .

Si V n'est pas absolument irréductible, alors $V(K)$ n'est pas Zariski-dense (car contenu dans l'ensemble des points où V n'est pas normal)

\mathbb{R} $x^2 + y^2 = 0$

$L \subset K(V)$, $K \subsetneq L$
fini

Si normal, $L \subset \mathcal{O}_x \forall x \in V$.

Supposons V absolument irréductible.

Définition:

On dit que V a la propriété de Hilbert si $V(K)$ n'est pas mince.

Définition:

K est Hilbertien si les propriétés équivalentes suivantes sont satisfaites si:

- ① il existe une K -variété V irréd. de $\dim \geq 1$ qui a la propriété de Hilbert
- ② \mathbb{P}^1 a la propriété de Hilbert
- ③ Toute variété K -rationnelle a la propriété de Hilbert.

② \Rightarrow ① OK ...

① \Rightarrow ② ?

La propriété de Hilbert est birationnelle:

Si V a la propr. H, toute var. birat. $\sim V$ l'a aussi.

F \mathbb{Z} -fermé, $\neq V$, $V - F$ a H.

l'union d'ensembles minces est mince.

Quitte à remplacer V par un ouvert, on peut trouver un morphisme $\varphi: V \rightarrow \text{Aff}^1$ génériquement surjectif.

$$\begin{array}{ccc}
 W_V \rightarrow W \ni w \\
 \downarrow \quad \downarrow \\
 \varphi: V \rightarrow \text{Aff}^1
 \end{array}
 \quad \text{carré cartésien}$$

Hyp: $\text{Aff}^1(K) = \pi W(K) \Rightarrow \text{contr?}$

1^{er} cas ("cas favorable") $W_V \rightarrow V$ n'a pas de section au point générique.

Il existe $x \in V(K)$ non dans l'image de $W_V(K)$.

$\varphi(x) = \pi w$ — contradiction.

On se ramène au cas favorable par une translation:

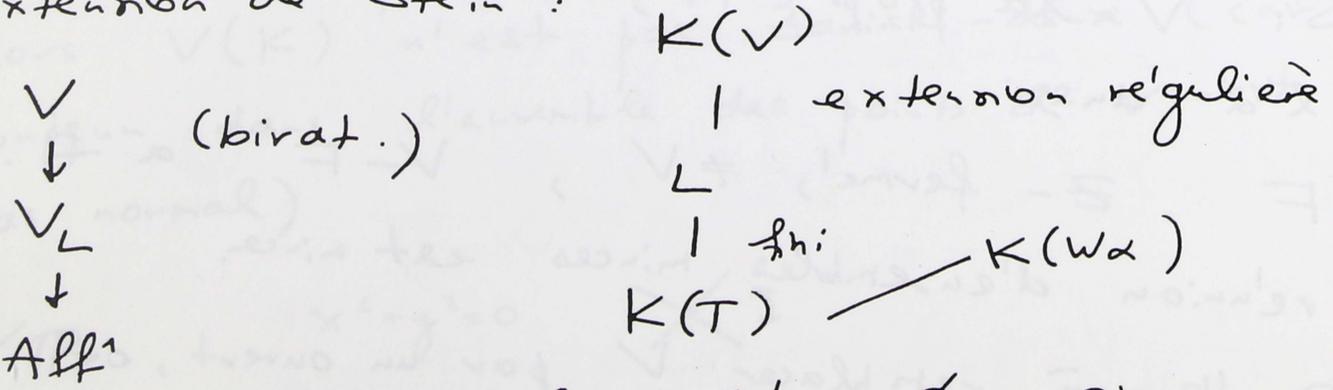
$$\begin{array}{ccc}
 & W \\
 & \downarrow \\
 V & \xrightarrow{\varphi} & \text{Aff}^1
 \end{array}$$

Il existe une translation $x \mapsto x + \lambda$, $\lambda \in K$ telle que $(\varphi + \lambda, \pi)$ soit de type favorable.

φ donne une ext.

$$\begin{array}{c}
 K(V) \\
 \downarrow \\
 K(T)
 \end{array}$$

"extension de Stein":



Si: $K(W_\alpha) \cap L = \emptyset$, OK.

$\dashrightarrow \mathbb{P}^1$

Deux extensions régulières de $K(T)$ dont les lieux de ramification sont disjoints, sauf peut-être à l'infini, sont linéairement disjointes.

Exemple : de corps hilbertiens :

Corps de nombres, certains corps de dim. infinie sur \mathbb{Q} (e.g. \mathbb{Q}^{ab} ?)

k corps quelconque de car 0, toute extension de type fini de k non algébrique est hilbertien.

k'/k finie, k hilbertien $\Rightarrow k'$ hilbertien.

Donc la propriété ci-dessus revient à montrer que $k(T)$ est hilbertien pour \forall corps de car 0.

Prouver (Bertini) que si A est une partie mince de $\text{Aff}^1(K) = K$, $K = k(T)$, alors il existe $a + bT \notin A$

(plus préc. les $a, b, a + bT \in A$ ne sont pas \mathbb{Z} -doux dans $k \times k$).

Thm d'irréductibilité de Hilbert :

Les corps de nombres sont hilbertiens.

Démonstration plus tard. On commence par donner une liste de propriétés des corps hilbertiens.

Ensembles minces

L/K ext. finite

V var. sur K

V/L var. sur L

Thm: Si $A \subset V(L)$ est mince (par rapport à V_L) alors $A \cap V(K)$ est mince par rap. à V .

Foncteur $\pi = \mathbb{R}_{L/K}$ restriction des scalaires.

V quasi-projective.

L -variétés \rightarrow K -variétés

Adjoint à droite du foncteur extension des scalaires:

$$W/L \quad \text{Hom}_L(W, V/L) = \text{Hom}_K$$

T K -variété, W L -variété

$$\text{Hom}_K(T, \mathbb{R}_{L/K} W) = \text{Hom}_L(T/L, W)$$

e.g. $T = \text{Spec } K$

$$(\mathbb{R}_{L/K} W)(K) = W(L)$$

Weil: descente à partir de πW^σ
 $\sigma: L \rightarrow \bar{K}$

W

$\downarrow \pi$

V/L

$$A \subset \pi(W(L))$$

$$\begin{array}{ccc}
 X & \longrightarrow & R_{L/K} W \\
 \downarrow & \square & \downarrow \\
 V & \xrightarrow{\Delta} & R_{L/K} V_L
 \end{array}$$

$$V(K) \longrightarrow () (K) = V(L)$$

$$A \subset \pi W(L)$$

$$A \cap V(K) \subset \pi X(K)$$

Il reste à vérifier que X n'a pas de section au pt. générique.

Se vérifie: $V \xrightarrow{\Delta} V \times \dots \times V$

rev. induits sur la diag. sont de degré $\geq m$.
 $w_1 \times \dots \times w_n$ non trivial rev. de degré m

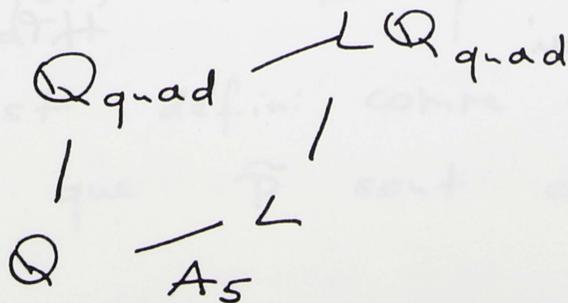
Entraîne que si V a la propriété de Hilbert sur K , V a la propriété de Hilbert sur L .

Sinon, $V(L)$ serait mince $\Rightarrow V(L) \cap V(K) = V(K)$ mince.

Cor. du Cor: K hilbertien $\Rightarrow L$ hilbertien.

Mais \Leftarrow est faux:

$\mathbb{Q}_{\text{quadr}}$ = clôture quadr. de \mathbb{Q}



saut erreur,
 $L \mathbb{Q}_{\text{quadr}}$ est hilbertien.

Thm: Soit A une partie mince de $\mathbb{P}^n(K)$. (77)

Soit $d \geq 1$, et soit Grass_n^d la Grassmannienne des d -plans de \mathbb{P}^n .

Alors il existe un \mathbb{Z} -ouvert dense

$U \subset \text{Grass}_n^d$ tel que si $u \in U(K)$,
et D_u est le d -plan correspondant,
alors $A \cap D_u(K)$ est mince dans D_u .

Corollaire:

Il existe un d -plan D rat. / K tel que
 $A \cap D(K)$ soit mince dans $D(K)$.

W
 \downarrow
 \mathbb{P}^n

$A \subset \pi(W(K))$

Bertini: il existe

U t. q. si $u \in U$

la restriction de W à D_u
n'a pas de section au point
général.

Corollaire

\mathbb{P}^n a la propriété de Hilbert $\Rightarrow \mathbb{P}^n$ a la
propriété de

\Leftarrow est aussi vrai
(déjà vu).

Hilbert

Prochaine fois: relation avec l'approximation faible. Idée de Ekedahl, complétée par Colliot-Thélène.

Approximation faible (affaiblie) \Rightarrow

Théorème d'irréductibilité de Hrbert.

Interprétation de la propriété de Hrbert
(conséquences) G groupe lin. op. sur W librement

W

\downarrow

$V = W/\mathfrak{a}$

Morphisme étale,
galoisien

On suppose W quasi-projectif.

$P \in V(K) \mapsto$ groupe de décomposition de P (de l'ini à conj. près)

On choisit un point fermé $Q \rightarrow P$

corps résiduel $K(Q)/K = K(P)$

ext. gal. de groupe $D_Q \subset G$

= groupe de décomposition.

On choisit un \bar{K} -point $\tilde{P} \rightarrow P$

$D_{\tilde{P}}$ est défini comme le s/g des $s \in G$

tels que \tilde{P} sont conjugués (Gal.) de \tilde{P} .

"Cas extrêmes":

- ① P est l'image d'un pt rat: $D = \{1\}$
- ② $D = G$, $Irr(P)$

"Cas d'irréductibilité" $Irr(P)$: la fibre de P est Spec d'un corps, ext. gal. de K à groupe G.

Thm (trivial): Supposons $|G| \geq 2$. Alors l'ensemble des $x \in V(K)$ qui n'ont pas la propriété $Irr(P)$ est mince.

Conséquence de

Thm Soit $H \subset G$, $H \neq G$. Les $P \in V(K)$ dont le groupe de déc. est conjugué de H est mince.

c'est clair, car W/H
 $\pi_H \downarrow$
 V degré $[G:H] \geq 2$

W irréduct.

$\pi_H(W/H)(K) = \{x \in V(K) \text{ dont le groupe de décomposition est contenu dans un conjugué de } H\}$.

$W/H(K)$?

$x \in W(K) \quad \sigma x \in Hx \quad \sigma \in Gal(F/K)$.

or $\pi_H(W/H)(K)$ est mince.

$Irr(P)$ donne L_P/K Galoisienne.

80

à groupe G . Une telle extension est "de type W ".

Si V a la propriété de Hilbert, il existe $x \in V(K)$ ayant la propr. $Irr(P)$.

Corollaire :

G est groupe de Galois sur K .

Plus précisément :

Théorème :

Supposons que V ait la propriété de Hilbert.

Soit K' une extension finie de K .

Alors il existe $P \in V(K)$ ayant la propriété $Irr(P)$ et tel que L_P soit lin. disjoint de K' .

Démonstration :

Soit $A \subset V(K')$ l'ensemble des $P \in V(K')$ n'ayant pas la propriété $Irr(P)$ relative à K' .

C'est un ensemble mince dans $V(K')$.

Donc $A \cap V(K)$ est mince dans $V(K)$.

Choisissons $P \in V(K)$, $P \notin A$.

Alors P a la propriété $Irr(P)$ sur K' .

Théorème d'irréductibilité de Hilbert (suite)

Erratum dans un des détails d'une preuve (si G réel sur \mathbb{R} ,
 "toe" construit = forme touchée de celui qu'on
 avait annoncé)

Interprétation en termes de polynômes des ensembles minces.

V/K K car O V abs^t irréduct.
 (quasi-proj.)

$A \subset V(K)$ mince si non Zariski-dense
 si W abs^t irred, $\dim W = \dim V$
 $\pi \downarrow$ π gén^{er}iq^t surject
 V de degré ≥ 2
 $\pi(W(K))$ mince ds $V(K)$

$K(V)$

$$P(X) = X^m + a_1 X^{m-1} + \dots + a_m$$

polyn. de degré m , $a_i \in K(V)$
 irréduct

groupe de Galois ($\subset S_m$) = G

Soit A l'ensemble des $t \in V(K)$ tels que,
 ou bien $a_i \notin \mathbb{C}_t$ pour un i , ou $P_t = \sum a_i(t) X^i$
 n'est pas irréductible sur K , ou il l'est mais de
 groupe de Galois $\neq G$.

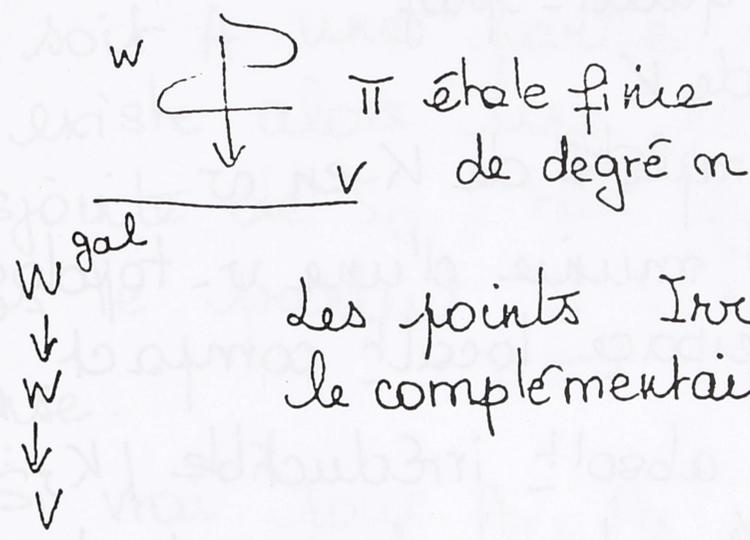
Si $t \notin A$ Tout va bien!

Théorème A est mince

Preuve: On commence par enlever de V
 les pôles des a_i et les zéros de $\Delta(P)$.

Ceci remplace V par un ouvert où les $a_i \in H^0(V, \mathcal{O}_V)$ et Δ est inversible.

On regarde $W \subset V \times \mathbb{A}^1_{\mathbb{F}} \quad W : (t, x) /$
 $0 = x^n + a_1(t)x^{n-1} + \dots + a_n(t)$



Les points $\text{Irr}(H), t \in V(k)$ sont le complémentaire d'un ens. mince.

Remarque: $K(W)$ monogène / $K(V)$ donc déf par un polynôme (à ens. z. dense).

W
 \downarrow
 V

Autrement dit mince au sens des revêtements \iff mince au sens des polynômes

On peut rendre cela tout à fait explicite

- $n=1$ il s'agit d'élever les pôles de a_i
- $n=2$ $a(t)$ non carré $x^2 - a$
- $n=3$ $\left\{ \begin{array}{l} a_i \text{ pas de pôles} \\ \Delta \text{ inv, non carré} \\ x^3 + \dots \text{ pas de solution ds } K \end{array} \right.$

\neq pour $n=4, 5 \dots$ ("Mordell-Weil" ^{cours sur}).

K corps de nombres

On va voir le rapport avec l'approximation faible (Freydahl et d'autres...).

V variété sur K , quasi-proj

Σ ens des places de K

$v \in \Sigma$ $K_v =$ complété de K en v

V/K $V(K_v)$ est munie d'une v -topologie d'espace local_h compact.

Thme 1 Si V est absol_h irréductible / K , on a $V(K_v) \neq \emptyset$ pour presque tout $v \in \Sigma$.

Corollaire Si $W \subset V$ est une ss-var_h fermée $\neq V$, alors pour tout $v \in \Sigma$, avec N_v assez grand, ~~il existe~~ $V(K_v) - W(K_v) \neq \emptyset$.

Thme 2 Soit $W \xrightarrow{\pi} V$, W absol_h irréduct. de $\dim = \dim V$, π géométr_h surjective, $\deg \pi \geq 2$. Soit $K(W)^{\text{gal}}$ la clôture galoisienne de $K(W) / K(V)$ et soit K_π la plus grande extension de K contenue dans $K(W)^{\text{gal}}$.

Soit Σ_π l'ensemble des places $v \in \Sigma$ complètement décomposées dans K_π .

Alors pour presque tout $v \in \Sigma_\pi$, l'application $W(K_v) \xrightarrow{\pi} V(K_v)$ n'est pas surjective.

Exemple $\sqrt[3]{0}$ si $K \neq \mathbb{R}$ $K_{\pi} = K(\sqrt[3]{1})$
 si v non déc. si v non décomp, $W(K_v) \cong V(K_v)$

Théorème Soient S_0 une partie finie de Σ
 et soit A une partie mince de $V(K)$.
 Il existe alors une partie finie S de Σ ,
 disjointe de S_0 , telle que l'image de A
 dans le produit $\prod_{v \in S} V(K_v)$ ne soit pas
 dense.

Preuve:
 * Si vrai pour A_1, A_2 , vrai pour $A_1 \cup A_2$

En effet: $S_0, A_1 \rightarrow S_1$ l'image de A_1 non
 dense ds $\prod_{v \in S_1} V(K_v)$

d'où $x_1 \in \prod_{v \in S_1} V(K_v)$ - adhérent de A_1

$S_0 \cup S_1, A_2 \rightarrow S_2$

d'où x_2

$(x_1, x_2) \in \prod_{v \in S_1 \cup S_2} V(K_v)$ - adhérent de $A_1 \cup A_2$.

* Si $A \subset W(K)$, $W \subset V$, $W \neq V$

par le thme 1, pour N grand, il existe
 $x \in V(K_v) - W(K_v)$. Un tel x n'est pas adhérent
 de A . Donc $S = \{v\}$ pour presque tout v
 convient.

* W avec hyp. habituelles
 \downarrow
 $A \subset \prod_{v \in S} W(K_v)$
 \downarrow
 V

En remplaçant V par un ouvert non vide, on peut supposer que π est un morphisme fini. Cela entraîne que $\pi: W(K_v) \rightarrow V(K_v)$ est propre pour la v -topologie (réf. ???).

L'image de $W(K_v)$ dans $V(K_v)$ est fermée. Par le thme 2, si N_v grand, v complètement déc, alors il existe $x \in V(K_v) - \pi W(K_v)$ donc $x \notin \text{adh de } A$.

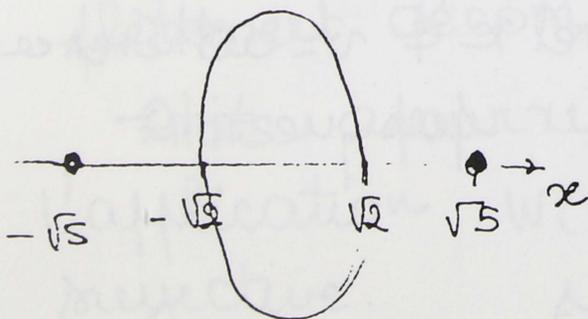
Σ_π est infini (Cebotarev).

Approximation faible

(AF_S) V S partie finie de Σ_K
 V a la propriété d'approximation vis à vis de S si $V(K)$ dense dans $\prod_{v \in S} V(K_v)$.

Théorème si V et V' sont lisses et birat^l isom., alors V possède (AF_S) si V' aussi.

Cm. ex si non lisse: $y^2 = (x^2 - 5)^2 (2 - x^2) \quad \mathbb{R}$
2 bir ég
 $y^2 = 2 - x^2$



mais les pts rationnels sont denses ds la seconde, pas ds la 1ère ($\sqrt{5}$ inapprochable!).

$$V' = V - W$$

W fermé ds V

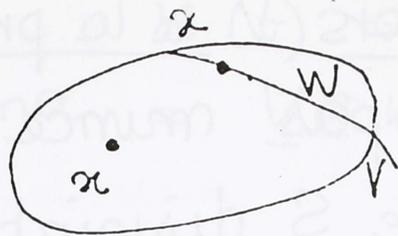
$$W \neq V$$

(86)

$$V \Rightarrow V - W$$

trivial

$$V - W \Rightarrow V$$



pour $x \notin W$
évident

$$x \in W(K_0)$$

$V(K_0) - W(K_0)$ dense
dans $V(K_0)$, à cause
de la lissité.

(local^r revient à esp affine
- ss-variété).

Usage C.T - S : si ouvert de lissité satisfait
le prop.

(AFA)

(AF_S) pour tout $S \subset \Sigma_K$.

approxim faible

(AFA) : Il existe une partie finie S_0 de Σ_K
telle que AF_S ait lieu pour tout S disjoint
de S_0 .

approx faible affaibli

Exemples 1) variété K -rationnelle satisfait (AF).
(car il suffit de le voir pour \mathbb{A}^m).

2) tore ne satisfait pas toujours à (AF)
cf chre-ex au principe de Noether (Norme = 1
dans bicyclique (2,2)).

Mais tous les tores satisfait (AFA).

par ex: $S_0 =$ places ramifiées ds L/K où L
ultramétriques

Ref: Voskresenski... (suffit celles où $G_0 \neq \text{cycl.}$) (6)

Théorème. Soit V une variété absol^t irréductible satisfaisant (AFA). Alors V a la propriété de Hilbert ($V(K)$ n'est pas munice).

Preuve: Sinon, il existe S disjoint de S_0 tq image de $V(K)$ dans $\prod_{v \in S} V(K_v)$ non dense.

Corollaire Une variété K -rationnelle a la propriété de Hilbert, i.e. K est Hilbertien.

Conjecture (C.T): Si V est une variété lisse K -unirationnelle, alors V a la propriété (AFA).

Théorème La conjecture entraîne que tout groupe fini est groupe de Galois sur \mathbb{Q} .

Preuve $G \subset V = (\mathbb{A}^n / G)$ lisse
 V est K unirationnelle \rightarrow AFA \rightarrow Hilbert

Reste à démontrer les théorèmes 1 et 2. On le fait par réduction modulo v .

\mathcal{O}_K anneau des entiers de K
 V schéma de type fini sur $\mathcal{O}_K[\frac{1}{d}]$,
 $d \in \mathcal{O}_K, \neq 0$, plat.

$$V \otimes_{\mathcal{O}_K[\frac{1}{d}]} K \simeq V$$

Σ places de K ; $\Sigma_d = \{v \in \Sigma, \text{non arch}, v \nmid d\}$ (7)

$v \in \Sigma_d \iff \mathfrak{p}_v$ idéal premier de $\mathcal{O}_k[\frac{1}{d}]$
 $k(v) =$ corps résiduel, de card Nv
 \underline{V}_v schéma = $\underline{V} \otimes k(v) :=$ réduction mod \mathfrak{p}_v
 de \underline{V} (et de " V ").

* si \underline{V}_1 et \underline{V}_2 contiennent, on a $\underline{V}_{1v} \cong \underline{V}_{2v}$
 pour presque tout v .

Thme (Lang-Weil): Supposons V abs^t irréductible
de dimension m . On a alors

$$|\underline{V}(k(v))| = Nv^m + O(Nv^{m-\frac{1}{2}}).$$

la dém consistait à se ramener au cas des courbes. Pour une courbe de genre g (OPS prof l), la contribution de $V'_{\text{bir}} \xrightarrow{*} V^*$ donne $clgt$ par $O(Nv^{n-1})$ et alors $|V| = Nv + 1 - a$. On se ramène à courbe en fibrant. est Weil

Maintenant $N = \sum_{\lambda} \pm (\lambda)$
 vap de Frobenius

$$|\lambda| = Nv^{m/2} \quad 0 \leq m \leq 2m$$

\underline{V} abs^t irred \iff 1 seule val. λ tq
 $|\lambda| = Nv^m, \lambda = Nv^m$

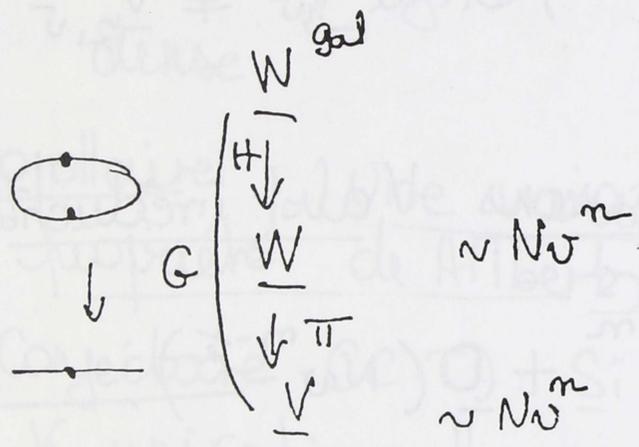
(dim cohom. l -adique des \underline{V}_v sont bornées).
 Ceci donne des bornes numériques précises (Bombieri).

Il manque une page dans le document original qui devait contenir la fin de la démonstration du théorème 1 et le début de celle du théorème 2, ainsi qu'un diagramme.

Le surj des flèches vient de la lissité

□ vient de ce que $\underline{W} \rightarrow \underline{V}$ étale fini.

Alors si $\pi(K(v))$ n'est pas surjectif, il en est de même de $\pi(K_v)$.



Lemme: $\exists c < 1$ telle que, si Nv assez grand, et $v \in \Sigma_\pi$

$$|\pi \underline{W}(K(v))| \leq c Nv^m + O(Nv^{m-\frac{1}{2}})$$

(vrai avec $c = 1 - \frac{1}{m!}$, $m = \deg \pi$)

Remarque: si galoisien, $c = \frac{1}{m}$

$$[G:H] = m = \deg \pi$$

$$\underline{W}(K(v)) = A \cup B$$

A pts relevables dans $\underline{W}^{\text{gal}}$. B = autres

$$|A| + |B| = Nv^m + \underline{O}$$

$$|\pi(B)| \leq |B|$$

$$|\pi(A)| \leq ?$$

$\left\{ \begin{matrix} Nv \text{ grand} \\ v \end{matrix} \right.$ se décompose complètement dans K_π , donc

$\underline{W}^{\text{gal}} / K(v)$ est \cup de $e (= [K_\pi : K])$ composantes absolument irréductibles de dimension m

$$|\underline{W}^{\text{gal}}(K(v))| = e (Nv)^m + \underline{O} \quad (\text{Lang-Weil})$$

On en déduit

$$|A| = \frac{e}{|H|} Nv^m + \underline{0}$$

$$|\pi(A)| = \frac{e}{|G|} Nv^m + \underline{0}$$

$$|\pi(A)| + |\pi(B)| \leq |B| + \frac{e}{|G|} Nv^m + \underline{0}$$

$$\leq \frac{e Nv^m}{|G|} + Nv^m \left(1 - \frac{e}{|H|}\right) + \underline{0}$$

$$\leq Nv^m \left(1 + \frac{e}{|G|} - \frac{e}{|H|}\right) + \underline{0}$$

$$\leq Nv^m \left(1 - \frac{1}{|G|}\right) + \underline{0}$$

$$|G| \leq m!$$

Ceci démontre le théorème 2.

Remarque: on a utilisé en dernier ressort le fait que \mathbb{A}^n a la prop. AF. On donnera d'autres dém (plus effectives) en utilisant le grand crible. Le dém de Hilbert est typiquement archimédienne (réf: Cours sur l'ordell Weil).

Théorème du grand crible

Il permet de donner une bonne estimation de la taille des ensembles minces :

Th Soit $A \subset \mathbb{Q}^m$ mince. Alors pour $N \rightarrow \infty$, le nombre des $a \in A \cap \mathbb{Z}^m$ de taille $|a| \leq N$, est $O(N^{m-\frac{1}{2}} \log N)$

On ne connaît pas d'ex où le log soit nécessaire.

Mais si $a = (a_1, \dots, a_n)$, $a_i \square$, on tombe sur $m - \frac{1}{2}$.

On va se limiter à \mathbb{Z}^m mais le grand crible marche sur des corps de nombres.

Théorème - Notations.

$n \geq 1 \quad N \geq 1 \quad A \subset \mathbb{Z}^n$

A contenu dans un cube de côté N

Pour tout p premier, soit $v_p \in \mathbb{R}$ avec $0 < v_p \leq 1$ tel que $|A_p| \leq v_p p^m$, $A_p = \text{image de } A \text{ dans } \mathbb{Z}_p^m$

(v_p est la proportion de classes mod p atteintes).

Enoncé Pour tout entier $D \geq 1$, on a

$$|A| \leq 2^m \sup (N, D^2)^m / L(D),$$

$$\text{où } L(D) = \prod_{\substack{q \text{ sqf} \\ q \leq D}} \prod_{\substack{p|q \\ p \leq D}} \frac{1 - v_p}{v_p}$$

$$\left(\geq 1 + \prod_{\substack{p \text{ premier} \\ p \leq D}} \frac{1 - v_p}{v_p} \right)$$

Si on choisit $D = N^{1/2}$ $|A| \leq (2N)^m / L(N^{1/2})$.

Exemples

(92)

(a) $\nu_p = \frac{1}{2}$ pour tout p

$$L(D) = \sum_{\substack{q \in D \\ q \text{ sst}}} 1 \quad \cup \quad D$$

$$|A| \ll N^{n-\frac{1}{2}}$$

"grand crible".

$$L'(D) \sim \frac{D}{\log D} \quad \text{on perd un peu } |A| \ll N^{n-\frac{1}{2}} \log N!$$

(b) "petit crible", on jette peu à chaque fois, type Eratosthène. $\nu_p = 1 - \frac{1}{p}$ par et.

$$L'(D) \sim \log \log D$$

$$|A| \ll \frac{N}{\log \log N}$$

$$L(D) \sim \log D$$

$$|A| \ll \frac{N}{\log N}$$

Montgomery-Vaughan: Dans tout intervalle de longueur N , il y a au plus $\frac{N}{\log N}$ nombres premiers.

"les nombres premiers ne s'accumulent pas trop".

Démonstration - $\mathbb{Z} =$ groupe des caractères du cercle.

$\Lambda = \mathbb{Z}^m =$ groupe des caractères de $T = \mathbb{R}^n / \mathbb{Z}^n$.

Si $a = (a_1, \dots, a_m) \in \mathbb{R}^m$ $\chi_a(x_1, \dots, x_n) = \exp(2\pi i \sum a_i x_i)$

$a \in \Lambda \mapsto \chi_a$ caractère sur T .

$A \mapsto \varphi = \varphi_A = \sum_{a \in A} \chi_a$ fonction sur T .

$\Lambda =$ groupe des car. de T , $\Lambda/p\Lambda$ est le groupe.

des caractères du noyau de $p: T \rightarrow T$. (93)

On traduit en termes de restriction à $T[p]$ les renseignements sur A_p :

le rest de ψ à $T[p]$ ne fait intervenir que χ_p p^n caractères de $T[p]$ (ceux qui sont ds A_p).

Principe: Une fonction faisant intervenir peu de caractères n'oscille pas beaucoup en valeurs absolues.

ex: fct de Dirac \leftarrow rep régulière \leftarrow ts les caractères
(oscille bcp) \leftarrow car \leftarrow caract.

constante \leftarrow 1 car.

Théorème Soit C_i ($i=1, \dots, h$) des groupes abéliens finis

$$C = \prod C_i \quad \widehat{C}_i = \text{dual de } C_i \quad \widehat{C} = \prod \widehat{C}_i$$

$$\Omega_i \subset \widehat{C}_i \quad \nu_i = \frac{|\Omega_i|}{|C_i|}$$

Soit ψ une fonction complexe sur C , ψ combinaison linéaire des caractères appartenant à $\Omega = \prod \Omega_i$.

Alors
$$\sum_{\substack{x \text{ primitif} \\ x \in C}} |\psi(x)|^2 \geq |\psi(0)|^2 \prod_{i=1}^h \frac{1 - \nu_i}{\nu_i}$$

$x = (x_1, \dots, x_h) \in C$ x primitif si $x_i \neq 0$ pour tout i .

Démonstration: Pour $h=1$

$$\psi = \sum_{x \in \Omega} c_x x$$

(3)

$$|\varphi(0)|^2 \leq \sum |c_x|^2 \sum_{x \in \Omega} 1 \leq \sum |c_x|^2 \cdot \nu_1 |C_1| \quad (14)$$

$$\sum |c_x|^2 = \frac{1}{|E|} \sum_{x \in C_1} |\varphi(x)|^2 \quad \text{Cauchy-Schw.}$$

$$\leq \nu_1 \left\{ |\varphi(0)|^2 + \sum_{x \text{ primitif}} |\varphi(x)|^2 \right\}$$

$$(1 - \nu_1) |\varphi(0)|^2 \leq \nu_1 \sum_{x \text{ primitif}} |\varphi(x)|^2.$$

Réurrence sur h :

Si $x \in C_2$, on note φ_x la fonction $(x_{1,1}, \dots, x_{h-1,1})$
sur $C_1 \times \dots \times C_{h-1}$.
 \downarrow
 $\varphi(x_{1,1}, \dots, x_{h-1,1}, x)$

$$\sum_{(x_{1,1}, \dots, x_{h-1,1}) \text{ prim.}} |\varphi(x_{1,1}, \dots, x_{h-1,1}, x)|^2 \geq |\varphi(0, \dots, 0, x)|^2$$

$$\sum_{x \text{ primitif}} |\varphi(x)|^2 \geq \frac{h-1}{\pi} \frac{1-\nu_i}{\nu_i} \sum_{x \neq 0} |\varphi(0, \dots, 0, x)|^2$$

\geq ce qu'on veut avec le ca: $h=1$.

ici $\varphi(0) = |A|$. On peut voir cela à la rigueur sur des points de division; ces points si suffisamment bien répartis.

Théorème (Davenport, Halberstam) Soit

a) une fonction φ sur \mathbb{T} , qui soit combinaison

linéaire de caract. χ_λ , où $\lambda \in \mathbb{C}$, cube de côté N

$$\varphi = \sum c_\lambda \chi_\lambda$$

b) $\delta > 0$ et $x_i \in \mathbb{T}$, δ -espacés ($|x_i - x_j| \geq \delta$ $i \neq j$)

$$\text{Alors } \sum_i |\varphi(x_i)|^2 \leq 2^m \sup \left(N, \frac{1}{\delta} \right)^m \|\varphi\|_2^2$$

$$\|\psi\|_2^2 = \int_T |\psi(x)|^2 dx = \sum_{\lambda \in C} |c_\lambda(\psi)|^2 \quad (95)$$

Remarque $|t| = \inf_{\substack{x \in \mathbb{R}^n \\ x \rightarrow t}} |x|$ $|x| = \sup(|x_1|, \dots, |x_n|)$.

Ces estimées entraînent l'inégalité du grand cube.

$$\psi = \sum_{a \in A} \chi_a$$

On va appliquer D.H avec $X = \bigcup_{\substack{q \text{ sup} \\ q \in \mathbb{D}}} T[q]$.

Ces points sont δ -espacés avec $\delta = \frac{1}{2^q}$.

$$\sum_{x \in X} |\psi(x)|^2 \leq 2^m \sup(N, \mathbb{D}^2)^m \|\psi\|_2^2$$

$$\|\psi\|_2^2 = \sum_{a \in A} 1^2 = |A|$$

d'où

$$\sum_{x \in X} |\psi(x)|^2 \leq 2^n \sup(N, \mathbb{D}^2) |A|$$

On va appliquer la lemme sur les groupes $\mathbb{Z}/q\mathbb{Z}$

$$T[q] = \prod_{p|q} T[p]$$

$X_q =$ els de X d'ordre égal à q
 $=$ pts primitifs de $T[q]$.

$$\sum_{x \in X_q} |\psi(x)|^2 \geq \frac{|\psi(0)|^2}{|A|^2} \times \prod_{p|q} \frac{1 - \nu_p}{2^p}$$

d'où

$$L(\mathbb{D}) |A|^2 \leq \sum_{x \in X} |\psi(x)|^2$$

Démonstration de D.H :

(56)

(a) si $\delta > \frac{1}{2}$ $|x - y| < \delta$ pour tout $x, y \in T$.

Dans ce cas il y en a au plus un x_i (si aucun c'est trivial).

On applique Cauchy - Schwarz à

$$\varphi(x) = \sum_{\lambda} c_{\lambda}(\varphi) \chi_{\lambda}$$

$$|\varphi(x)|^2 \leq \|\varphi\|_2^2 (N+1)^m$$

or $N+1 \leq 2N \dots$

(b) $\delta \leq \frac{1}{2}$

On fabrique une fonction auxiliaire

On construit une fonction continue θ sur \mathbb{R}^m à support ds $|x_i| \leq \frac{1}{2}$

/ Transformée de Fourier est en val absolue ≥ 1 sur C .

/ $\|\theta\|_2^2 \leq 2^m M^m$ $M = \sup(N, \frac{1}{\delta})$.

Soit λ le centre du cube C .

On prend $\theta(x) = \chi_{\lambda}(x) M^m \prod_{i=1}^m 2 \cos(\pi M x_i)$ si $|x_i| \leq \frac{1}{2}$
 $= 0$ sinon

Sur \mathbb{R}
 fonction type

$$\theta_0 = \begin{cases} 2 \cos \pi x & \text{si } |x| \leq \frac{1}{2} \\ 0 & \text{sinon.} \end{cases}$$

$$|\widehat{\theta_0}(y)| \geq 1 \quad \text{si } |y| < \frac{1}{2}$$

$$\int |\theta_0(x)|^2 dx = 2$$

car $\widehat{\theta_0}(y) = \frac{1}{\pi} \frac{\cos \pi y}{\frac{1}{4} - y^2}$

On identifie θ à une fonction sur T .

(97)

$$\mathbb{R}^m \rightarrow T$$

$$\theta dx_1 \dots dx_m$$

Si $\lambda \in \Lambda$, $c_\lambda(\theta)$ coefficient de Fourier pour θ vue sur T = valeur de la transf. de Fourier de θ en λ .
 ie i.e. $|c_\lambda(\theta)| \geq 1$ si $\lambda \in \Lambda \cap \mathbb{C}$.

$$\text{Soit } g = \sum_{\lambda \in \Lambda \cap \mathbb{C}} \frac{c_\lambda(\varphi)}{c_\lambda(\theta)} \chi_\lambda.$$

$$c_\lambda(g) \cdot c_\lambda(\theta) = c_\lambda(\varphi) \text{ pour tout } \lambda \in \Lambda.$$

$$\text{Donc } \varphi = g * \theta.$$

$$\varphi(x_i) = \int_T \theta(x_i - x) g(x) dx.$$

$$= \int_{\mathbb{B}_i} \theta(x_i - x) g(x) dx$$

$$\{x \mid |x - x_i| < \frac{1}{2} \delta\}$$

$$|\varphi(x_i)|^2 \leq \int_{\mathbb{B}_i} |\theta(x_i - x)|^2 dx \times \int_{\mathbb{B}_i} |g(x)|^2 dx$$

Cauchy-Schwarz

$$\leq 2^m \pi^m \times \int_{\mathbb{B}_i} |g(x)|^2 dx$$

des \mathbb{B}_i ne se recouvrent pas (x_i δ -espacés !!)

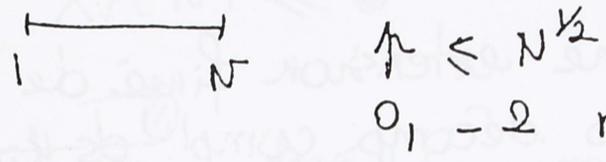
$$\sum |\varphi(x_i)|^2 \leq 2^m \pi^m \int_T |g(x)|^2 dx.$$

$$\leq 2^m \pi^m \sum_{\lambda \in \Lambda \cap \mathbb{C}} |c_\lambda(g)|^2 \leq (2\pi)^m \sum_{\lambda \in \Lambda \cap \mathbb{C}} |c_\lambda(\varphi)|^2$$

$$\leq (2\pi)^m \|\varphi\|_2^2$$

Application aux ensembles minces et à S.D. Cohen (L.P.S ~ 1982).

nombre premiers jumeaux $V_p = 1 - \frac{2}{p}$
On doit éliminer $m \equiv 0$ ou $-2 \pmod p$.
 $V_2 = \frac{1}{2}$



Les premiers jumeaux entre $N^{1/2}$ et N sont de ce qui reste et leur nombre est $O(N / (\log N)^2)$.

$\sum \frac{1}{p \text{ jumeau}}$ converge.

Application aux ensembles minces d'entiers.

A ensemble mince $C \mathbb{Z}^m$. (mince ds $\mathbb{A}_m^m(\mathbb{Q})$)

$A_N =$ pts de A dans un cube de côté N.

Th(Cohen) $|A_N| \ll N^{m-1/2} \log N$ pour $N \rightarrow \infty$
de $\log N$ est remplaçable par $(\log N)^\tau$, $\tau = \tau(A) < 1$.

Preuve 1^{er} type $(x_1, \dots, x_n) \in \mathbb{Z}^m$ satisf. à $\phi(x_1, \dots, x_n) = 0$ $\phi \neq 0$.
Pour ceux-là maj. en N^{m-1} $\phi = 0$.



2^e type correspond aux $x = (x_1, \dots, x_n)$ tels qu'une équation $a_0(x) x^m + \dots + a_m(x) = 0$, $a_i(x)$ polyn à coeff entiers, ait une solution dans \mathbb{Q} . ($m \geq 2$ ϕ abs. irréduct.).

On peut se ramener au cas où $a_0(x) = 1$ (en multipl par $a_0(x)^{m-1}$).

l'équation définit donc un schéma sur \mathbb{Z} .

$A_p \subset$ le sens de \mathbb{F}_p^m où $X^m + a_1(x) X^{m-1} + \dots + a_m(x) \equiv 0 \pmod p$ a une solution mod p .

$$W \xrightarrow{\pi} \mathbb{A}_{\mathbb{F}_p}^m$$

On a vu qu'il existe une extension finie de \mathbb{Q} , K_π / \mathbb{Q} telle que si p décomp compl. ds K_π , alors $\pi(W(\mathbb{F}_p)) \subseteq c p^m$ avec $c > 1$, p grand.

Dans le théorème du crible, on prend $v_p = c$ ($c < 1$) pour tout p premier décomp. compl. ds K_π , assez grand, $v_p = 1$ pour les autres.

$$L(D) = 1 + \sum_{\substack{p \text{ premier} \\ p \in D}} \frac{1 - v_p}{v_p} = 1 + \sum_{\substack{p \text{ grand} \in D \\ \text{d'éc. compl.} \\ \text{ds } K_\pi}} \frac{1 - c}{c}$$

$$\gg \frac{D}{\log D}$$

On obtient ainsi la majoration en $N^{\frac{1}{2}} \log N$.

On peut calculer $L(D)$ (cf cours sur "ordell") si :

$$L(D) \gg \frac{D}{(\log D)^\gamma}, \quad \gamma < 1.$$

$V \subset \mathbb{P}_r / \mathbb{Q}$ On a une notion de hauteur

$$x = (x_0, \dots, x_r) \quad H(x) = \sup |x_i|$$

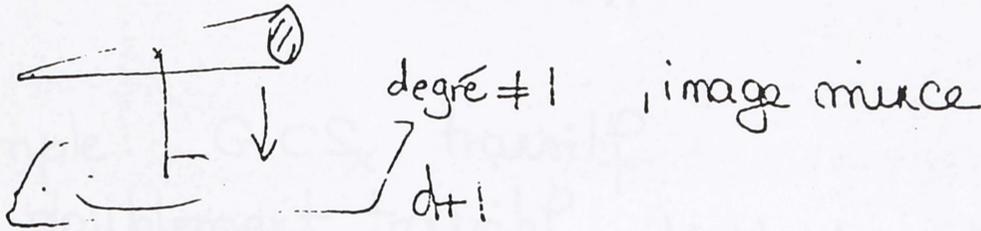
les x_i étant choisis dans \mathbb{Z} et premiers entre eux.

$N_V(N) = \#$ Nbre de points de $V(\mathbb{Q})$ avec $H(x) \leq N$, $N \rightarrow \infty$
 V variété linéaire de dim. d

$$X_V(N) \sim c N^{-d+1} \quad d \geq 1$$

Théorème si V est de dimension $d \geq 1$ et irréductible et non linéaire

$$X_V(N) \ll N^{d+\frac{1}{2}} \log N$$



Conjecture $\ll N^{-d} (\log N)^d$ pour un d convenable.

Exemple V surface cubique dans P_3
 $d = 2$

$$X_V(N) \ll N^{2+\frac{1}{2}} (\log N)$$

Si V contient une droite rationnelle \mathbb{Q} , les points rationnels sur \mathbb{Q} fournissent N^2 .

cf conjecture Manin : si on exclut les droites ; $N \log \dots$

Exemples avec groupes de Galois S_n, A_n

$PSL_2(\mathbb{F}_p)$ (K-y Shih) rest sur \mathbb{F}_p .

quelques propriétés caractéristiques de S_n et A_n .

$$G \subset S_n$$

G transitif

G primitif

$S_n =$ permutations de $\{1, \dots, n\}$. On préfère

$S_X =$ groupe des permutations de X , X est à n élts, $n \geq 2$.

$G \subset S_X$ imprimitif s'il existe une partition (Y_1, \dots, Y_k) de X , stable par G et non triviale ($|Y_i| \geq 2$, $k \geq 2$).

$$(Y_i) \Leftrightarrow R$$

$$G \curvearrowright X$$



$$G \curvearrowright X/P = \{1, \dots, k\}$$

G imprimitif \Leftrightarrow existence d'un quotient non trivial pour l'espace homogène X .

$\neq G$ primitif: "non imprimitif".

$X = G/H$ H fixateur d'un point.

$X/P \Leftrightarrow H'$ avec $G \supset H' \supset H$.

G primitif sur $X \Leftrightarrow$ fixateur d'un pt H est un ss-gpe maximal de G

$$G \leq L \setminus L^H \quad H \subsetneq G$$

$$n = (G:H)$$

H max de $G \Leftrightarrow$ pas de ceps (st.) intermédiaire entre K et L^H .

Exemple: $G \subset S_X$ transitif
doublement transitif si l'action de G sur les couples de points distincts est transitive.

Si $H =$ fixateur d'un point x
 G doublement transitif $\Leftrightarrow H$ transitif sur $X - \{x\}$.

Un groupe doublement transitif est primitif.

Lemme Soit $G \subset S_X$ transitif. Supposons que G soit engendré par des cycles d'ordre premier. Alors G est primitif.

$X = \{x_1, \dots, x_m\}$

Si non $\gamma_1 \cup \dots \cup \gamma_k$ partition non triviale stable par G .
Il y a un cycle d'ordre premier p ne stabilisant pas γ_1 .
OPS $s\gamma_1 = \gamma_2, s\gamma_2 = \gamma_3, \dots$
des éléments de $\gamma_1 \cup \dots \cup \gamma_p$ ne sont pas fixés par s
donc au plus p points donc $|\gamma_1| \leq 1$ Contradiction.

Lemme Soit $G \subset S_X$ transitif primitif.

Tout sous-groupe normal G' de $G, G' \neq \{1\}$ est transitif sur X :
des orbites de G' forment une partition de X ; cette partition est stable car G' est normal.

Théorème Soit $G \subset S_X$ transitif et primitif

(a) Si G contient une transposition, $G = S_X$.

(b) Si G contient un cycle d'ordre 3, on a $G = A_X$ ou S_X .

(c) Si G un cycle d'ordre 5, on a $G = A_X$ ou S_X pourvu que $|X| \geq 7$.

Contre exemple pour $|X|=5$, G cyclique d'ordre 5
 $|X|=6$, $A_5 \subset G \subset S_6$
(C. Jordan, TI + Traité de Subst...) action sur les 5-sylows.

Démonstration de (a):

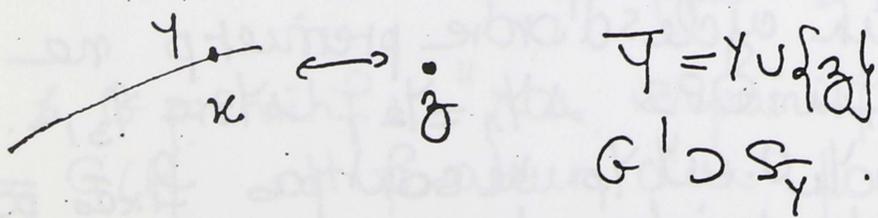
Soit $Y \subset X$ maximale telle que $S_Y \subset G$

Supposons $Y \neq X$.

$2 \leq |Y| \leq n-1$. $m = |X|$.

Soit G' le sig de G engendré par les transp. appartenant à G , G' est sig normal donc transitif.

Y n'est pas stable par G' . D'où une transposition $(xz) \in G'$ qui ne laisse pas stable Y . On peut supposer $x \in Y, z \notin Y$.



S_Y est engendré par S_Y et (xz) . Car ce groupe est transitif sur Y et il contient S_Y .

Lemme:

$B \subset A$ groupe de perm. trans. trans.

$B_x \subset A_x$ fixe x
Alors $B_x = A_x \Rightarrow B = A$.

(3)

Alors $G' \supset S_{\bar{y}}$ contrairement à la maximalité de γ .

Dem de b)

Soit G' le s/g de G engendré par les cycles d'ordre 3 de G . Alors G' est transitif. Soit $\gamma \subset X$ maximal tel que $G' \supset A_{\gamma}$. Supposons $\gamma \neq X$. $|\gamma| \geq 3$. Il existe un cycle $(abc) \in G'$ qui ne stabilise pas γ .

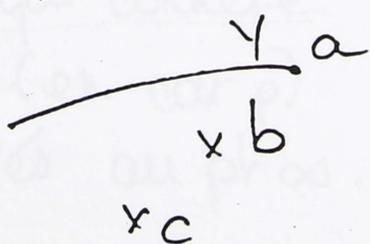
Deux possibilités : $(a, b, c) \cap \gamma$ a 1 ou 2 éléments.

1^{er} cas $\begin{cases} a \text{ et } b \text{ sont dans } \gamma \\ c \notin \gamma \end{cases}$

On pose alors $\bar{\gamma} = \gamma \cup \{c\}$

On a $A_{\bar{\gamma}} \subset G'$ car eng par A_{γ} et (a, b, c)

2^{ème} cas $a \in \gamma \quad b, c \notin \gamma$



$|\gamma| \geq 3$ il existe $b', c' \in \gamma$ tels que a', b', c' tous \neq .

Dans le groupe $A_5 = A_{\{a, b, c, b', c'\}}$, (abc) $(a b' c') \in G' \cap A_5$. Or ces deux éléments engendrent le groupe A_5 .

Donc $A_5 \subset G'$; en particulier $(b' a b)$

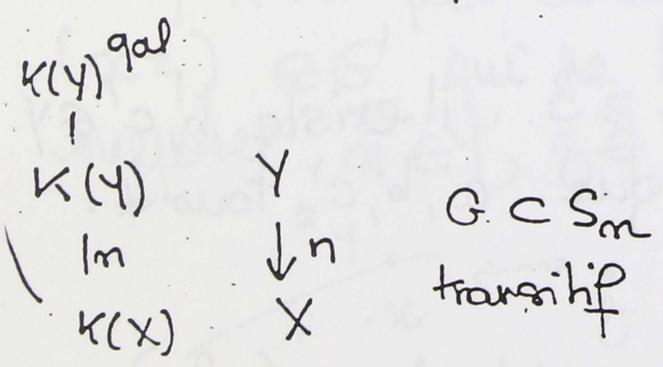
Théorème Soit $G \subset S_n$, transitif et engendré par des cycles d'ordre premier. Alors si G contient une transp. (resp. un cycle d'ordre 3), on a $G = S_n$ (resp. $G = A_n$ ou S_n).

Si $G \ni$ cycle d'ordre p , alors le groupe est $n - \varepsilon(p)$ -transitif.
 $\varepsilon(p) = 1$ pour $p = 2$
 $\varepsilon(p) = 2$ pour $p = 3$.

Si $*transitif$, contient donc le A_* correspondant. Alors classif des gpes finis, les $*transitifs$ pour x grand et sont A_x ou S_x .

Lemme Soit $G \subset A_n$ transitif contenant A_m , $m > \frac{n}{2}$. Alors $G = A_n$.

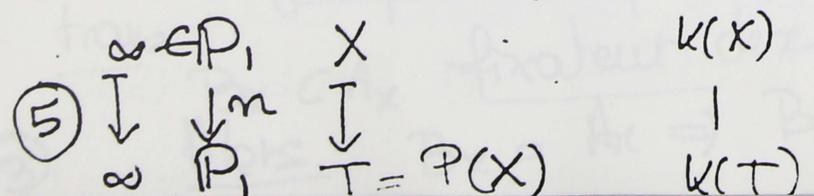
Car G primitif et contient un cycle d'ordre 3.



Hilbert Exemples d'extension de $\mathbb{Q}(T)$ à groupe de Galois S_m

$K = \text{car } \mathbb{Q}$.

$P(X) = X^m + \alpha_1 X^{m-1} + \dots + \alpha_n$ $\alpha_i \in K$



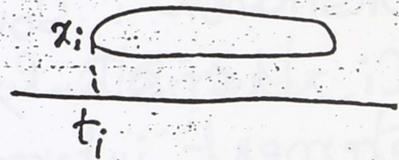
$K(T)$ adj1 racine de $X^m + a_1 X^{m-1} + \dots + a_{m-1} X + a_m = 0$.

Théorème : Si P est une fonction de Morse, alors le groupe de Galois de la cl. gal. de $K(X)/K(T)$ est S_m .

Fcton de Morse: p-critiques quadratiques et valeurs de fcton \neq .
 P de Morse: les racines de $\frac{dP}{dX}$ sont simples, x_1, \dots, x_{n-1} et les valeurs $t_i = P(x_i)$ sont distinctes.

∞ total ramif

les autres pts de ram et les x_i



Corollaire Il est $K(X)^{gal}/K(T)$ est régulière.

On peut supposer K alg. clos. (car G ne peut que diminuer).

Th (en car $\neq 0$): la droite projective est simplement connexe (ie pas de revêt fini étale connexe de degré > 1).

Thme (en car $\neq 0$) la droite proj P^1 , privée d'un pt, est simplement connexe.

(en car p) idem pour les revêts modérément ramifiés au pt ∞ . (gpe d'inertie d'ordre premier $\neq p$).

si

X

\downarrow

P^1

rev d'ordre $m \geq 2$

nr en dehors de ∞
mod ram à l' ∞

$$e_{i,1} = k$$
$$\sum e_i = m$$

la formule de Hurwitz donne ce qu'on veut.

Revenons en car 0

(107)

X

↓ rev galoisien à gr G ramifié en des points $t_1, \dots, t_h \in P_1(K)$.

Soient C_1, \dots, C_h des groupes d'inertie relatifs à des $x_i \in X(K)$ au-dessus de t_i .

Théorème G est engendré par les conjugués de C_1, \dots, C_{h-1} .

Démonstration : Soit G' le groupe engendré par les conjugués des C_i $1 \leq i \leq h-1$; G' est normal $\subset G$, d'où un revêtement intermédiaire

X

↓

X/G'

nr en t_1, \dots, t_{h-1} donc trivial

↓ G/G'

$G = G'$

P_1

En car $p > 0$, G est engendré par les conjugués des C_i ($1 \leq i \leq h$).

en car $p > 0$ si la ramif. est modérée ^{en t_h} r_1 , alors G eng par les conj des C_i ($1 \leq i \leq h-1$).

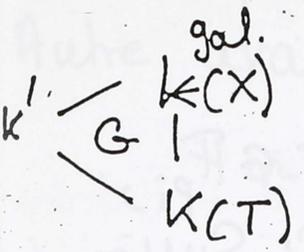
En car 0 : il y a un choix des C_i tq G soit engendré par C_1, \dots, C_{h-1} .

A appliquer au revêtement donné par $P(x) - T = 0$ où P est une fonction de Torse de deg n.

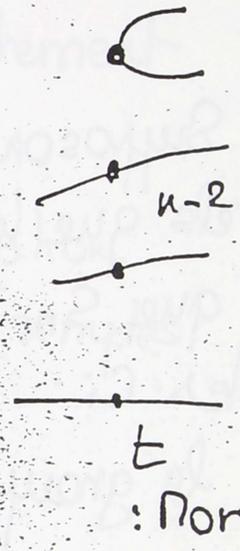
G est eng par les conjug des gps d'inertie en des t_i , où $t_i = P(x_i)$ - et même de n-1.

⊕

$\begin{cases} G_i \text{ est eng. par une transposition pour } i \leq n-1 \end{cases}$ (H_i)
 G_n (inertie à l'v) cycle d'ordre n .



$$K(X) \otimes_{K(T)} \widehat{K(T)}_t = \prod_{x \rightarrow t} \widehat{K(X)}_x$$



$K(X) \otimes_{K(T)} \widehat{K(T)}_t =$ ext quad ramif des corps local
 $x \rightarrow t$ étale de degré $n-2$.

l'inertie qu'on a par permutation de 2 éléments.

G est transitif car $K(X)/K(T)$ est de degré n .
engendré par des transpositions.
donc G est primitif $\Rightarrow G = S_n$.

Extensions sur $\mathbb{Q}(T)$ à groupe de Galois $S_n \Rightarrow$ ext de \mathbb{Q} (thème d'ind.).

Valeurs de T pour lesquelles on trouve par spécialisation ce qu'on veut.

$$P = X^m - X$$

$$X^m - X - t = 0 \quad t \in \mathbb{Q}, t \neq \text{ent mûce}$$

est une ext ind. à groupe S_n .

Fixons $m=5$ par exemple

$$x^5 - x - t = 0 \quad \text{mod } p$$

gpe de Galois eng par l'elt de Frob σ_p .

On cherche des val des $t \in \mathbb{F}_p$ et des f, σ_f soit une classe de conj imposée dans G .

$$\sigma_f = (12)(345) \dots$$

Supposons trouvés t_i, p_i tels que $t_i \in \mathbb{F}_{p_i}$, tels que la classe de conj de Frob_{p_i} soit C_i . Supposons que S_n soit le seul σ de S_n rencontrant tous les C_i . Alors si $t \in \mathbb{Z}$ $t \equiv t_i \pmod{p_i} \forall i$ le groupe de Galois de l'ext relat à t est S_n .

Lemme (Jordan) Soit G un groupe fini et $H \subset G$ rencontrant toutes les classes de conjugaison de G . Alors $H = G$.

car $\bigcup_{g \in G} gHg^{-1} = G \implies H = G$.

en effet $1 + \bigcup_{g \in G/H} g(H - \{1\})g^{-1} = \bigcup_{g \in G} gHg^{-1}$

$$|\bigcup_{g \in G} gHg^{-1}| \leq 1 + \frac{|G|}{|H|} (|H| - 1) < |G| \text{ si } \frac{|G|}{|H|} \geq 2.$$

Sans Jordan, énoncé : $G \subset S_X, |X| \geq 2, G$ transitif, il existe $g \in G$ qui opère sans point fixe.

Autre exemple $X^m - X^{n-1} - T = 0$. (pas de torsion) donne S_m .

On regarde la ramif : cycle d'ordre 2, cycle $nX^{n-1} - (n-1)X^{n-2} = +X(Xc)$ d'ordre $n-1$, cycle d'ordre n (à l'as).

si $G \subset S_n$ contient ces élt, il vaut S_n . Car transitif et m d'bt transitif (car \ni cycle).

donc il est primitif et il contient transpos.

Cet exemple intervient dans la rigidité.

Autre avantage: on peut expliciter le revêtement

n P_{m-1} $x = (x_1, \dots, x_n)$

S_n opère par permutation

On va écrire les équations invariantes les + simples

$\sum x_i = 0$

$\sum x_i x_j = 0$

etc...

$\sum x_1 \dots x_{n-2} = 0.$

car 0.

(marche en corp si $p \neq n, p \neq n-1$).

ou encore

$\left\{ \begin{array}{l} \sum x_i = 0 \\ \sum x_i^2 = 0 \\ \vdots \\ \sum x_i^{m-2} = 0. \end{array} \right.$

On obtient une courbe lisse C_n connexe, int. complète, S_n opère dessus \in

$g(C_m) = 1 + (m-2)! \frac{m^2 - 5n + 2}{4}$

$n=3 \quad 0 \quad 4$

$n=4 \quad 0$

$n=5 \quad 4$

$n=6 \quad 49$

⋮

$C_n / S_n \cong P_1$

$x \mapsto \frac{\sigma_{n-1}(x)^m}{\sigma_n(x)^{n-1}}$

$\sigma_{n-1} = [x_1 \dots x_{n-1}]$

$\sigma_n = x_1 \dots x_n$

C_n
↓

$C_n / S_{n-1} \cong P_1(x) \quad x^n - x^{n-1} = T$

n=3 g=0.

C₃ = P₁ avec action de S₃ (CPG₂)

n=4

C₄ ≃ conique ss pt (associée aux quaternions)

(x₁, ..., x₄) P₃
x₁ + ... + x₄ = 0 P₂
x₁² + ... + x₄² = 0 conique (ss pt) sur Q

action de S₄ (C → PGL₂ tordus de quater.)

n=5

C₅
() P₄
Σ x_i = 0 P₃
Σ x_i² = 0
Σ x_i³ = 0 quad ∩ cub = courbe de Bring

g=4.

Action de S₅

Bring / S₅ = P₁

Π (X - x_i) = Xⁿ + λX + μ

Bring - Jerrard: Toute equation de d° 5 peut se ramener apres ext de racines □ et □ à X⁵ + λX + μ = 0.

K₅ | degre 5 / K

x ∈ K₅ x ∉ K
Tr x = 0 Tr x² = 0 Tr x³ = 0

K₅ ≃ Kx · -x K

Ces x st un cone sur une courbe de type Bring.

Une telle Ω est un pt rationnels sur une ext de K
quad / cub.

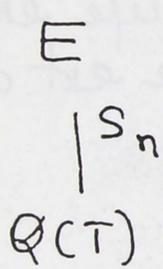
quad Ω cub de \mathbb{P}_2 .

contient
l'cte (quies.
extension)

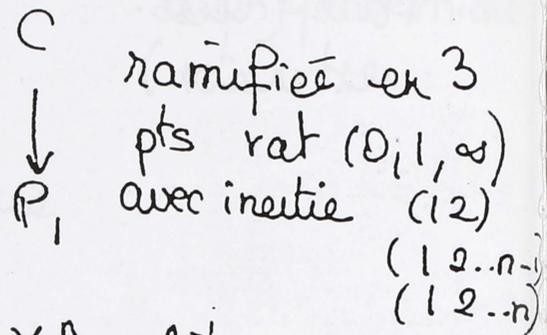
si dte \neq cub, la coupe en 3
pts rationnels sur une ext de
degre 3.

Construction d'extensions régulières de $\mathbb{Q}(T)$
à groupe de Galois $A_n, PSL_2(\mathbb{F}_p)$.

Pour A_n :

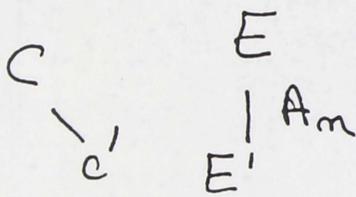


la dernière fois:



$$X^n - X^{n-1} - T = 0$$

à peu de choses près



$$\mathbb{P}^1 \xrightarrow{2} \mathbb{Q}(T) \quad y^2 = \Delta(T) \text{ (disc. de l'équation précédente)}$$

donc C' courbe de genre 0 avec pt rationnel (les 2 pts de ram le st) donc $\cong \mathbb{P}^1$

$$E' = \mathbb{Q}(T')$$

Le cas de $PSL_2(\mathbb{F}_p)$.

Construction modulaire de K -y Shil.
Pts de division des courbes elliptiques

① c. ell sur $\mathbb{Q}(T)$.

$$j(E) = T$$

ex (Tate) $y^2 + xy = x^3 - \frac{36}{T+28}x - \frac{1}{T+28}$

l nombre premier

$$T_\ell E = \lim_{\leftarrow} E_{\ell^m} \quad \mathbb{Z}_\ell \text{ libre de } \mathbb{Z}_\ell$$

$$E_{\ell^m} = \text{Ker } \ell^m : E(\bar{k}) \rightarrow E(\bar{k})$$

$$\rho_\ell : G_K = \text{Gal}(\bar{k}/K) \rightarrow GL_2(\mathbb{Z}_\ell)$$

ici $\dots \rightarrow$

cf par ex Weber (T III)

$$G_K \xrightarrow{P} G_b(\mathbb{Z}_e) \xrightarrow{\det} \mathbb{Z}_e^*$$

$\xrightarrow{\text{car cyclotomique } \chi_e}$

$$G_K \longrightarrow \mathbb{Z}_e^* \text{ surject.}$$

Sur $\mathbb{C}(T)$, image à $\det = 1$, en fait tout $SL_2(\mathbb{Z}_e)$
 car image contient (mod ± 1) l'image de $SL_2(\mathbb{Z})$

$$E_e: G_K \longrightarrow G_b(\mathbb{F}_e) \xrightarrow{\det} \mathbb{F}_e^*$$

$\xrightarrow{\chi_e \text{ car cycl.}}$

$$SL_2 \left\{ \begin{array}{l} L \\ | SL_2 \\ \mathbb{Q}(\zeta_e)(T) \\ | \mathbb{F}_e^* \\ \mathbb{Q}(T) \end{array} \right. \quad \begin{array}{l} \text{Pas régulière } \mathbb{Q}(\zeta_e) / \mathbb{Q}. \\ l > 2. \end{array}$$

la méthode de Shih consiste à tordre cette construction.

On se donne ^{Caro} une extension quadratique K/k
 avec $\langle \sigma \rangle = Gal$. On se donne E sur K
 On se donne aussi une N -isogenie $\varphi: E \rightarrow E^\sigma$
 (défini sur \bar{K}).

Hyp E n'a pas de mult complexe
 Dans ce cas, les 2 seules N -isogenies sont φ et φ .

Soit l premier $\neq 2$, $l \nmid N$.

$$\varphi_e: E_l \xrightarrow{\sim} E_l^\sigma \quad (\text{canonique au signe près}).$$

$P\varphi_e: PE_e \xrightarrow{\sim} PE_e^\sigma$
 droite projective
 à l+1 pts

(115)

$$E \xrightarrow{\pm\varphi} E^\sigma \xrightarrow{\pm\varphi'} E$$

$\pm\varphi^\sigma$

$$\varphi^\sigma = \pm\varphi'$$

G_k agit sur PE_e
 (x, y)

$x \in PE_e$
 $y \in PE_e^\sigma$ qui se correspondent
 par $P\varphi_e$.

d'où: $G_k \xrightarrow{P} PG_2(\mathbb{F}_e)$

$G_k \supset G_k$
 sg d'indice 2

$s \in G_k$
 s agit sur E_e
 d'où un élt de $G_2 \rightarrow PG_2$

si $s \notin G_k$ s induit σ
 $E_e \rightarrow E_e^\sigma \xrightarrow{\varphi_e^{-1}} E_e$

$PG_2(\mathbb{F}_e) \rightarrow PG_2(\mathbb{F}_e) \xrightarrow{\det} \{\pm 1\} \rightarrow 0$

$\delta(\varphi): G_k \rightarrow \{\pm 1\}$

$l^* = (-1)^{\frac{l-1}{2}} l$

$\mathbb{Q}(\sqrt{l^*}) \subset \mathbb{Q}(\zeta_l)$

unique corps quadratique
 de $\mathbb{Q}(\zeta_l)$.

Théorème

① si $\left(\frac{N}{l}\right) = 1$, alors

$\delta(\varphi) = \varepsilon_e$

② si $\left(\frac{N}{l}\right) = -1$ alors

$\delta(\varphi) = \varepsilon_e \varepsilon_{k|k}$

Notons $\varepsilon_e: G_k \rightarrow \{\pm 1\}$
 qui donne l'action
 de G_k sur $k(\sqrt{l^*})$

$\varepsilon_{k|k}: G_k \rightarrow \{\pm 1\}$ via G_k

Démonstration

$\Lambda^2 E_e \simeq \mu_e$
 choix du signe
 par

$E = \mathbb{C}/L \quad E_e = L/eL \quad \Lambda^2 L = \mathbb{Z}$

$\Lambda^2 E_e = \mathbb{Z}/e\mathbb{Z} = \mu_e$
 $\underbrace{\hspace{1cm}}_{e^{2\pi i/e}}$

$d: E \rightarrow F$

$\alpha_e: E_e \rightarrow F_e$

$\Lambda^2 d_e: \mu_e \rightarrow \mu_e$ multipl. par degré

fait $E_e = H_1(E, \text{mod } e)$

$\mu_e = H_2(E, -)$

$s \in G_{\mathbb{R}} \quad PE_e$

Ⓐ si $s \in G_{\mathbb{R}} \quad \delta(p)(s) = E_e(s)$

$E_e \xrightarrow{s} E_e$
 det mod \square

Ⓑ si $s \in G_{\mathbb{R}} - G_{\mathbb{R}}$

$E_e \xrightarrow{s} E_e \xrightarrow{\varphi_e^{-1}} E_e$
 $\mu_e \xrightarrow{s} \mu_e \xrightarrow{N^{-1}} \mu_e$

$N^{-1} \chi_e(s) \in \mathbb{F}_e^{\times} / \square = \{\pm 1\}$
 d'où le théorème

On va supposer $\left(\frac{N}{e}\right) = -1$ dans la suite

$\delta(p) = E_e E_{k|k}$

Etape suivante : choix de k, κ, E .

$\chi_0(N)$ classifie les isogénies de degré m

corps de fonctions $\mathbb{Q}(j, j_N)$

$j = \frac{1}{q} + 744 + 196884q \dots \quad j(z) = e^{2\pi i z}$

$j_N(z) = j(Nz) = \frac{1}{q^N} + 744 + 196884q^N \dots$ (4)

On prendra $k = \mathbb{Q}(j, j_N)$ (de trace)

Il existe une involution σ ν permutant j et j_N ^(σ, w_1, w_n selon auteurs)

$$k = \text{corps des pts fixes} = \mathbb{Q}(j, j_N)^+$$

$$= \text{--- de fonctions de } X_0(N)^+ = X_0(N) / \{1, w_N\}$$

E courbe elliptique sur k d'invariant j .

$$\Phi_N(j, j')$$

$$k = \mathbb{Q}[j, j_N] / (\Phi_N(j, j_N)).$$

Il est bien vrai que E^σ a comme invariant j_N et est donc N -isogène à E .

D'où un homom de $G_k \xrightarrow{p} PGL_2(\mathbb{F}_e)$ associé à k, N, E, N, l .

① p surjectif

② $\delta(p) = E_l E_{kl} k$

③ d'ext. corresp de $k \cong \mathbb{Q}(j, j_N)^+$ est rég.

$$1 \rightarrow PSL_2(\mathbb{F}_e) \rightarrow PGL_2(\mathbb{F}_e) \rightarrow \{t | y \rightarrow y\}$$

image de G_k contient $PSL_2(\mathbb{F}_e)$, car c'est vrai

$$\mathbb{Q}(j, j_N) = (\mathbb{Q} \otimes k) \text{ fract sur } \mathbb{Q}.$$

$$\mathbb{Q}(j, j_N) = k$$

$G_{\mathbb{Q}(j)}$ agissant sur $T_e(E) \times \prod_{2|N} T_{e^1}(E)$

donne $SL_2(\mathbb{Z}_e) \times \prod SL_2$.

D'où une ext gal. régulière de $k = \mathbb{Q}(j, j_N)^+$ à groupe $PGL_2(\mathbb{F}_e)$.

Supposons que $N \in S = \{2, 3, 5, 7, 11, 13, 19, 23, 29, 31, 41, 47, 59, 71\}$

$N \in S \iff$ genre de $X_0(N) = 0$.

$X_0(N)$ a 2 ptes ($0, \infty$).

Alors $k = \mathbb{Q}(\Gamma)$.

Théorème : Si l premier ≥ 3 est tel que $(\frac{N}{l}) = -1$ pour au moins un $N \in S$, alors $PSL_2(\mathbb{F}_l)$ a la prop. Gal.

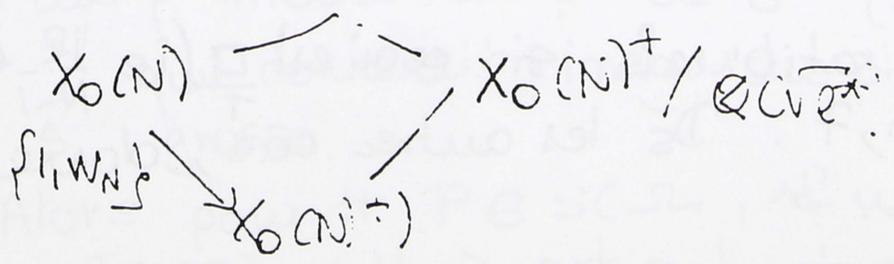
(vrai pour $l < 5329271$)

On veut PSL_2 .

$E_{K|k} \cdot E_e$
 $K = \mathbb{Q}(j, j_N)^+$ $\xrightarrow{2}$ $\mathbb{Q}(\sqrt{e^*}) \cdot \mathbb{Q} = \mathbb{Q}(\sqrt{e^*}, j, j_N)^+$
 E_e

Dans le composé (ciquadratique) sur k , on regarde le corps intermédiaire $K_1(N, e)$, car associé $E_{K|k} \cdot E_e$.

D'où une ext. régulière de $K_1(N, e)$ à groupe de Galois $PSL_2(\mathbb{F}_l)$.



$K_1(N, e)$ est le corps de fonctions de $X_0(N)$ tordue par le groupe d'automorphismes $\{1, w_N\}$ relatif à l'ext quid $\mathbb{Q}(\sqrt{e^*}) / \mathbb{Q}$.

$G_{\mathbb{Q}} \xrightarrow{E_e} \{1, w_N\} \rightarrow \text{Aut } X_0(N)$

On appelle cette courbe $X_0(N)_\ell$.

genre $X_0(N)_\ell = 0$ si $N \in \{2, 3, 5, 7, 13\}$
(N 1^{er})

a 1 pt rationnel si $N \in \{2, 3, 7\}$.

Le corps $K = (\mathbb{C}, \ell)$ est isomorphe à $\mathbb{Q}(T)$ si $N \in \{2, 3, 7\}$ $\left(\frac{N}{\ell}\right) = 1$

Pour $N = 5$ ou 13 $\left(\frac{N}{\ell}\right) = -1$ jamais de points!!!.

Si $N = 2, 3, 7$ l'involution w_N de $X_0(N)$ a deux points fixes rationnels sur \mathbb{Q} . Ils donnent des pts rationnels dans $X_0(N)_\ell$.

Si $N = 2, 3, 5, 7, 13$ $N-1$ divise 12.

$K = \mathbb{Q}(T)$ avec un T explicite

$K = \mathbb{Q}(\{j_m\}_N) \subset$ séries formelles en q .

$$T = \left(\frac{\Delta(z)}{\Delta(Nz)} \right)^{\frac{1}{N-1}} = q^{-1} \prod_{m=1}^{\infty} (1 - q^m)^{\frac{24}{N-1}}$$

$$\Delta = q \prod_{m=1}^{\infty} (1 - q^m)^{24}$$

$N \times m$

$$w_N(T) = N^{\frac{12}{N-1}} \frac{1}{T}$$

les pts fixes sont rationnels si ceci est \square (ie $\frac{12}{N-1}$ est pair) soit $N = 2, 3, 7$. Dans les autres cas, donne équation conique.

Autre manière de procéder:

Description explicite des pts fixes de w $N = 2, 3, 7$.

$N = 2$ $\left\{ \begin{array}{l} \text{m.c. par } \mathbb{Z}(i) \\ \text{endu } 1+i \end{array} \right.$
 $\rightarrow \sqrt{-2}$ et $\sqrt{2}$.

(7)

$N=3$ m.c. par $\mathbb{Z} \left[\frac{\sqrt{-3}+1}{2} \right]$, $-\sqrt{3}$
 $\mathbb{Z} [\sqrt{-3}]$, $\sqrt{3}$

$N=7$ m.c. par $\mathbb{Z} \left[\frac{1+\sqrt{-7}}{2} \right]$, $\sqrt{-7}$
 $\mathbb{Z} [\sqrt{-7}]$, $\sqrt{-7}$

des pts correspondants st rationnels car nombre de classes = 1
 pour isogénie $\bar{\pi} = -\pi$
 ou $\bar{\pi} =$ unité π .

5 et 13 ne marchent pas car $h=2$.

Théorie Shih si $\sigma_i \left(\frac{N}{p} \right) = -1$ pour au moins un $N \in \{2, 3, 7\}$
 alors $PSL_2(\mathbb{F}_p)$ a le μ op Gal $_{\mathbb{Z}}$.

Premier ex ne marche pas $p=47$.

Théorie d'irréductibilité avec paramètre elliptique (Néron).
 Soit $X \rightarrow S$ un revêtement ramifié régulier galoisien
 à groupe G , S courbe de genre 1 sur \mathbb{Q} (\mathbb{C} de nbs)
 On suppose qu pour tout sous-groupe H de G contenant
 (G, G) et $\neq G$, le revêtement $X/H \rightarrow S$ ~~soit~~ est ramifié
 en au p moins un pt de S (cette d'avoir isogénie
 qui donnerait image des pts rationnels trop
 grosse).

Alors pour $H \neq P \in SC(\mathbb{Q})$, et un nbre fini, on
 a $Int(P)$ (d'où ext gal. de g $_{\mathbb{Z}}$ σ).

En effet X/H de genre ≥ 2 \rightarrow nombre fini
 Faltings
 Néron (ignoraient Faltings!) : nombre fini \rightarrow ext - gal
 que $SC(\mathbb{Q})$.

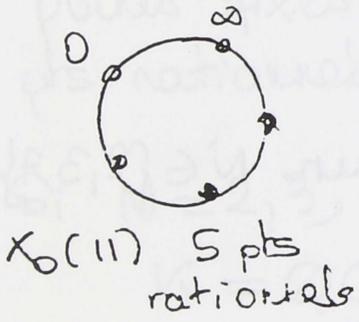
Courbe Si on tel revêt existe sur \mathbb{Q} avec $S(\mathbb{Q}) \neq \emptyset$,
H cours de nbres a des ext. galois de gpe G .

Très bon théorème mais pas pour les calculs numériques!

Ex $p=47$ $N=1$

$S_{inh} \Rightarrow$ ext galois $PSL_2(\mathbb{F}_{47})$ au-dessus de $K_1(N, \ell)$
c. des fct'ns de $X_0(N)_\ell$.

$X_0(11)_{47}$ a une orbite de pts rationnels.



$-47y^2 = f(x)$

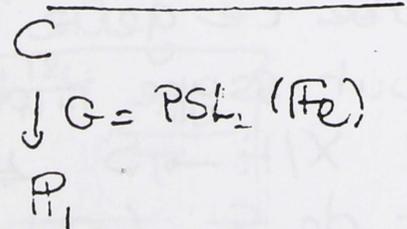
On peut prendre $f(x) = 4x^3 - 4x^2 + 1$
(donne courbe isogène à $X_0(11)$)

$x = -2, y = 1$ d'ordre ∞ (cf par réduct)
 $x = -8, y = 7$

It cours de nbres possède ext gal à gpe de Galois
 $PSL_2(\mathbb{F}_{47})$.

explicite sur \mathbb{Q} par Ekerès.

$N = 2, 3, 7$
 $(\ell, \frac{N}{\ell}) = -1$



Ramification

$N=2$ 3 pts

inertie d'ordre $2, \ell, \ell$
i.e $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$

(méthode de rigidité donne ce qu'on veut)

$N=3$ idem $3, \ell, \ell$

$N=7$ ram en 4 pts inertie d'ordre
 $3, 3, \ell, \ell$.

On peut choisir le paramètre pour que
les pts soient $\sqrt{-27}, \sqrt{-27}^*$

(pas obtenu par rigidité)