JEAN-PIERRE SERRE
E. BAYER (réd.)
C. GOLDSTEIN (réd.)

Problèmes Galoisiens – I

Cours de Jean-Pierre Serre, tome 9 (1989)
<http://www.numdam.org/item?id=CJPS_1989__9_>

Jean-Pierre SERRE

Problèmes Galoisiens - I

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

Notes de E. Bayer et C. Goldstein

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 $n \geqslant 1$ tel que tout élément de G soit d'ordre $\leqslant p^n$.

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

(S_n) – Pour tout nombre premier $q \in \mathrm{ram}(L/\mathbf{Q})$, 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 $\mathrm{Gal}(K/\mathbf{Q}) = G/C$, 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 $\mathrm{ram}(L/\mathbf{Q}) = \mathrm{ram}(K/\mathbf{Q}) \cup \{q\}$, 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 $\mathbf{Q}(T_1, \ldots, T_n)$, $n \geqslant 1$.)

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 $n \geqslant 1$ et une extension galoisienne régulière de $\mathbf{Q}(T_1, \ldots, T_n)$ de groupe de Galois G.

(Le fait que (ii) $\Longrightarrow$ (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 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 = $\mathbf{PSL}_2(\mathbf{F}_p)$, 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 $L = \mathbf{Q}(X_1, \ldots, X_n)$. 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. $K(T_1, \ldots, T_m)$ est isomorphe à $\mathbf{Q}(T_1, \ldots, T_{n+m})$ 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'analogue de (N) sur $\mathbf{C}$ peut être en défaut : le corps $K_\mathbf{C}$ des invariants de G dans $\mathbf{C}(X_1, \ldots, X_n)$ 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 $K_\mathbf{C}$ 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 $K_\mathbf{C}$. (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 **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 $\mathbf{Q}(X_1, \ldots, X_n)$.

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), 2ᵉ 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* **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* 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 degré ... 13

Théorème de Scholz - Reichardt ... 21

Sous-groupes de Frattini ... 41

Ishanov - Šafarevič ... 45

Variétés rationnelles ... 49

Lemme sans nom ... 51

Gal_T ... 56

Bitangentes réelles ... 59

Construction de Saltman ... 65

Th. d'irréd. de Hilbert ... 70

Ensembles minces ... 72

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 Morse ... 106

La construction de Shih ... 113

Serre 9/1/89

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 :

$$\left.\begin{array}{cc} A_5 & 60 \\ SL_3(\mathbb{F}_2) & 168 \\ A_6 & 360 \\ SL_2(\mathbb{F}_8) & 504 \\ \vdots & \end{array}\right\} \text{connus pour être groupes de Galois d'ext. de } \mathbb{Q}(T)$$

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

M_{23} ?

Les petits groupes sont souvent des PSL_2 et la conjecture est connue dans ce cas.

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

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

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

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

Hilbert 1890, théorème d'irréductibilité
$\implies S_n, A_n$ 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

$$P_t(X) = 0$$

<u>Hilbert</u> 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.

$$\begin{array}{l} Y \\ \downarrow \pi \\ X \end{array}$$

G groupe qui opère sur Y librement

$$X = Y/G$$

$/K$ revêtement galoisien étale.

$$\begin{array}{l} Y \\ \downarrow \pi \\ X = \mathbb{P}_1 - \{\text{ram.}\}. \end{array}$$

(param. par T)

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

Sur $\overline{K}$, $\pi^{-1}(x)$ ds $Y(\overline{K})$

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

<u>Irr</u> Si les points $y \in \pi^{-1}(x)$ sont conjugués entre eux par $\mathrm{Gal}(\overline{K}/K)$

$\Rightarrow$ extension galoisienne de K à groupe de Galois G.

Cas général (i.e. si <u>Irr</u> n'est pas vraie).

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

$$s \in \mathrm{Gal}(\bar{K}/k) \longrightarrow G$$

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

$$s \longmapsto g(s)$$

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

$$\left(\begin{array}{ccc} K(X)^{gal} & & Y \\ | & & \downarrow \\ K(X) & & X_n \\ | & & \downarrow \text{ de degré } n \\ K(T) & & X = \mathbb{P}_1 - \{\Delta = 0\} \end{array}\right)$$

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

K corps de nombres

X variété K-rationnelle

($K(X)$ ext. transcendante pure de K).

Alors le théorème d'irréductibilité de Hilbert marche

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

?? de E - CT $\Longrightarrow$ conjecture

S_n

S_n agissant sur Aff^n par perm. des coord.

$$\mathrm{Aff}^n \xrightarrow{S_n} \mathrm{Aff}^n$$

$$K[x_1, \dots, x_n]$$
$$|$$
$$K[\sigma_1, \dots, \sigma_n].$$

E. Noether ($\sim$ 1918)
Méthode de Hilbert s'applique à tout s/g 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 s/g de S_4.

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

Démonstration la semaine prochaine

G d'ordre p^m

On peut choisir $E/\mathbb{Q}$, $Gal = G$

E ramifiée en seulement m nombres premiers.

$m = 1$ groupe cyclique d'ordre p

$\ell \equiv 1 \pmod p$

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

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

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 paraitra bientôt.

G résoluble d'ordre impair : démonstration de Neukirch (197)

R. Swan (1969)

le corps des invariants de C 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 ($\sim$ 1984) pas tis pur sur $\mathbb{C}$ p-groupe, p^9 ou mieux).

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

Aussi résultats de Voskresenskii.

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

Wang ($\sim$ 1949)

"thm" de Grünwald. On donne des caractères locaux

$i = 1, \dots, k$ $\quad G_{\mathbb{Q}_{p_i}} \xrightarrow{\chi_i} C_n$ cyclique d'ordre n

p_i distincts

$$\mathbb{Q}_{p_i}^* \longrightarrow C_n$$

Il existe un homomorphisme global

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

qui, localement en p_i, donne χ_i

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

algèbre galoisienne, donnée localement.

Publiée par Grünwald ~ 1938.

Contre-exemple de Wang : $n = 8$

$k = 1$, $p_i = 2$.

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

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

Une telle extension E est associée à un caractère

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

$2 \nmid n$, $\chi(2)$ engendre C_8.

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

$n = \prod_{\ell \neq 2} \ell$ $\qquad \chi = \prod \chi_{\ell}$

$$\chi_{\ell} : (\mathbb{Z}/\ell\mathbb{Z})^* \longrightarrow C_8 .$$

Il existe un ℓ tel que $\chi_\ell(2)$

engendre C_8.

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

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

$\Longrightarrow \chi(2) = \chi(x)^2 \Longrightarrow \chi(2)$ n'est pas un générateur !

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

Si "Noether" marche :

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

on obtient une extension générique (universelle) elle donne par spécialisation toutes les extensions à groupe de Galois G.

$$\begin{array}{c} E \\ \Big|\, G \\ K \end{array} \qquad \begin{array}{c} Y \\ \Big\downarrow G \\ P \in X \end{array} \qquad \mathrm{Gal}(E/K) \xrightarrow[\varphi_E]{} G$$

On "tord" : $\begin{array}{c} Y_\varphi \\ \Big\downarrow \\ X \end{array}$ points rat de Y_φ $\to$ ext.

vérifier que Y_φ a des points rat.

Hilbert 90.

pureté C_n $\Longrightarrow$ Grünwald

$X_i \hookrightarrow$ 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. P donne l'extension voulue.

Méthode d'E. Noether

Si elle fonctionne, donne ext. génériques.

Autre méthode : méthode de "rigidité" :

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

Thomson : $M = F_1$ "Monstre" 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 rationelles

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

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

<u>Théorème</u> (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 ∞).

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

voir exposé Bourbaki.

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

engendrent s/g $H \subsetneq G$

$\downarrow$

quotients simples . Voir atlas

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

$\mathbb{C}(T)$

Groupe fondamental libre ~~de~~ à 2 générateurs

$$\begin{array}{c} E \\ \downarrow G \\ \mathbb{P}_1/\mathbb{C} \end{array}$$

unique, à isomorphisme unique près.

Variantes (Matzat).

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

Matzat fait intervenir le groupe des tresses.

Groupes sporadiques: connus, sauf M_{23}.

Groupes non sporadiques

$PSL_2(\mathbb{F}_p)$ $\quad p \equiv$?

$G_2(\mathbb{F}_p)$ $\quad$ (Thomson)

Industrie des $\mathrm{Tr}(x^2)$:

groupes de centre d'ordre 2.

E.g. $\tilde{A}_n$ $\quad$ Vila $\quad n \equiv$? (8)

Mestre en général.

Exemples d'extensions de bas degré

$n = 2$

K car $\neq 2$

$$\begin{array}{ccc} \mathbb{P}_1 & & x \\ \downarrow & & \downarrow \\ \mathbb{P}_1 & & x^2 = T \end{array}$$

$\{0, \infty\}$ - ram.

$K(\sqrt{T})$ corps si T non carré

$$\begin{array}{ccc} \mathbb{G}_m & & x \\ \downarrow & & \downarrow \\ \mathbb{G}_m & & x^2 \end{array}$$

Cyclique d'ordre 3 $\quad C_3$

$C_3 \hookrightarrow GL_2$

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

C_3 agit sur $\mathbb{P}_1$

$$\begin{array}{c} \mathbb{P}_1 \\ \downarrow \\ \mathbb{P}_1 = \mathbb{P}_1 / C_3 \end{array}$$

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

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

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

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

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

Comment montre-t-on que c'est générique ?

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

$$\begin{array}{c} \mathbb{P}_1 = Y \\ \downarrow \\ \mathbb{P}_1 = X \end{array} \qquad \begin{array}{c} E \\ | \\ K \end{array} \text{ cubique cyclique}$$

$$C_K \xrightarrow{\varphi_E} C_3$$

On tord $Y = \mathbb{P}_1$ par φ_E.

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

$$\varphi_E \in H^1(G_K, GL_2) = 0 \quad \text{Hilbert 90.}$$

$$\downarrow$$

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

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

Autre démonstration : Y_{φ_E} a des points rationnels sur une extension de degré impair. Par Springer, Y_{φ_E} a des points rationnels.

Extensions cycliques de degré 4.

K $\qquad K_2 = K(\sqrt{\varepsilon})$, $\varepsilon \in K^*$ non carré.

car $\neq 2$

Existe-t-il K_4 tel que

$$C_4 \left(\begin{array}{c} K_4 \\ | \\ K_2 \\ | \\ K \end{array} \right. ?$$

Décrire les K_4 possibles.

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

<u>Théorème</u> K_4 est cyclique de $d^o 4$ sur K
$\Longleftrightarrow$ $\exists c \in K^*$ avec $a^2 - \varepsilon b^2 = \varepsilon c^2$.

<u>Corollaire :</u> K_4 existe $\Longleftrightarrow$ $a^2 - \varepsilon b^2 - \varepsilon c^2 = 0$ a solutions

$\Longleftrightarrow (\varepsilon, \varepsilon) = 0$ dans $Br_2(K)$.

$$\begin{array}{c} (\varepsilon,\varepsilon) \\ \| \\ (-1, \varepsilon) \end{array}$$

$\Longleftrightarrow$ ε est somme de 2 carrés

$$\begin{tikzcd} & C_4 \arrow[d] \\ G_K \arrow[r, "\varepsilon"] \arrow[ur, dashed] & C_2 \end{tikzcd} \quad \text{surj.}$$

$$0 \to C_2 \to C_4 \to C_2 \to 0$$
$$\mathbb{Z}/2\mathbb{Z} \qquad \mathbb{Z}/4\mathbb{Z}$$

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

$$\underset{\varepsilon}{\Psi} \qquad\qquad \underset{Br_2(K)}{\parallel}$$

$$\delta\varepsilon = 0 \ ? \quad \in Br_2(K)$$

Pour tout groupe G, on a

$$\delta x = xx \quad x \in H^1.$$

(cas particulier de formules sur les carrés de Steenrod)

$$G = \mathbb{Z}/2\mathbb{Z} \qquad H^1(G) = \mathbb{Z}/2\mathbb{Z} \qquad x \overset{\delta}{\mapsto} xx$$

$$H^2(G) = \mathbb{Z}/2\mathbb{Z}$$

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

Entraine que c'est vrai pour tout G

$$x \in H^1(G)$$

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

"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 $\varepsilon : G \to C_2$ surjectif

Soit H le noyau, $(G : H) = 2$.

$G = G_K$, $H = G_{K_2}$.

Soit $\chi : H \to C_2$. Soit $H_\chi = \operatorname{Ker} \chi$.

Théorème : Pour que H_χ soit invariant dans G à quotient $\cong C_4$ il faut et il suffit que $\operatorname{Cor}_H^G \chi = \varepsilon$ dans $H^1(G)$

$\varepsilon \in H^1(G) = \operatorname{Hom}(G, \mathbb{Z}/2\mathbb{Z})$

$\chi \in H^1(H) = \operatorname{Hom}(H, -)$

$$\operatorname{Cor}_H^G : H^1(H) \to H^1(G)$$

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

Ver_H^G = transfert

Application : $G = G_K$, $H^1(G) = K^*/K^{*2}$

$H = G_{K_2}$ $H^1(H) = K_2^*/K_2^{*2}$

$$\operatorname{Cor}_H^G : K_2^*/K_2^{*2} \longrightarrow K^*/K^{*2}$$

$\parallel$

norme $N_{K_2/K}$.

$\chi \in H^1(H)$ corr. à $a + b\sqrt{\varepsilon}$

$\varepsilon \in H^1(G) \longleftrightarrow \varepsilon \in K^*/K^{*2}$

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

Même genre de question en car 2 :

$K_2 = K(x)$ $\quad \wp x = x^2 + x$
$\quad \wp x = \varepsilon \quad \varepsilon \in K$

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

K_4 cyclique de $d^o 4$?

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

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

Cor = trace

$$Tr(a+bx) \equiv \varepsilon \mod \wp K$$

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

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

Serre, 16/1/89

Compléments sur les extensions cycliques de degré 4

$$\begin{array}{l} K_4 = K_2\left(\sqrt{a+b\sqrt{\varepsilon}}\right) \\ \quad | \\ K_2 = K\left(\sqrt{\varepsilon}\right) \\ \quad | \\ K \end{array}$$

cyclique de degré 4

$$\Updownarrow$$

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

$\varepsilon \neq 0$ és. alg. gal. $\quad \sigma \quad c$

$c \neq 0$ $\quad \sigma^{-1} \quad -c$

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

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

$$\begin{tikzcd} & C_8 \arrow[d] \\ \mathrm{Gal}(\bar{K}/K) \arrow[ur, "?"] \arrow[r, "\text{sur.}"'] & C_4 \end{tikzcd}$$

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

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

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

Aute méthode pour obtenir une famille dlextensions cycliques de degré 4 :

$C_4 \subset PGL_2(\mathbb{Q})$

$$\begin{array}{c} \mathbb{P}_1 \\ \big| \, C_4 \\ \mathbb{P}_1/C_4 = \mathbb{P}_1 \end{array}$$

Famille dlextensions 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 $(-1, a) = 0$).

<u>Exercice</u> : Si $\sqrt{-1} \notin K$, car $K \neq 2$, il n'existe pas dlextension générique à 1 paramètre de groupe C_4.

Théorème de Scholz - Reichardt

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

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

$\mathrm{ram}(L/\mathbb{Q})$ = ens. des p ramifiés dans $L/\mathbb{Q}$.

Soit N un entier.

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

1 $\quad p \equiv 1 \pmod{\ell^N}$

2 $\quad$ 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

$I_v \subset D_v \subset G$ $\quad$ inertie et déc.

2 : $\quad I_v = D_v$

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

$$\Updownarrow$$

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

$$\Updownarrow$$

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

Théorème principal :

Soit $1 \to C_\ell \to \tilde{G} \to G \to 1$

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.

$$x^{\ell^N} = 1 \quad \text{pour tout } x \in \tilde{G}.$$

Théorème :

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

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

Corollaire :

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

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 :

$$\begin{tikzcd}
 & LK \\
K \arrow[ur, dash] & L_\phi \arrow[u, dash] \\
\mathbb{Q} \arrow[u, dash] \arrow[ur, dash] &
\end{tikzcd}$$

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

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.) $\phi = \varprojlim (\to \phi_m \to \phi_{m-1} \to)$, (dénombrable)

ϕ_i finis, flèches surjectives.

Si $\phi = \mathrm{Gal}(L/K)$, 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 $\mathrm{Gal}(\overline{\mathbb{C}(T)}/\mathbb{C}(T))$ 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 : $\iff \exists N$ 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

$$1 \to \underbrace{C_\ell}_{\text{cyclique d'ordre } \ell,} \to \phi_n \to \phi_{n-1} \to 1$$

ℓ^N : exponent des Φ_n

$$\Phi_n \left(\begin{array}{c} L_{n+1} \\ | \\ L_n \end{array} \right. \qquad (S_N)$$

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

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

Démonstration du théorème de Scholz-Reichardt :

$$1 \longrightarrow C_\ell \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$$

N t.q. $\exp(\tilde{G})$ divise ℓ^N.

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

Construire $\tilde{L}$?

<u>1^er cas</u> $\tilde{G} = G \times C_\ell$

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

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

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

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

Conditions sur q :

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

q totalement décomposé dans $L/\mathbb{Q}$

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

$$\Updownarrow$$

q est totalement décomposé dans

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

L,

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

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

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

où $\ell^n = |G|$.

<u>Lemme standard</u> :

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 $q = \dfrac{1}{[F:\mathbb{Q}]}$.

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

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

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 $p \equiv 1\ (n)$.

Soit q un nombre premier totalement décomposé dans $L(\sqrt[\ell]{1}, \sqrt[\ell]{p_1}, \dots, \sqrt[\ell]{p_k})$.

Alors il existe un homomorphisme surjectif

$$\chi : (\mathbb{Z}/q\mathbb{Z})^* \longrightarrow C_\ell$$

(car $q \equiv 1 \ (\ell^N)$)

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

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

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

$\mathrm{Gal}(\tilde{L}/\mathbb{Q}) = \tilde{G} = G \times C_\ell$.

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

Vérifions (S_N) pour $\tilde{L}$:

Si $p \in \mathrm{ram}(L/\mathbb{Q})$, on a $p \equiv 1 \ (\ell^N)$.

$\tilde{D}_p = D_p \times 1$ car p est décomposé
$\tilde{I}_p = I_p \times 1$ dans $E/\mathbb{Q}$.

Frob_p dans $E = \chi(p) \in C_\ell$

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

- condition pour q : $q \equiv 1 \pmod{\ell^N}$

$\tilde{D}_q = 1 \times C_\ell$ car q est tot. déc. dans $L/\mathbb{Q}$.

$\tilde{I}_q = 1 \times C_\ell$

2ème cas :

L'extension

$$1 \to C_\ell \to \tilde{G} \to G \to 1 \quad (*)$$

est non triviale.

Problème de plongement $(*)$ définit $e \in H^2(G, C_\ell)$.

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

$$\begin{tikzcd} & \tilde{G} \arrow[dr] & \\ G_\mathbb{Q} \arrow[ur, "\tilde{\varphi}?"] \arrow[rr, "\varphi"'] & & G \end{tikzcd}$$

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

$$\varphi^* : H^2(G, C_\ell) \to H^2(G_\mathbb{Q}, C_\ell).$$

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

$H^i(G_K, C) =: H^i(K, C)$

(K corps, $G_K = \mathrm{Gal}(\bar{K}/K)$)

car $K = 0$

Théorème :

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

Alors l'homomorphisme

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

est injectif.

Idée de la démonstration :

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

$$\begin{array}{c} K' \\ | \\ K \end{array} \quad \text{ext. de degré premier à } \ell$$

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

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

$C = \mu_\ell$. $\quad H^2(K, \mu_\ell) = Br_\ell(K)$.

Mais on sait que

$$Br_\ell(K) \longrightarrow \prod_v Br_\ell(K_v)$$

est injective.

En fait, $Br(K) \to \prod_v Br(K_v)$ est injective.

Théorème de Brauer - Hasse - Noether (?)

Il en existe plusieurs démonstrations.

(voir par ex. Weil : dém. analytique, utilise fct zéta).

L'énoncé est <u>faux</u> pour C_8 !

mais vrai pour C_4, et C_N, N impair.

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

a) p non ramifié : évident

$$\begin{tikzcd} & & \tilde{G} \arrow[d] \\ G_{\mathbb{Q}_p} \arrow[r] & \hat{\mathbb{Z}} \arrow[ur] \arrow[r] & G \end{tikzcd}$$

b.) p ramifié :

$(S_N) \Longrightarrow$ obstruction nulle.

$$\begin{tikzcd} & \pi^{-1}(D_p) \arrow[d] & \subset \tilde{G} \arrow[d, "\pi"] \\ G_{\mathbb{Q}_p} \arrow[r, "\varphi_p"'] & D_p & \subset G \\ & I_p \arrow[u, equal] & \end{tikzcd}$$

ramification modérée car $(p, \ell) = 1$

puisque $p \equiv 1 \ (\ell^N)$, $N \geq 1$.

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 ℓ^N.

$\mathbb{Q}_p$ contient μ_{ℓ^N} (car $p \equiv 1$ (ℓ^N)).

<u>Lemme :</u>

Soit K un corps, $\mu_n \subset K$, $(n, \operatorname{car} K) = 1$.

Soit

$$1 \to C \to A \to B \to 1$$

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

Kummer :

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

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

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 $\operatorname{ram}(\tilde{L}/\mathbb{Q}) = \operatorname{ram}(L/\mathbb{Q})$

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

Lemme :

Pour tout p premier, soit

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

Supposons que $\varepsilon_p(\text{inertie en } p) = 1$ pour presque tout p. Alors il existe $\varepsilon : G_{\mathbb{Q}} \to C$ tel que pour tout p, $\varepsilon | G_{\mathbb{Q}_p} = \varepsilon_p$ 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

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

$p_i^{n_i}$ conducteur de ε (———)

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

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

Proposition:

Soit $1 \to C \to \tilde{\Phi} \to \Phi \to 1$

une suite exacte de groupes finis,

$C \subset$ centre de $\tilde{\Phi}$.

Soit $\varphi : G_{\mathbb{Q}} \to \Phi$ un homomorphisme

relevable en un homomorphisme dans $\tilde{\Phi}$.

Soit $\tilde{\varphi}_p : G_{\mathbb{Q}_p} \to \tilde{\Phi}$ relevant φ_p.

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

On choisit un relèvement $\psi : G_{\mathbb{Q}} \to \tilde{\Phi}$.

Soit ψ_p la restriction de ψ à $G_{\mathbb{Q}_p}$.

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

t.q. $\psi_p = \varepsilon_p \tilde{\varphi}_p$. Par le lemme on obtient un ε global. Alors $\tilde{\varphi} = \varepsilon^{-1}\psi$ convient.

Conclusion de la $2^{\text{ème}}$ étape:

$$\begin{tikzcd} & \tilde{G} \arrow[d] \\ G_{\mathbb{Q}} \arrow[ur] \arrow[r] & G \end{tikzcd}$$

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

Condition de Scholz :

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

$D_p = I_p$? pas nécessairement.

$$\begin{array}{ccccc} \tilde{I}_p & \subset & \tilde{D}_p & \subset & \tilde{G} \\ & & & & \downarrow \\ I_p & = & D_p & \subset & G \end{array}$$

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

$\tilde{I}_p \underset{\ell}{\subset} \tilde{D}_p$.

Il faut modifier l'extension.

La $3^{\text{ème}}$ étape utilisera Cebotarev dans $L(\sqrt[\ell^N]{1}, \sqrt[\ell]{p_i})$.

23/1/89

ℓ, $N \geq 1$, $\ell \neq 2$.

$$1 \to C_\ell \to \tilde{G} \to G \to 1$$

G ℓ-groupe, C_ℓ cyclique d'ordre ℓ

$$\tilde{G}\left(\begin{array}{l}\tilde{L}\\ \mid C_\ell \\ L \\ \mid G \\ K\end{array}\right. \quad \text{condition } (S_N)$$

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

On peut construire un $\tilde{L}$ avec
$ram(\tilde{L}/\mathbb{Q}) = ram(L/\mathbb{Q})$
(qui ne satisfait pas à priori à la condition (S_N))

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

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

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

$$\begin{array}{lcl} \ell^{\alpha+1} & \pi^{-1}(I_p) \subset \tilde{G} & \\ & \downarrow \quad\quad \downarrow \pi & \\ \text{d'ordre } \ell^\alpha & I_p = D_p \subset G & \end{array}$$

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

$$\begin{array}{c} \tilde{I}_p \subset \tilde{D}_p \subset \pi^{-1}(I_p) \subset \tilde{G} \\ \downarrow \\ I_p \end{array}$$

puisque $\pi^{-1}(I_p)$ 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).

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

$$\downarrow$$

$$I_p$$

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

$$\tilde{I}_p \xrightarrow{\sim} I_p \qquad \pi^{-1}(I_p) = C_\ell \times \tilde{I}_p$$

$$\mathrm{Frob}_p \in \tilde{D}_p / \tilde{I}_p \hookrightarrow C_\ell$$

$$p \in S \longmapsto c_p \in C_\ell$$

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

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

On peut supposer $c_1 \neq 1 \in C_\ell$

Soit $c_i = c_1^{\nu_i} \qquad 0 \leq \nu_i \leq \ell - 1$

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

1. $q \equiv 1 \pmod{\ell^N}$
2. q totalement décomposé dans L
3. q pas totalement décomposé dans $\mathbb{Q}(\sqrt[\ell]{1}, \sqrt[\ell]{p_1})$.

(4) q totalement décomposé dans

$$\mathbb{Q}(\sqrt[\ell]{1}, \sqrt[\ell]{p_i/p_1^{\nu_i}}).$$

c'est ici que $\ell \neq 2$ est important !

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

F cyclique de degré ℓ^{N-1}.

On demande donc décomposition totale de q ds

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

et dans L

comportement prescrit dans

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

Lemme : Les corps F, L et $\mathbb{Q}(\sqrt[\ell]{1}, \sqrt[\ell]{p}, p \in S\}$ 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 un ℓ-groupe.

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

(b) $\Longleftarrow$ (c) :

(c) Le groupe de Galois de

$H = \mathbb{Q}(\sqrt[\ell]{1}, \sqrt[\ell]{p}, p \in S)$ n'a aucun quotient

d'ordre une puissance de ℓ, à part $\ell^0 = 1$

(ceci est faux si $\ell = 2$)

$$\begin{array}{c} H \\ | \\ \mathbb{Q}(\sqrt[\ell]{1}) \\ | \\ \mathbb{Q} \end{array}$$

Gal(groupe de Galois $(\ell, \dots, \ell)$ k fois

$\mathbb{F}_\ell^*$

$\mathrm{Gal}(H/\mathbb{Q})$ est produit direct de $\mathbb{F}_\ell^*$

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

action de $\mathbb{F}_\ell^*$ sur $\mathrm{Gal}(H/\mathbb{Q}(\sqrt[\ell]{1}))$

est par homothétie.

$\mathbb{F}_\ell^* \neq \{1\}$ si $\ell \neq 2$.

Donc $\mathrm{Gal}(H/\mathbb{Q})$ n'a aucun quotient

d'ordre ℓ. D'où (c).

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

q totalement décomposé dans F et L

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

$H/\mathbb{Q}(\sqrt[\ell]{1})$ = composé de $\mathbb{Q}(\sqrt[\ell]{1}, \sqrt[\ell]{p_1})$

et de $\mathbb{Q}(\sqrt[\ell]{1}, \sqrt[\ell]{p_i / p_1^{\nu_i}})$ $i \geq 2$

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

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

Il existe un caractère surjectif

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

ramifié seulement en q.

correspond à

$$\begin{array}{c} \mathbb{Q}(\sqrt[q]{1}) \\ | \\ ? \\ | \\ \mathbb{Q} \end{array} \quad \text{cyclique de degré } \ell$$

On peut parler de $\varepsilon(\mathrm{Frob}_{p_i})$, notés $\varepsilon(p_1), \dots, \varepsilon(p_k) \in C_\ell$.

On a $\begin{cases} \varepsilon(p_i) = \varepsilon(p_1)^{\nu_i} & i = 2, \dots, k \\ \varepsilon(p_1) \neq 1 \end{cases}$

(4) $\Longleftrightarrow$ $p_i / p_1^{\nu_i}$ est une puissance ℓ ième mod q.

D'où la 1ère formule

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

$\Updownarrow$

$\varepsilon(p_1) \neq 1$

On peut remplacer ε par une puissance (d'ordre premier à ℓ) on peut supposer

$\varepsilon(p_1) = c_1 \in C_\ell \Rightarrow \varepsilon(p_i) = c_i$ pour tout i

On "tord" par ε^{-1}

$$\begin{tikzcd} & C_\ell \arrow[d, phantom, "\cap"] \\ G_{\mathbb{Q}} \arrow[ur, "\varepsilon"] \arrow[r, "\varphi_{\tilde{\Sigma}}"'] & \tilde{\Sigma} \end{tikzcd}$$

$$\varphi_{\tilde{\Sigma}}\, \varepsilon^{-1} : G_{\mathbb{Q}} \to \tilde{G} .$$

condition (S_N) est satisfaite

Intermède sur groupes finis

Sous-groupe de Frattini d'un groupe fini :

G groupe fini, le s/g de Frattini de G est $\phi(G) = \bigcap\limits_{\substack{H \\ \text{maximal}}} H$ (maximal ds G : parmi les s/g propres de G)

Si H est un s/g de G tel que $H . \phi(G) = G$, alors $H = G$.

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

$\Updownarrow$

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

Si 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, p168 vol I)
Soit G un groupe fini, et soit H un s/g distingué de G, avec

$$G \supset H \supset \Phi(G)$$

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

$\Updownarrow$

$\iff$ 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.

$\prod_p S_p \to G$ on 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 $g \in G$, gSg^{-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 $tgSg^{-1}t^{-1} = S$. Autrement dit,

$tg \in N_G(S)$. D'où $G = S\,\Phi(G) N_G(S)$

$g = t^{-1}tg$ $= \Phi(G) N_G(S)$

$\Longrightarrow N_G(S) = G$

<u>Théorème (Ore)</u> : 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)

$G \supset \Phi(G)$, $G/\Phi(G)$ résoluble $\neq \{1\}$

Si $|G|>1$, alors $G \neq \Phi(G)$.

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

Soit $N \subset G$ avec $N \supset \Phi(G)$,
$N/\Phi(G) = A$. Par le thm précédent
N est nilpotent et distingué ds G.
N n'est pas contenu dans $\Phi(G)$.
Il existe un s/g 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 $N \not\subset R$.

Énoncé (Ishanov) :

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

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

Alors le problème de plongement pour $(*)$ est résoluble. Autrement dit, il existe $\tilde{L} \supset L$, $\tilde{L}$ Galoisienne sur K,

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

$$\begin{array}{l} \tilde{L} \\ \big| \ \text{nilpotent } N \\ L \\ \big| \ G \\ K \end{array}$$

Théorème (Shafarevicz)

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 $|G| \neq 1$, par le théorème précédent

$G \simeq$ qt de $N \rtimes R$, R résoluble d'ordre $< |G|$.

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

Énoncé $\Rightarrow$ il existe $L_1 \supset L_0 \supset K$ avec $\mathrm{Gal}(L_1/K) \simeq N \rtimes R$

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 $\begin{array}{c} N' \rtimes G \\ \downarrow \text{sur} \\ N \rtimes G \end{array}$).

$$G' \left(\begin{array}{l} L' \\ | \\ L \\ |\, G \\ K \end{array} \right.$$

N nilpotent

$G' \xrightarrow{\text{sur}} G$

$N \rtimes G' \xrightarrow{\text{sur}} N \rtimes G$

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

On peut supposer que $L \supset \mu_n$

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

Soit p totalement décomposé dans $L/\mathbb{Q}$, premier à n.

$p_1, \dots, p_k$ tot. déc. ...

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

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

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

$$(s v_i)(x_j) = 0$$

sauf si $s = 1$ et $i = j$, auquel cas $s v_i (x_j) = 1$.

$$\begin{array}{cc} v_1 & v_2 \\ {\scriptstyle s}\downarrow & \\ s v_1 & s v_2 \end{array}$$

$$\tilde{L} = L\left(\sqrt[n]{s x_1}, \dots, \sqrt[n]{s x_k}, \ s \in G\right)$$

répond à la question.

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

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

$$1 \to N \to \mathrm{Gal}(\tilde{L}/K) \to G \to 1$$

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

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

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 Hilbert.

30/1/89

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

V var. alg. $/K$ irréductible, réduite

$K(V)$: corps de fonctions

Si K est algébriquement fermé dans $K(V)$

$$\Updownarrow$$

V absolument irréductible

$$\Updownarrow$$

$V/\bar{K}$ irréductible

~~$V(K)$~~ $K(V)/K$ est dite régulière

$$\begin{array}{c} L'^{gal} \\ | \\ L' \\ |\ \text{finie} \\ L \\ |\ \text{régulière} \\ K \end{array} \qquad \text{régulière}$$

L'^{gal} : clôture alg. de L'/K

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

Par exemple:

$$\begin{array}{c} \mathbb{Q}(\mu_3, \sqrt[3]{T}) \\ | \\ \mathbb{Q}(\sqrt[3]{T}) \\ | \\ \mathbb{Q}(T) \\ | \\ \mathbb{Q} \end{array}$$

V est dite <u>K-rationnelle</u> si: $K(V)$ est une extension transcendante pure de K.

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

V birat. isom. /K à $\mathbb{P}_n$, 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.

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

$$\begin{array}{c} \mathbb{P}_n \quad \text{appl. rat.} \\ \vdots \\ \downarrow \\ V \end{array}$$

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

$\mathbb{P}_n \dashrightarrow$ génériquement surjectif quitte à restreindre à ouverts conv., morphisme fini

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

V est stablement K-rationnelle $\Longleftrightarrow$
$\exists n$ 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 $L = K(X_1, \dots, X_n)^G$.

$$\begin{array}{c} Y = \mathbb{A}^n \\ \downarrow \\ Y/G = X \end{array}$$

G opère sur Y

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 ? (stablement K-rationnelle suffirait pour entraîner l'existence d'ext. gal. de $\mathbb{Q}$ de groupe de Galois G).

"Lemme sans nom" :

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

$X = Y/G$.

K Y

G opère sur Y

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

Revêtement étale, galoisienne

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

V espace vect. $/K$ de dim finie n

On obtient fibré vectoriel $\mathcal{V}$ sur X :

$$\begin{array}{ccc}(V\times Y)/G & = & \mathcal{V} \\ & & \downarrow \\ & & X\end{array}$$

est un fibré vectoriel localement trivial

Descente des faisceaux.

$$\begin{array}{c}\mathcal{O}_Y \otimes V \\ \downarrow \\ Y\end{array}$$ 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 $V_1\times(V_2/G)$

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

Corollaire 1 :

Si V_2/G est K-rationnelle, il en est de même de V/G, où $V_? = V_1 \oplus V_2$.

Corollaire 2 :

Si 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 tout K)

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

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

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

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

Représentation de d° 4 de G donnée par $\mathbb{H}_\mathbb{Q}$

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

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 $\mathrm{Nrd} \neq 0$.

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

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

variété $\mathbb{Q}$-rationnelle ??

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

$$\begin{array}{c} \mathbb{H}^*_{\mathbb{Q}} / \{\pm 1\} \\ \wr\wr \\ SO_3 \times \mathbb{G}_m \end{array} \qquad x^2 + y^2 + z^2$$

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

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

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

$r_q = 1 \Rightarrow q$ = cte

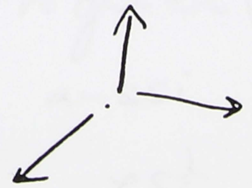
$\Rightarrow \lambda^2 = 1 \Rightarrow \lambda = \pm 1$.

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

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

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 : $(Ox\ ,\ Oxy)$

(ou drapeau complet : $(O, Ox, Oxy, Oxyz)$)

Fixateur de ce drapeau dans SO_3 est D.

<u>Drap</u> : variété des drapeaux

$$SO_3/D \xrightarrow[\text{birat. isom.}]{} \underline{\text{Drap}} \qquad \dim 3$$

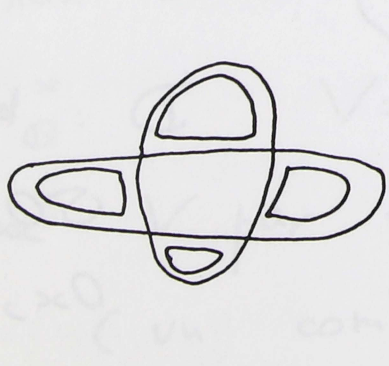
(T lisse, connexe, dim n

G de dim n opère sur T, $t \in T$

$\mathrm{Fix}_G t = D \qquad G/D \to T$ isom. birat (car $=0$!))

<u>Drap</u> est rationnelle.

<u>Réf</u> : Quaternion extensions, C. Jensen, N. Yui
Alg. Geom. and Comm. Alg. 1987, 155–182



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

$$0 < \varepsilon < 0{,}72$$

$G \qquad K$

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

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

de groupe G, qui soit régulière sur K

$$\begin{array}{ccc} L & & Y \\ | & & \downarrow \\ K(T) & & \mathbb{P}_1 \end{array}$$

courbe abs. irréd. lisse, projective, avec action fidèle de G,

$Y/G \simeq \mathbb{P}_1$.

Théorème d'irréductibilité de Hilbert

$\Downarrow$

$\mathrm{Gal}_{K(T)}$, 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.

<u>Théorème</u> : 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. $\mathrm{Gal}_{K(T)}$ est vrai)

$$\begin{array}{c} Y \\ \downarrow \\ \mathbb{P}_n \end{array}$$ rev. (ramifié)

$Y/G \simeq \mathbb{P}_n$

On applique le thm de Bertini :

$\mathcal{G}$ = grassmannienne des droites de $\mathbb{P}_n$

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

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

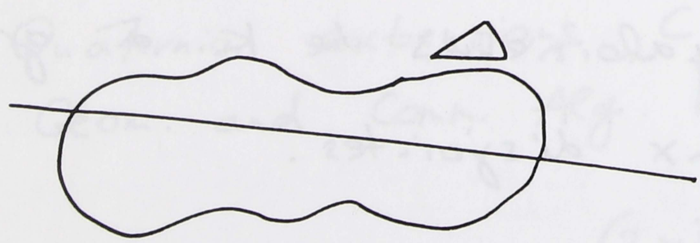
(Hartshorne, p. 179

$Y \longrightarrow \mathbb{P}_n$, image de dim ≥ 2 abs. irréd.)

Construction explicite de U :

$$
\begin{array}{c}
Y \\
\downarrow \\
\mathbb{P}_n
\end{array}
$$

Δ hypersurface de $\mathbb{P}_n$, lieu de ramification (réduite).



Les droites coupant transversalement Δ en des points lisses forment un ouvert U de $\mathcal{G}$, dense.

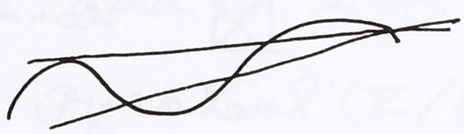
U convient.

$$\begin{tikzcd} \pi_1(\mathbb{P}_2 - \Delta, \cdots) \arrow[r, "\text{sur}"] & G \\ \pi_1(D_2 - \Delta \cap D_2) \arrow[u] \arrow[ur, "\text{sur ?}"'] & \end{tikzcd}$$

vrai pour dte générique

aussi pour droites voisines

<u>Exemple</u>.



Δ : quartique non sing $\subset \mathbb{P}_2$

Plan double ramifié le long de Δ.

$$t^2 = \phi(x, y, z) \qquad \phi : \text{équation de } \Delta.$$

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

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

φ sect. de L. On définit rev. ramifié le long de φ comme suit :

$$\underbrace{t}_{\text{sect. de } M}{}^2 = \underbrace{\varphi}_{\text{sect. de } L}$$

4 pts distincts $\to$ courbe elliptique

3 " " de genre 0

28 bitangentes $\to$  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

 donnent chacune 4 bitangentes !

$4+6\cdot 4=28$.

(si $\varepsilon>\frac{9}{8}$ pas de points réels)

= 2 coniques imag.

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

Problème :

Démontrer ceci.

Exercice :

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

Théorème : Un groupe abélien fini a la propriété Gal_T.

Utilisation des tores :

Un tore S est un K-groupe algébrique qui est $\bar{K}$-isom. à un produit de $\mathbb{G}_m$.

Groupe des caractères de S :

$$X(S) = \hat{S} = \mathrm{Hom}_{\bar{K}}(S, \mathbb{G}_m)$$

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

Groupe $Y(S) = \mathbb{Z}$-dual de $X(S)$
$= \mathrm{Hom}_{\bar{K}}(\mathbb{G}_m, S)$
("s/g" à un paramètre de S)

Certains sont K-rationnels :

Tore déployé : isom. à un produit de $\mathbb{G}_m$
$\Longleftrightarrow$ 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. fini où opère G

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

Décomposons I en orbites de G_K

$\Longrightarrow$ 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 s/g ouvert de G_K

H correspond à ext.

$$\begin{array}{c} L \\ | \\ K \end{array} = \text{s/corps de } \overline{K} \text{ fixé par } H$$

$S_I = \underline{L^*}$ vu comme groupe alg. $/K$

$= R_{L/K}\, \mathbb{G}_m$ (Weil)

$= \prod_{L/K} \mathbb{G}_m$ (Grothendieck)

S_I est K-rationnelle.

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

Lemme de Shapiro :

$H^1(K, S_I) = H^1(L, \mathbb{G}_m) = 0$ (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

$$0 \to A \to S \to S' \to 0$$

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

<u>Théorème</u> :

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).

<u>Corollaire</u> :

A a la propriété Gal_T.

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

<u>Démonstration</u> :

Suite exacte de tores $\to$ ste exacte des caractères.

$$0 \to M \to S \to S' \to 0$$

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

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

$M^\vee$: dual de Cartier de M

$= \mathrm{Hom}_{\bar{K}}(M, \mu_{\bar{K}})$.

$$0 \to Y(S) \to Y(S') \to \tilde{M} \to 0$$

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

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

$H \subset G_K$ $\quad \bigoplus \mathbb{Z}[G_K/H] \to \tilde{A}$

opère triv.

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 $\tilde{G} = A \rtimes G$.
Si G a la propriété $\mathrm{Gal}_{K(T)}$, il en est de même de $\tilde{G}$.

Principe de la construction :

$$\begin{array}{ccc} Y & & Y \\ \downarrow G & & \downarrow G \quad \text{fini, étale} \\ \mathbb{P}_1 & & X \quad \text{ouvert de } \mathbb{P}_1 \\ & & \neq \emptyset \end{array} \qquad /K$$

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

On peut supposer A induit, i.e.

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

$$A = \underbrace{B \times \cdots \times B}_{G}$$

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

On choisit un tore S contenant B :

$$0 \to B \to S \to S' \to 0 \qquad S, S' \text{ tores}$$

S' quasi-trivial

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

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

$$0 \to A \to \Sigma \to \Sigma' \to 0 \qquad \Sigma' = S' \times \cdots \times S'$$

$Y \times \Sigma$, action de $\tilde{G} = A \rtimes G$ (G opère). 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 s/g abélien bicyclique.

$Br_{nr}(V/G) \simeq$ {groupe des α tués par les s/g bicycliques}

Exemple (Saltman)

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

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

extension centrale

inv. évidents:

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

hom. $\varphi_G : V \to U$

$\varphi_G = 0 \iff x^p = 1$ pour $\forall\, x \in G$

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

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

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

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

$$1 \to \Lambda^2 V \to \tilde{G} \to V \to 1 \qquad \begin{cases} \varphi = 0 \\ \psi = id \end{cases}$$

$\tilde{G} = \{ (v,x) \quad v \in V,\ x \in \Lambda^2 V$

$(v,x)(v',x') = (v+v', x+x'+\frac{1}{2} v \wedge v') \}$

(signe ?)

On choisit $X \subset \Lambda^2 V$, X cyclique d'ordre p indécomposable : 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 $G = \tilde{G}/X$

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

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

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

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

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

$$H^1(\ , \mathbb{Q}/\mathbb{Z}) \to H^2(\ \ ) \to H^2(\ \ ) \to H^2(\ \ )$$

$$\alpha \longmapsto 0$$

alors $\exists\, \theta : G \to \mathbb{Q}/\mathbb{Z}$ dont α est l'image extensions obtenues :

$$
\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] & \mathbb{Z}/p^2\mathbb{Z} \arrow[r] \arrow[dr] & \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d, "\theta"] & 0 \\
& & & \mathbb{Q}/\mathbb{Z} &
\end{tikzcd}
$$

On aurait des éléments d'ordre p^2.

α restr. aux s/g bicycliques abéliens de G est 0.

Soit B bicyclique abélien dans G.

Soit B_V l'image de B dans V.

On a $rg(B_V) \leq 1$.

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

$\mathrm{Ker}\, \psi_G = X$.

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 ≤ 1 (donc cyclique).

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

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

$0 \to X \to \tilde{B} \to B \to 0$ est décomposée

Donc $\tilde{B}$ est extension scindée de B

$\Longleftrightarrow$ $\alpha | B = 0$.

Exemple minimal obtenu ainsi:

$|V| = p^4$, $|V/X| = p^5$, $|G| = p^9$

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

Fin d'une démonstration

K corps, $\begin{array}{c} Y \\ \downarrow G \\ \mathbb{P}_1 \end{array}$ $/K$

A groupe abélien fini où opère G,

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

<u>Théorème</u> : Si G a la propriété $\mathrm{Gal}_{K(T)}$, il en est de même de $\tilde{G}$.

$$0 \to A \to S \to S' \to 0$$

S, S' tores $/\mathbb{Q}$

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

On a vu que l'on pouvait supposer $A = \bigoplus_{g \in G} gB$

B groupe abélien:

On écrit $A = B \oplus \cdots \oplus B$ indexé par G

changement de notation:

$$0 \to B \to S \to S' \to 0 \quad , \; B \subset S(Q)$$

S' quasi-trivial

$$0 \to A \to \Sigma \to \Sigma' \to 0 \qquad \Sigma = S \times \cdots \times S$$

$$\Sigma' = S' \times \cdots \times S'$$

$$\begin{array}{c} Y \\ \downarrow G \\ \mathbb{P}_1 / K \end{array}$$

$Y \times \Sigma$ action de $\tilde{G}$: sur Y par $\tilde{G} \to G$

sur Σ : A agit par translations

G en permutant les facteurs.

A voir:

$$\begin{array}{c} Y \times \Sigma \\ \downarrow \\ Y \times \Sigma / \tilde{G} \end{array}$$

variété rationnelle

Plusieurs étapes:

$$\begin{tikzcd} Y \times \Sigma \arrow[dr, "A"] \arrow[dd] & & \\ & Y \times \Sigma' \arrow[r] \arrow[dl, "G"] & Y \arrow[d] \\ X = Y \times \Sigma / \tilde{G} \arrow[rr] & & \mathbb{P}_1 \end{tikzcd}$$

$$\begin{array}{c} Y \\ \downarrow G \\ \mathbb{P}_1 \end{array}$$

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

$$\begin{array}{c} X \\ \downarrow \\ \mathbb{P}_1 \end{array}$$

fibré à fibres le groupe Σ'.

Ce fibré X est birationellement un produit.

Fibre au pt. gén. $\to \alpha \in H^1(K(T), \Sigma')$

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

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

Il aurait été plus naturel de montrer que

$$\begin{array}{c} Y \\ \downarrow G \\ X \end{array} \text{ se plonge dans } \begin{array}{c} \tilde{Y} \\ \downarrow \tilde{G} \\ X \end{array}, \text{ mais}$$

la démonstration ne parait pas marcher.

Théorème d'irréductibilité de Hilbert

K corps, $\begin{array}{c} Y \\ \downarrow \text{fini} \\ X \end{array}$ $\begin{array}{c} Y(K) \\ \downarrow \\ X(K) \end{array}$ "image petite" en général.

Par exemple, $K = \mathbb{F}_q$ $\begin{array}{c} Y \\ \downarrow \\ X \end{array}$ quadratique

Y, X (courbes) abs. irréd.

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

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

On a une involution de Y, $y \mapsto y'$

y, y' ont m̂ image ds X. Donc $|\pi Y(\mathbb{F}_q)| \sim \frac{1}{2} q$.

Définitions :

K corps de caract. 0

V var. irréd. $/K$. $V(K)$: pts rat. de V

$A \subset V(K)$, A est de "type C_1" s'il existe une sous-variété $W \subset V$, W fermée $\neq V$ $(\dim W < \dim V)$, 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 irréd. de W ne s'applique birat. sur V (pas de section générique)

Définition :

$A \subset V(K)$ est dit <u>mince</u> 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)

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

$L \subset K(V)$, $K \underset{\text{fini}}{\overset{\subset}{\neq}} L$

Si normal, $L \subset \mathcal{O}_v \quad \forall v \in V$.

Supposons V absolument irréductible.

Définitions :

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 ≥ 1 qui a la propriété de Hilbert
2. $\mathbb{P}_1$ a la propriété de Hilbert
3. Toute variété K-rationelle a la propriété de Hilbert.

(2) $\Rightarrow$ (1) ok ...

(1) $\Rightarrow$ (2) ?

La propriété de Hilbert est birationelle : Si V a la propr. H, toute var. birat. $\sim V$ l'a aussi.

F Z-fermé, $\neq V$, $V - F$ a H.

réunion d'ensembles minces est mince.

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

$$\begin{tikzcd} W_V \arrow[r] \arrow[d] & W \ni w \arrow[d] \\ \varphi : V \arrow[r] & \mathrm{Aff}' \end{tikzcd}$$ carré cartésien

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

1er cas ("cas favorable") $W_V \to V$ 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 :

$$\begin{tikzcd} & W \arrow[d] \\ V \arrow[r, "\varphi"'] & \mathrm{Aff}^1 \end{tikzcd}$$

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" : $K(V)$

$\begin{array}{c} V \\ \downarrow \\ V_L \\ \downarrow \\ \mathrm{Aff}^1 \end{array}$ (birat.)

$K(V)$ | extension régulière
L
| fini
$K(T)$ — $K(W_\alpha)$

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

~~$\mathbb{\#}$~~ $\mathbb{P}_1$

Deux extensions régulières de $K(T)$ dont les lieux de ramification sont disjointes, 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 tt corps de car 0.

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

(plus préc. les a, b, $a+bT \in A$ ne sont pas Z-denses 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. finie

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 $\prod_{L/K} = R_{L/K}$ restriction des scalaires.

V quasi-projective.

L-variétés $\longrightarrow$ K-variétés

Adjoint à droite du foncteur extension des scalaires :

W/L $\qquad \mathrm{Hom}_L(W, V_{/L}) = \mathrm{Hom}_K$

T K-variété, W L-variété

$$\mathrm{Hom}_K(T, R_{L/K} W) = \mathrm{Hom}_L(T_{/L}, W)$$

e.g. $T = \mathrm{Spec}\, K$

$(R_{L/K} W)(K) = W(L)$

Weil : descente à partir de $\prod_{\sigma : L \to \bar{K}} W^\sigma$

$$\begin{array}{c} W \\ \downarrow \pi \\ V_{/L} \end{array} \qquad A \subset \pi(W(L))$$

$$\begin{tikzcd} X \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & R_{L/K} W \arrow[d] \\ V \arrow[r, "\Delta"] & R_{L/K} V_L \end{tikzcd}$$

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

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

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

Il reste à vérifier que $\begin{matrix} X \\ \downarrow \\ V \end{matrix}$ n'a pas de section au pt. générique.

Se vérifie : $V \xrightarrow{\Delta} \begin{matrix} W_1 \times \cdots W \times \cdots W_n \\ \downarrow \\ V \times \cdots \times V \end{matrix}$ non trivial rev. de degré m

rev. induits sur la diag. sont de degré $\geq m$.

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 :

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

$$\begin{tikzcd} & L\mathbb{Q}_{quad} & \\ \mathbb{Q}_{quad} \arrow[ur, no head] & & \\ & & L \arrow[uul, no head] \\ \mathbb{Q} \arrow[uu, no head] \arrow[urr, no head, "A_5"'] & & \end{tikzcd}$$

sauf erreur, $L\mathbb{Q}_{quad}$ est hilbertien.

<u>Thm</u> : Soit A une partie mince de $\mathbb{P}_n(K)$. Soit $d \geq 1$, et soit Grass_n^d la Grassmannienne des d-plans de $\mathbb{P}_n$. Alors il existe un Z-ouvert dense $U \subset \mathrm{Grass}_n^d$ 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.

<u>Corollaire</u> :

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

$$\begin{array}{c} W \\ \downarrow \\ \mathbb{P}_n \end{array} \qquad A \subset \pi(W(K))$$

Bertini : il existe U t.q. si $u \in U$ la restriction de W à D_u n'a pas de section au point générique.

<u>Corollaire</u>

$\mathbb{P}_1$ a la propriété de Hilbert $\Rightarrow$ $\mathbb{P}_n$ a la propriété de Hilbert

$\Leftarrow$ est aussi vrai (déjà vu).

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

Approximation faible (affaiblie) $\Rightarrow$ Théorème d'irréductibilité de Hilbert.

<u>Interprétation</u> de la propriété de Hilbert (conséquences)

G groupe fini op. sur W librement

$$\begin{array}{c} W \\ \downarrow \\ V = W/G \end{array}$$

Morphisme étale, galoisien

On suppose W quasi-projectif.

$P \in V(K) \longmapsto$ groupe de décomposition de P (défini à conj. près)

On choisit un point fermé $Q \to P$

corps résiduel $K(Q)/K = K(P)$

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

= groupe de décomposition.

On choisit un $\overline{K}$-point $\tilde{P} \to P$

$D_{\tilde{P}}$ 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.

<u>Thm</u> (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

<u>Thm</u> 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

$$\begin{array}{c} W/H \\ \pi_H \downarrow \\ V \end{array} \quad \text{degré } [G:H] \geq 2$$

W irréd.

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

$W/H(K)$?

$x \in W(\bar{K})$ $\quad \sigma x \in Hx \quad \sigma \in Gal_{\bar{K}/K}$.

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

$Irr(P)$ donne L_P/K Galoisienne 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 $P \in V(L)$ n'ayant pas la propriété $Irr(P)$ rel. 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'.

Serre 27/12/89 (81)

Théorème d'irréductibilité de Hilbert (suite)

Erratum dans un des détails d'une preuve (si G réal sur $\mathbb{R}$, $G \times L$ aussi)
"tore" construit = <u>forme tordue</u> de celui qu'on avait annoncé

Interprétation en termes de polynômes des ensembles minces.

V/K K car 0 V abs^t irréduct (quasi-proj.)

$A \subset V(K)$ mince si non Zariski-dense

si $\begin{array}{c} W \\ \pi\downarrow \\ V \end{array}$ abst irred, $\dim W = \dim V$, π génériq^t surject de degré ≥ 2

$\pi(W(K))$ mince ds $V(K)$

$K(V)$

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

polyn. de degré n, $a_i \in K(V)$

irréduct

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

Soit A l'ensemble des $t \in V(K)$ tels que,

ou bien $a_i \notin \mathcal{O}_t$ 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 $W \subset V \times \mathrm{Aff}^1$ $\quad W : (t, x) /$
$0 = x^n + a_1(t)x^{n-1} + \dots + a_n(t)$

$$\begin{array}{c} W \\ \downarrow \pi \\ V \end{array}$$ π étale finie de degré n

$$\begin{array}{c} W^{gal} \\ \downarrow \\ W \\ \downarrow \\ V \end{array}$$

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

Remarque: $K(W) \big/ K(V)$ monogène donc défini par un polynôme (à ens. Z. dense).

$W \to V$ 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'enlever les pôles de a_1

$n = 2$ $a(t)$ non carré $X^2 - a$

$n = 3$ $\left\{ \begin{array}{l} a_i \text{ pas de pôles} \\ \Delta \text{ inv, non carré} \\ X^3 + \dots \text{ pas de solution ds } K \end{array} \right.$

cf pour $n = 4, 5 \dots$ (cours sur "Mordell-Weil").

K corps de nombres

On va voir le rapport avec l'approximation faible (Ekedahl 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 localt compact.

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

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

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

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 $\sqrt[3]{\frac{\rho}{T}}$ si $K \not\ni \sqrt[3]{1}$ $K_\pi = K(\sqrt[3]{1})$

si v non déc.

si v non décomp, $W(K_v) \simeq V(K_v)$

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

d'où $x_1 \in \prod V(K_v)$ - adhér de A_1

. $S_0 \cup S_1, A_2 \longrightarrow S_2$

d'où x_2

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

* si $A \subset W(K)$, $W \overset{\text{fermé}}{\subset} V$, $W \neq V$

par le thme 1, pour Nv grand, il existe $x \in V(K_v) - W(K_v)$. Un tel $x \notin v$-adhérence de A. Donc $S = \{v\}$ pour presque tt v convient.

* W avec hyp. habituelles

$$\begin{array}{c} W \\ \downarrow \\ V \end{array} \quad A \subset \pi W(K).$$

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

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 $x \notin$ adh de A.

Σ_π est infini (Cebotarev).

Approximation faible

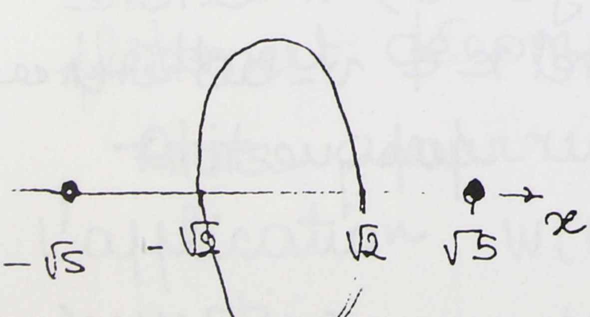
(AF_S) V S partie finie de Σ_K
V a la propriété d'approximation vis à vis de S si $V(K)$ dense dans $\prod_{v \in S} V(K_v)$.

Théorème si V et V' sont lisses et birat^t isom., alors V possède (AF_S) ssi V' aussi.

Cne. ex si non lisse: $y^2 = (x^2-5)^2(2-x^2)$ / $\mathbb{R}$

2 bir ég

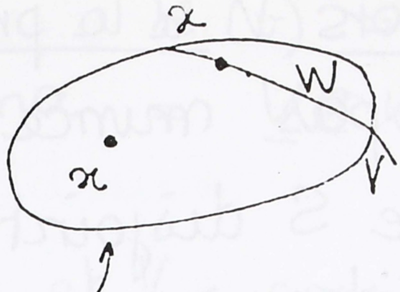
$y^2 = 2 - x^2$



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

$V' = V - W$ | W fermé ds V, $W \neq V$

$V \Rightarrow V - W$ trivial



pour $x \notin W$ évident

$V - W \Rightarrow V$

$x \in W(K_v)$

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

(localt revient à esp affine - ss-variété).

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

(AF~~A~~) (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 affaiblie

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

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

Mais tous les tores satisfont (AFA).

par ex : S_0 = places ramifiées ds L/K où le tore se déploie (suffit celles où $G_v \neq$ cycl.) ultramétriques gal

Ref : Voskresenski ....

Théorème. Soit V une variété abs^{lt} irréduct satisfaisant (AFA). Alors V a la propriété de Hilbert ($V(K)$ n'est pas mince).

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 $V = (\mathrm{Aff}^n/G)^{\text{lisse}}$

V est K unirationnelle $\overset{?}{\to}$ AFA $\to$ Hilbert

Reste à démontrer les théorèmes 1 et 2. On le fait par réduction modulo v.

$\mathcal{O}_K$ anneau des entiers de K

$\underline{V}$ schéma de type fini sur $\mathcal{O}_K[\frac{1}{d}]$, $d \in \mathcal{O}_K, \neq 0$, plat.

$$\underline{V} \underset{\mathcal{O}_K[\frac{1}{d}]}{\otimes} K \simeq V$$

Σ places de K ; $\Sigma_d = \{v \in \Sigma, \text{ non arch}, v \nmid d\}$

$v \in \Sigma_d \longleftrightarrow \mathfrak{P}_v$ idéal premier de $\mathcal{O}_K[\frac{1}{d}]$

$\kappa(v)$ = corps résiduel, de card Nv

$\underline{V}_v$ schéma $= \underline{V} \otimes \kappa(v) :=$ réduction mod $\left\{\begin{matrix}\mathfrak{P}_v \\ v\end{matrix}\right.$ de $\underline{V}$ (et de "V").

& si $\underline{V}_1$ et $\underline{V}_2$ conviennent, on a $\underline{V}_{1,v} \simeq \underline{V}_{2,v}$ pour presque tout v.

Thme (Lang-Weil) : Supposons V abst irréductible de dimension n. On a alors

$$|\underline{V}(\kappa(v))| = Nv^n + \underline{O}(Nv^{n-\frac{1}{2}}).$$

La dém consistait à se ramener au cas des courbes. Pour une courbe de genre g (OPS proj lisse) la contribution de $V'_{\text{bir}} \sim V^{*}$ donne chgt par $O(Nv^{n-1})$ et alors $|V| = Nv + \underbrace{1-a}_{\text{est Weil}}$. On se ramène à courbe en fibrant.

Maintenant $N = \sum \pm (\lambda)$
vap de Frobenius

$|\lambda| = Nv^{m/2} \quad 0 \leq m \leq 2n$

$\underline{V}$ abst irred $\Leftrightarrow$ 1 seule val. λ tq $|\lambda| = Nv^n$, $\lambda = Nv^n$

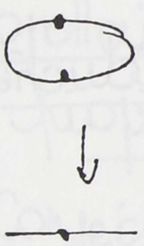
(dim cohom. l-adique des V_v sont bornées).
Ceci donne des bornes numériques précises (Bombieri).

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

$\square$ vient de ce que $\underline{\tilde{W}} \to \underline{V}$ étale fini.

Alors si $\pi(K(v))$ n'est pas surjectif, il en est de même de $\pi(K_v)$.



$$\begin{tikzcd} \underline{W}^{gal} \arrow[d, "H"'] & \\ \underline{W} \arrow[d, "\pi"] & \sim N v^n \\ \underline{V} & \sim N v^n \end{tikzcd} \qquad G$$

Lemme : $\exists\, c<1$ telle que, si Nv assez grand, et $v \in \Sigma_\pi$

$$|\pi \underline{W}(K(v))| \leq c N v^n + O(N v^{n-\frac{1}{2}})$$

(vrai avec $c = 1 - \frac{1}{m!}$, $m = \deg \pi$)

Remarque : si galoisien, $c = \frac{1}{m}$

G/H $(G:H) = m = \deg \pi$

$\underline{W}(K(v)) = A \cup B$ $\quad$ A pts relevables dans $\underline{W}^{gal}$. B = autres

$$|A| + |B| = N v^n + \underline{O}$$

$$|\pi(B)| \leq |B|$$

$$|\pi(A)| \leq ?$$

$\left\{\begin{array}{l} Nv \text{ grand} \\ v \end{array}\right.$ se décompose complètement dans K_π, donc $\underline{W}^{gal}/K(v)$ est $\cup$ de $e\,(=[K_\pi : k])$ composantes absolument irréductibles de dimension n

$$|W^{gal}(K(v))| = e\,(Nv)^n + \underline{O} \quad \text{(Lang-Weil)}$$

On en déduit

$$|A| = \frac{e}{|H|} N v^n + \underline{O}$$

$$|\pi(A)| = \frac{e}{|G|} N v^n + O$$

$$|\pi(A)| + |\pi(B)| \leq |B| + \frac{e}{|G|} N v^n + O$$

$$\leq \frac{e N v^n}{|G|} + N v^n \left(1 - \frac{e}{|H|}\right) + \underline{O}$$

$$\leq N v^n \left(1 + \frac{e}{|G|} - \frac{e}{|H|}\right) + \underline{O}$$

$$\leq N v^n \left(1 - \frac{1}{|G|}\right) + \underline{O}$$

$$|G| \leq m!$$

Ceci démontre le théorème 2.

Remarque : On a utilisé en dernier ressort le fait que Aff^n a la prop. AF. On donnera d'autres dém (plus effectives) en utilisant le grand crible. La dém de Hilbert est typiquement archimédienne (réf : Cours sur Mordell Weil).

Jeudi 6.3.89

91

Théorème du grand crible

Il permet de donner une bonne estimation de la taille des ensembles minces :

Th Soit $A \subset \mathbb{Q}^n$ mince. Alors pour $N \to \infty$, le nombre des $a \in A \cap \mathbb{Z}^n$ de taille $|a| \leq N$, est $O(N^{n-\frac{1}{2}} \log N)$

On ne connaît pas d'ex où le log soit nécessaire.
Mais si $a = (a_1, \dots, a_n)$, $a_1 \square$, on tombe sur $n - \frac{1}{2}$.

On va se limiter à $\mathbb{Z}^n$ 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 $\nu_p \in \mathbb{R}$ avec $0 < \nu_p \leq 1$
tel que $|A_p| \leq \nu_p p^n$, A_p = image de A dans $\mathbb{Z}^n_{/p\mathbb{Z}^n}$
(ν_p est la proportion de classes mod p atteintes).

Enoncé Pour tout ~~entier~~ $D \geq 1$, on a

$$|A| \leq 2^n \sup(N, D^2)^n / L(D),$$

où
$$L(D) = \sum_{\substack{q \text{ saf} \\ q \leq D}} \prod_{p \mid q} \frac{1 - \nu_p}{\nu_p}$$

$$\left(L(D) \geq 1 + \sum_{\substack{p \text{ 1}^{\text{er}} \\ p \leq D}} \frac{1 - \nu_p}{\nu_p} \right)$$

Si En choisissant $D = N^{1/2}$ $\quad |A| \leq (2N)^n / L(N^{1/2})$.

Exemples

(a) $\nu_p = \frac{1}{2}$ pour tout p

$$L(D) = \sum_{\substack{q \leq D \\ q \text{ sqf}}} \frac{1}{\nu_q} \asymp D$$

$$|A| << N^{n-\frac{1}{2}}$$

"grand crible".

$L'(D) \sim \frac{D}{\log D}$ on perd un peu $|A| << N^{n-\frac{1}{2}} \log N$!

(b) "petit crible", on jette peu à chaque fois, type Eratosthène. $\nu_p = 1 - \frac{1}{p}$ par ex.

$L'(D) \sim \log\log D$ $\qquad |A| << \frac{N}{\log\log N}$

$L(D) \sim \log D$ $\qquad |A| << \frac{N}{\log N}$.

Montgomery – Vaughan : Dans tout intervalle de longueur N, il y a au plus $2\frac{N}{\log N}$ nombres premiers.

"Les nombres premiers ne s'accumulent pas trop".

Démonstration – $\mathbb{Z}$ = groupe des caractères du cercle.

$\Lambda = \mathbb{Z}^n$ = groupe des caractères de $T = \mathbb{R}^n / \mathbb{Z}^n$.

Si $a = (a_1, \dots, a_n) \in \mathbb{R}^n$ $\qquad \chi_a(x_1, \dots, x_n) = \exp(2\pi i \sum a_i x_i)$

$a \in \Lambda \mapsto \chi_a$ caractère sur T.

$A \longmapsto \varphi = \varphi_A = \sum_{a \in A} \chi_a$ fonction sur T.

Alors Λ = groupe des car. de T, $\Lambda/p\Lambda$ est le groupe

des caractères du noyau de $p : T \to T$
$$T[p]$$

On traduit en termes de restriction à $T[p]$ les renseignements sur A_p :

La rest de φ à $T[p]$ ne fait intervenir que $\nu_p\, p^n$ 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 : fction de Dirac ⟷ rep régulière ⟷ ts les ~~car~~ carach. (oscille bcp)

constante ⟷ 1 car.

Théorème Soit C_i $(i = 1, \dots, h)$ des groupes abéliens finis

$C = \pi C_i$ $\quad \hat{C}_i =$ dual de C_i $\quad \hat{C} = \pi \hat{C}_i$.

$\Omega_i \subset \hat{C}_i$ $\quad \nu_i = \dfrac{|\Omega_i|}{|C_i|}$.

Soit φ une fonction complexe sur C, φ combinaison linéaire des caractères appartenant à $\Omega = \pi \Omega_i$.

Alors
$$\sum_{\substack{x \text{ primitif} \\ x \in C}} |\varphi(x)|^2 \geq |\varphi(0)|^2 \prod_{i=1}^{h} \frac{1 - \nu_i}{\nu_i}$$

$x = (x_1, \dots, x_h) \in C$ $\quad x$ primitif si $x_i \neq 0$ pour tout i.

Démonstration : Pour $h = 1$

$$\varphi = \sum_{\chi \in \Omega} c_\chi \chi$$

$$|\varphi(0)|^2 \leq \sum |c_x|^2 \sum_{x\in\Omega} 1 \leq \sum |c_x|^2 \cdot \nu_1 |C_1|$$ (14)

Cauchy-Schw.

$$\sum |c_x|^2 = \frac{1}{|C_1|} \sum_{x\in C_1} |\varphi(x)|^2$$

$$\leq \nu_1 \left\{ |\varphi(0)|^2 + \sum_{x \text{ primitif}} |\varphi(x)|^2 \right\}$$

$$(1-\nu_1)|\varphi(0)|^2 \leq \nu_1 \sum_{x \text{ primitif}} |\varphi(x)|^2.$$

Récurrence sur h:

Si $x \in C_h$, on note φ_x la fonction $(x_1,\dots,x_{h-1}) \mapsto \varphi(x_1,\dots,x_{h-1},x)$

sur $C_1 \times\dots\times C_{h-1}$.

$$\sum_{(x_1,\dots,x_{h-1}) \text{ prim.}} |\varphi(x_1,\dots,x_{h-1},x)|^2 \geq |\varphi(0,\dots,0,x)|^2 \times \prod_{i=1}^{h-1} \frac{1-\nu_i}{\nu_i}$$

$$\sum_{x \text{ primitif}} |\varphi(x)|^2 \geq \prod_{i=1}^{h-1} \frac{1-\nu_i}{\nu_i} \sum_{x\neq 0} |\varphi(0,0,\dots,0,x)|^2$$

$\geq$ ce qu'on veut avec le cas $h=1$.

Ici $\varphi(0) = |A|$. On peut relier cela à la valeur sur des points de division ; ces points si suffisamment bien répartis.

<u>Théorème</u> (Davenport. Halberstam) Soit

a) une fonction φ sur T, qui soit combinaison linéaire de caract. χ_λ, où $\lambda \in C$, cube de côté N

$\varphi = \sum c_\lambda(\varphi)\chi_\lambda$.

b) $\delta > 0$ et $x_i \in T$, δ-espacés ($|x_i - x_j| \geq \delta$, $i \neq j$)

Alors $\sum_i |\varphi(x_i)|^2 \leq 2^m \sup\left(N, \frac{1}{\delta}\right)^m \|\varphi\|_2^2$

$$\|\varphi\|_2^2 = \int_T |\varphi(x)|^2 dx = \sum_{\lambda \in C} |C_\lambda(\varphi)|^2 \quad (95)$$

Remarque $\quad |t| = \inf_{\substack{x \in \mathbb{R}^n \\ x \to t}} |x| \qquad |x| = \sup(|x_1| \ldots |x_n|).$

$t \in T.$

Ces théorèmes entraînent l'inégalité du grand crible.

$$\varphi = \sum_{a \in A} \chi_a$$

On va appliquer D.H avec $X = \bigcup_{\substack{q \text{ sqf} \\ q \leq D}} T[q]$.

Ces points sont δ-espacés avec $\delta = \frac{1}{D^2}$.

$$\sum_{x \in X} |\varphi(x)|^2 \leq 2^n \sup(N, D^2)^n \|\varphi\|_2^2.$$

$$\|\varphi\|_2^2 = \sum_{a \in A} 1^2 = |A|.$$

d'où

$$\boxed{\sum_{x \in X} |\varphi(x)|^2 \leq 2^n \sup(N, D^2)\, |A|}.$$

On va appliquer le lemme sur les groupes finis

$$T[q] = \prod_{p|q} T[p]$$

X_q = élts de X d'ordre égal à q

= pts primitifs de $T[q]$.

$$\sum_{x \in X_q} |\varphi(x)|^2 \geq \frac{|\varphi(0)|^2}{|A|^2} \times \prod_p \frac{1-\nu_p}{\nu_p}$$

d'où $\quad \boxed{L(D)\,|A|^2 \leq \sum_{x \in X} |\varphi(x)|^2}$

Démonstration de DH :

ⓐ Si $\delta > \frac{1}{2}$ $|x-y| < \delta$ pour tout $x, y \in T$.

Dans ce cas : il y a au plus un x_i (si aucun c'est trivial).

On applique Cauchy-Schwarz à

$$\varphi(x) = \sum c_\lambda(\varphi)\chi_\lambda$$

$$|\varphi(x)|^2 \leq \|\varphi\|_2^2 (N+1)^n.$$

or $N+1 \leq 2N$ ...

ⓑ $\delta \leq \frac{1}{2}$

On fabrique une fonction auxiliaire

On construit une fonction continue θ sur $\mathbb{R}^n$ à support ds $|x| \leq \frac{1}{2}\delta$

/ Transf de Fourier est en val absolue ≥ 1 sur C.

/ $\|\theta\|_2^2 \leq 2^n M^n$ $M = \sup(N, \frac{1}{\delta})$.

Soit λ le centre du cube C.

On prend $\theta(x) = \chi_\lambda(x)\, M^n \prod_{i=1}^{n} 2\cos(\pi M x_i)$ si $|x_i| \leq \frac{1}{2M}$ $\forall i$.

$= 0$ sinon

Sur $\mathbb{R}$ fonction type $\theta_0 = \begin{cases} 2\cos \pi x & \text{si } |x| \leq \frac{1}{2} \\ 0 & \text{sinon.} \end{cases}$

$$|\hat{\theta}_0(y)| \geq 1 \quad \text{si } |y| < \frac{1}{2}$$

$$\int |\theta_0(x)|^2 dx = 2$$

car $\hat{\theta}_0(y) = \frac{1}{2\pi} \frac{\cos \pi y}{\frac{1}{4} - y^2}$

On identifie θ à une fonction sur T. (97)

$\mathbb{R}^n \longrightarrow T$

$\theta \, dx_1 .. dx_n$

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 ici $|c_\lambda(\theta)| \geq 1$ si $\lambda \in \Lambda \cap C$.

Soit $g = \sum_{\lambda \in \Lambda \cap C} \frac{c_\lambda(\varphi)}{c_\lambda(\theta)} \chi_\lambda$.

$c_\lambda(g) \cdot c_\lambda(\theta) = c_\lambda(\varphi)$ pour tout $\lambda \in \Lambda$.

Donc $\varphi = g * \theta$.

$$\varphi(x_i) = \int_T \theta(x_i - x) \, g(x) \, dx$$

$$= \int_{B_i} \theta(x_i - x) \, g(x) \, dx$$

$B_i = \{x, |x - x_i| < \frac{1}{2}\delta\}$

$$|\varphi(x_i)|^2 \underset{\text{Cauchy-Sc.}}{\leq} \int_{\bar{B}_i} |\theta(x_i - x)|^2 dx \times \int_{\bar{B}_i} |g(x)|^2 dx$$

$$\leq 2^n M^n \times \int_{B_i} |g(x)|^2 dx$$

les B_i ne se rencontrent pas (x_i δ-espacés !)

$$\sum |\varphi(x_i)|^2 \leq 2^n M^n \int_T |g(x)|^2 dx.$$

$$\leq 2^n M^n \sum_{\lambda \in \Lambda \cap C} |c_\lambda(g)|^2 \leq (2\pi)^n \sum_{\lambda \in \Lambda \cap C} |c_\lambda(\varphi)|^2$$

$$\leq (2\pi)^n \|\varphi\|_2^2$$

l'application aux ens. minces est dû à S.D. Cohen (L.M.S ~1982).

nombres premiers jumeaux $\nu_p = 1 - \frac{2}{p}$.

On doit éliminer $n \equiv 0$ ou $-2 \bmod p$.

1 —— N $\quad p \leq N^{1/2}$ $\quad \nu_2 = \frac{1}{2}$

0, $-2 \bmod p$ refusé.

Nbres premiers jumeaux entre $N^{1/2}$ et N sont ds ce qui reste et leur nombre en $\leq N$ est $O(N/(\log N)^2)$.

$$\sum_{p \text{ jumeau}} \frac{1}{p} \text{ converge.}$$

Application aux ensembles minces d'entiers.

A ens mince $\subset \mathbb{Z}^n$. (mince ds $\mathbb{A}^n(\mathbb{Q})$)

A_N = pts de A dans un cube de côté N.

Th (Cohen) $|A_N| \ll N^{n-\frac{1}{2}} \log N$ pour $N \to \infty$

le $\log N$ est remplaçable par $(\log N)^\gamma$, $\gamma = \gamma(A) < 1$.

Preuve 1er type $(x_1, \dots, x_n) \in \mathbb{Z}^n$ satisf. à

$\phi(x_1, \dots, x_n) = 0$ $\quad \phi \neq 0$.

Pour ceux-là maj. en N^{n-1}. $\quad n=2$ $\quad \phi = 0$.

2e type correspond aux $x = (x_1, \dots, x_n)$ tels qu'une équation $a_0(x) X^m + \dots + a_m(x) = 0$, $a_i(x)$ polynᵐ 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 s/ens de $\mathbb{F}_p^n$ où $X^m + a_1(x) X^{m-1} + \dots + a_m(x) =$
mod p a une solution mod p.

$$W \xrightarrow{\pi} \mathbb{A}_{\pi}^{n}$$

On a vu qu'il existe une extension finie de $\mathbb{Q}$, $K_\pi / \mathbb{Q}$ telle que si p décomp compl. ds K_π, alors $\pi(W(\mathbb{F}_p)) \leq c\, p^n$ avec $c > 1$, p grand.

Dans le théorème du crible, on prend $\nu_p = c$ $(c<1)$ pour tout p premier décomp. compl. ds K_π, assez grand, $\nu_p = 1$ pour les autres.

$$L(D) = 1 + \sum_{\substack{p \text{ } 1^{er} \\ \leq D}} \frac{1-\nu_p}{\nu_p} = 1 + \sum_{\substack{p \text{ grand} \leq D \\ \text{déc. compl} \\ \text{ds } K_\pi}} \frac{1-c}{c}$$

$$\gg \frac{D}{\log D}$$

On obtient ainsi la majoration en $N^{n-\frac{1}{2}} \log N$.

On peut calculer $L(D)$ (cf cours sur Mordell) :

$$L(D) \gg \frac{D}{(\log D)^{\gamma}}, \quad \gamma < 1.$$

$V \subset \mathbb{P}_r / \mathbb{Q}$ On a une notion de hauteur

$$x = (x_0, \dots, x_r) \qquad H(x) = \sup |x_i|$$

les x_i étant choisis dans $\mathbb{Z}$ et premiers entre eux.

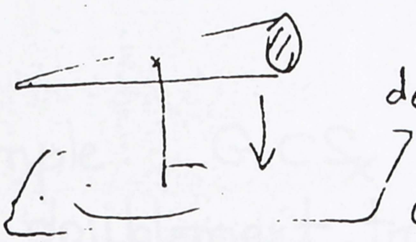
$\mathcal{N}_V(N) = \{$ Nbre de points de $V(\mathbb{Q})$ avec $H(x) \leq N \}$, $N \to \infty$

V variété linéaire de dim. d

$X_V(N) \sim c N^{d+1}$ $d \geq 1$

Théorème <u>si</u> V est de dimension $d \geq 1$ et irréductible et non linéaire

$X_V(N) \ll N^{d+\frac{1}{2}} \log N$



degré $\neq 1$, image mince

Conjecture $\ll N^{d} (\log N)^{\alpha}$ pour un α convenable.

Exemple V surface cubique dans $\mathbb{P}_3$

$d = 2$

$X_V(N) \ll N^{2+\frac{1}{2}} (\log N)$

Si V contient une droite rationnelle $/\mathbb{Q}$, les points rationnels sur $\mathbb{Q}$ fournissent N^2.

cf conj Manin : si on enlève les droites, $N^2 \log \ldots$

Serre 13/3/89 (101)

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 préfèrera
S_X = groupe des permutations de X, X ens. 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 ($|Y_i| \geq 2$, $k \geq 2$).

$(Y_i) \Leftrightarrow R$

$$\begin{array}{c} G \circlearrowright X \\ \downarrow \\ G \circlearrowright X/R = \{1, \dots, k\} \end{array}$$

G imprimitif $\Leftrightarrow$ existence d'un quotient non trivial pour l'espace homogène X.

G primitif: "non imprimitif".

$X = G/H$ H fixateur d'un point.

$X/R \leftrightarrow H'$ avec $G \underset{\neq}{\supset} H' \underset{\neq}{\supset} H$.

G primitif sur $X \Leftrightarrow$ fixateur d'un pt H est un ss-gpe maximal de G

$$G \overset{L}{|} \searrow L^H \quad H \underset{\neq}{\subset} G$$
$$K^n$$

$n = (G : H)$

H max ds $G \Leftrightarrow$ pas de corps (ð.) 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 doublt 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 $x_1, \dots, x_m$.
Sinon $Y_1 \cup \dots \cup Y_k$ partition non triviale stable par G. Il y a un cycle s d'ordre premier p ne stabilisant pas Y_1. QPS $sY_1 = Y_2$, $sY_2 = Y_3, \dots$
les éléments de $Y_1 \cup \dots \cup Y_p$ ne sont pas fixés par s donc au plus p points donc $|Y_1| \leq 1$ Contradiction

Lemme Soit $G \subset S_X$ transitif primitif.
Tout ss-gpe normal G' de G, $G' \neq \{1\}$ est transitif sur X : ~~Si~~ les 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

ⓐ Si G contient une transposition, $G = S_X$.

ⓑ Si G contient un cycle d'ordre 3, on a : $G = A_X$ ou S_X.

ⓒ Si G contient 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

$|X| = 6$, $A_5 \hookrightarrow S_6$ action sur les 5-Sylows.

(C. Jordan, TI + Traité des Subst...)

Démonstration de ⓐ :

Soit $Y \subset X$ maximale telle que $S_Y \subset G'$

Supposons $Y \neq X$.

$2 \leq |Y| \leq n-1$. $n = |X|$.

Soit G' le s/g de G engendré par les transp. appart. à G, G' est s/g 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 $x \in Y$, $z \notin Y$.

Y, $x \longleftrightarrow z$ $\quad \overline{Y} = Y \cup \{z\}$

$G' \supset S_{\overline{Y}}$.

$S_{\overline{Y}}$ est engendré par S_Y et (xz). Car ce groupe est transitif sur $\overline{Y}$ et il contient S_Y.

Lemme:

$B \subset A$ groupe de permut. trans.

trans.

$B_x \subset A_x$ fixateur de x

Alors $B_x = A_x \Rightarrow B = A$.

Alors $G' \supset S_{\overline{Y}}$ contrairement à la maximalité de Y.

Dém de b)

Soit G' le s/g de G engendré par les cycles d'ordre 3 de G. Alors G' est transitif. Soit $Y \subset X$ maximal tel que $G' \supset A_Y$. Supposons $Y \neq X$. $|Y| \geq 3$. Il existe un cycle $(abc) \in G'$ qui ne stabilise pas Y.

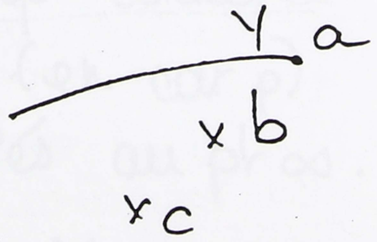
Deux possibilités : $(a,b,c) \cap Y$ a 1 ou 2 élts

1^er cas $\begin{cases} a \text{ et } b \text{ sont dans } Y \\ c \notin Y \end{cases}$

On pose alors $\overline{Y} = Y \cup \{c\}$

On a $A_{\overline{Y}} \subset G'$ car eng par A_Y et $\{a,b,c\}$

2^e cas. $a \in Y$ $b, c \notin Y$



$|Y| \geq 3$ il existe $b', c' \in Y$ tels que a, b', c' tous $\neq$.

Dans le groupe $A_5 = A_{\{a,b,c,b',c'\}}$, (abc) $(a\,b'c') \in G' \cap A_{\overline{5}}$. Or ces deux éléments engendrent le groupe $A_{\overline{5}}$.

Donc $A_5 \subset G'$; en particulier $(b'ab)$

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 $G \supset$ cycle d'ordre p, alors le groupe est $n-\varepsilon(p)$-transitif.

$$\varepsilon(p) = 1 \text{ pour } p=2$$
$$\varepsilon(p) = 2 \text{ pour } p=3.$$

Si $*$transitif, contient donc le A_* correspondant. Alors classif des gpes finis, les $*$transitifs pour $*$ grand et seult A_* ou S_*.

Lemme Soit $G \subset A_n$ transitif contenant A_m, $m > \frac{n}{2}$. Alors $G = A_m$.

Car G primitif et contient un cycle d'ordre 3.

$$\begin{array}{ll} K(Y)^{gal} & \\ \mid & \\ K(Y) & Y \\ \mid m & \downarrow n \\ K(X) & X \end{array} \qquad \begin{array}{l} G \subset S_n \\ \text{transitif} \end{array}$$

Hilbert Exemples d'extension de $\mathbb{Q}(T)$ à groupe de Galois S_n

K = car 0.

$$P(X) = X^n + \alpha_1 X^{n-1} + \cdots + \alpha_n \quad \alpha_i \in K$$

$$\begin{array}{cccc} \infty \in \mathbb{P}_1 & & X & K(X) \\ \downarrow & \downarrow n & \downarrow & \mid \\ \infty & \mathbb{P}_1 & T = P(X) & K(T) \end{array}$$

K(T) adj 1 racine de $X^n + a_1 X^{n-1} + \dots + a_n - T = 0$.

Théorème : Si P est une fonction de Morse, alors le groupe de Galois de la cl. gal. de $K(X)/K(T)$ est S_n.

Fction de Morse : pts critiques quadratiques et valeurs de fction $\neq$.

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.

∞ totalt ramif

les autres pts de ram st les x_i

Corollaire L'ext $K(X)^{gal}/K(T)$ est régulière.

On peut supposer K alg. clos. (car G ne peut que diminuer).

Th ~~(en car 0)~~ : La droite projective est simplt connexe (ie pas de revêt fini étale connexe de degré >1).

Thme (en car 0) La droite proj $\mathbb{P}_1$, privée d'un pt, est simplt connexe

(en car p) idem pour les revêts modérément ramifiés au pt ∞. (gpe d'inertie d'ordre premier à p).

Si

$$\begin{array}{ll} X & \\ \downarrow & \text{rev d'ordre } n \geq 2 \quad \begin{array}{l} \text{nr en dehors de } \infty \\ \text{mod ram à l'}\infty \end{array} \quad e_1, \dots, e_k \\ \mathbb{P}_1 & \qquad\qquad\qquad\qquad \sum e_i = n \end{array}$$

la formule de Hurwitz donne ce qu'on veut.

Revenons en car 0

$$\begin{array}{l} X \\ \downarrow \text{ rev galoisien à gr } G \text{ ramifié en des points} \\ \mathbb{P}_1 \qquad t_1, \dots, t_h \in \mathbb{P}_1(k). \end{array}$$

Soient $C_1, \dots, C_h$ les 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 ssgpe engendré par les conj des C_i $1 \leq i \leq h-1$; G' est normal $\subset G$, d'où un revêtement intermédiaire

$$\begin{array}{l} X \\ \downarrow \\ X/G' \qquad \text{nr en } t_1, \dots, t_{h-1} \text{ donc trivial} \\ \downarrow G/G' \qquad\qquad\qquad G = G'. \\ \mathbb{P}_1 \end{array}$$

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 alors G eng par les conj des C_i $(1 \leq i \leq h-1)$.

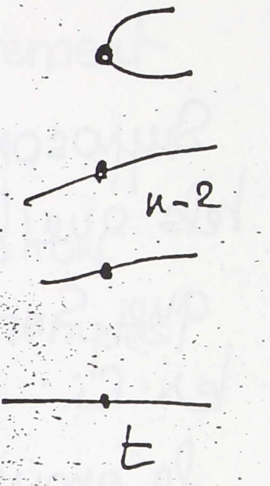
En car 0 : il y a un choix des C_i tq G soit engendré par $C_1, \dots, C_{h-1}$.

A Appliquer au revêtement donné par $P(X) - T = 0$ où P est une fction de Morse de deg n.

G est eng par les conjug des gps d'inertie en des $\{t_i, \infty\}$ $t_i = P(x_i)$ – et même de $n-1$.

$\begin{cases} C_i \text{ est eng. par une transposition pour } i \leq n-1 \ (H_i) \\ C_n \text{ (inertie à l'}\infty\text{) cycle d'ordre } n. \end{cases}$

$$\begin{array}{ccc} & & k(X) \\ K' & & \Big| \ G \quad \text{gal.} \\ & & K(T) \end{array} \qquad K(X) \underset{K}{\otimes} \widehat{K_t} = \prod_{x \to t} \widehat{K(X)}_x \qquad \widehat{K(T)}_t$$



$K(X) \underset{K(T)}{\otimes} \widehat{K(T)}_t =$ ext quad ramif des corps local

x étale de degré $n-2$. : Morse

l'inertie opère 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 $\mathbb{Q}$ (thme d'irréd.).

Valeurs de T pour lesquels on trouve par spécialisation ce qu'on veut.

$$P = X^n - X$$

$$X^n - X - t = 0 \qquad t \in \mathbb{Q},\ t \notin \text{ens mince}$$

est une ext irréd. à groupe S_n.

Fixons $n = 5$ par exemple

$$x^5 - x - t = 0 \qquad \text{mod } p$$

gpe de Galois eng par l'élt de Frob σ_p.

On cherche des val des $t \in \mathbb{F}_p$ et des p, σ_p soit une classe de conj imposée dans G.

$$\sigma_p = (12)(345)\ldots$$

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 s grpe de S_n rencontrant tous les C_i. Alors si $t \in \mathbb{Z}$ $\quad t \equiv t_i \bmod p_i \quad \forall i$ 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 $1 + \bigcup_{g \in G/H} g\{H - \{1\}\}g^{-1} = \bigcup_{g \in G} gHg^{-1}$

$$\left|\bigcup gHg^{-1}\right| \leq 1 + \frac{|G|}{|H|}(|H| - 1) < G \text{ si } \frac{|G|}{|H|} \geq 2.$$

Sans Jordan, énoncé : $G \subset S_X$, $|X| \geq 2$, G transitif, il existe $g \in G$ qui opère sans point fixe.

Autre exemple $X^n - X^{n-1} - T = 0$. (pas de Morse) donne S_n.

On regarde la ramif : cycle d'ordre 2, cycle $nX^{n-1} - (n-1)X^{n-2} = *X^{n-2}(X-c)$ d'ordre $n-1$, cycle d'ordre n (à l'∞).

Si $G \subset S_n$ contient ces élts, il vaut S_n. Car

 transitif et mi dbt transitif (~~ds~~ 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 $\quad \mathbb{P}_{n-1}$ $\quad x=(x_1,\dots,x_n)$

S_n opère par permutation

On va écrire les équations invariantes les + simples

$$\Sigma x_1 = 0$$
$$\Sigma x_1 x_2 = 0$$
etc...
$$\Sigma x_1 \dots x_{n-2} = 0.$$

car 0.
(marche en car p si $p \nmid n$, $p \nmid n-1$).

ou encore
$$\begin{cases} \Sigma x_i = 0 \\ \Sigma x_i^2 = 0 \\ \vdots \\ \Sigma x_i^{n-2} = 0. \end{cases}$$

On obtient une courbe lisse C_n connexe, int. complète, S_n opère dessus ϵ

$$g(C_n) = 1 + (n-2)!\,\frac{n^2-5n+2}{4}$$

$n=3$	0
$n=4$	0
$n=5$	4
$n=6$	49
$\vdots$	

$$C_n/S_n \xrightarrow{\sim} \mathbb{P}_1$$

$$x \longmapsto \frac{\sigma_{n-1}(x)^n}{\sigma_n(x)^{n-1}}$$

$\sigma_{n-1} = \Sigma x_1 \dots x_{n-1}$
$\sigma_n = x_1 \dots x_n$

C_n
$\downarrow$
$C_n/S_{n-1} \simeq \mathbb{P}_1(X)$ $\quad X^n - X^{n-1} = T$
$\downarrow \qquad\qquad \downarrow n$

$n=3 \quad g=0.$ $\quad C_3 \simeq \mathbb{P}_1$ avec action de S_3

$(\subset PGl_2)$

$n=4$ $\quad C_4 \simeq$ conique ss pt (associée aux quaternions)

$(x_1, \dots, x_4) \quad \mathbb{P}_3$

$x_1 + \dots + x_4 = 0 \quad \mathbb{P}_2$

$x_1^2 + \dots + x_4^2 = 0$ conique (ss pt) sur $\mathbb{Q}$

action de S_4 ($\hookrightarrow PGl_2$ tordu de quater.).

$n=5$ $\quad C_5$

$(\quad\quad) \quad \mathbb{P}_4$

$\Sigma x_i = 0 \quad \mathbb{P}_3$

$\begin{cases} \Sigma x_i^2 = 0 \\ \Sigma x_i^3 = 0 \end{cases}$ quad $\cap$ cub $=$ courbe de Bring.

$g=4.$

Action de S_5

$\text{Bring} / S_5 = \mathbb{P}_1$

$\prod (X - x_i) = X^n + \lambda X + \mu$

Bring - Jerrard : Toute équation de d° 5 peut se ramener après ext de racines $\square$ et $\cube$ à $X^5 + \lambda X + \mu = 0$.

K_5 | degré 5 | K $\quad x \in K_5 \quad x \notin K$

$\mathrm{Tr}\, x = 0 \quad \mathrm{Tr}\, x^2 = 0 \quad \mathrm{Tr}\, x^3 = 0$

$K_5 \simeq K \times \dots \times K$ $\quad$ Ces x st un cône sur une courbe de type Bring.

Une telle $\cap$ a un pt rationnels sur une ext de K quad / cub.

quad $\cap$ cub ds $\mathbb{P}_3$.

contient 1 dte (cf. extension)

si dte $\not\subset$ cub, la coupe en 3 pts rationnels sur une ext de degré 3.

Serre 20/3/89

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:

$$\begin{array}{c} E \\ \big|\, S_n \\ \mathbb{Q}(T) \end{array}$$

$C \to \mathbb{P}_1$ ramifiée en 3 pts rat $(0, 1, \infty)$ avec inertie (12), $(12..n-1)$, $(12..n)$

$X^n - X^{n-1} - T = 0$ à peu de choses près

$$\begin{array}{ccc} C & & E \\ \searrow & & \big|\, A_n \\ & C' & E' \\ \swarrow & & \big|\, 2 \\ \mathbb{P}_1 & & \mathbb{Q}(T) \end{array}$$

$Y^2 = \Delta(T)$ (disc. de l'équation précédente)

donc C' courbe de genre 0 avec pt rationnel (les 2 pts de ram le st) donc $\simeq \mathbb{P}_1$

$E' \simeq \mathbb{Q}(T')$.

Le cas de $PSL_2(\mathbb{F}_p)$.

Construction modulaire de K-y Shih.

Pts de division des courbes elliptiques

① c. ell sur $\mathbb{Q}(T)$.

$j(E) = T$ ex (Tate) $Y^2 + XY = X^3 - \frac{36}{T-1728}X - \frac{1}{T-1728}$

l nombre premier $T_l E = \varprojlim E_{l^n}$ $\mathbb{Z}_l$-m libre de rg 2

$E_{l^n} = \operatorname{Ker} l^n : E(\bar{K}) \to E(\bar{K})$

$\rho_l : G_K = \operatorname{Gal}(\bar{K}/K) \longrightarrow GL_2(\mathbb{Z}_l)$

ici $\dashrightarrow\!\!\!\!\to$

cf par ex Weber (T III)

$$G_K \xrightarrow{\rho} Gl_2(\mathbb{Z}_\ell) \xrightarrow{\text{dét}} \mathbb{Z}_\ell^*$$

car cyclotomique χ_ℓ

$G_K \longrightarrow \mathbb{Z}_\ell^*$ surject.

Sur $\mathbb{C}(T)$, image à dét 1, en fait tout $Sl_2(\mathbb{Z}_\ell)$ car image contient (mod ± 1) l'image de $Sl_2(\mathbb{Z})$

$$E_\ell : \quad G_K \longrightarrow Gl_2(\mathbb{F}_\ell) \xrightarrow{\det} \mathbb{F}_\ell^*$$

χ_ℓ car cycl.

$$Sl_2 \begin{cases} L \\ \mid Sl_2 \\ \mathbb{Q}(\zeta_\ell)(T) \\ \mid \mathbb{F}_\ell^* \\ \mathbb{Q}(T) \end{cases}$$

Pas régulière $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}$. $\ell > 2$.

La méthode de Shih consiste à tordre cette construction.

On se donne une extension quadratique K/k car 0 avec $\langle\sigma\rangle = Gal$. On se donne E sur K.

On se donne aussi une N-isogénie $\varphi : E \to E^\sigma$ (définie sur $\overline{K}$).

Hyp E n'a pas de mult complète

Dans ce cas, les 2 seules N-isogénies sont φ et $-\varphi$.

Soit ℓ premier $\neq 2$, $\ell \nmid N$.

$\varphi_\ell : E_\ell \xrightarrow{\sim} E_\ell^\sigma$ (canonique au signe près).

$P\varphi_\ell : \quad PE_\ell \xrightarrow{\sim} PE_\ell^\sigma.$ (115)

droite projective à $\ell+1$ pts

$E \xrightarrow[\pm\varphi]{} E^\sigma \xrightarrow[\pm\varphi' \atop \pm\varphi^\sigma]{} E \qquad \varphi^\sigma = \pm\varphi'.$

G_k agit sur PE_ℓ

(x,y) $\quad x \in PE_\ell$, $y \in PE_\ell^\sigma$ qui se correspondent par $P\varphi_\ell$.

d'où : $G_k \xrightarrow{\rho} PGl_2(\mathbb{F}_\ell)$

$G_k \supset G_K$ $\qquad s \in G_K$

sg d'indice 2 $\qquad s$ agit sur E_ℓ

d'où un élt de $Gl_2 \to PGl_2$

Si $s \notin G_K$ $\quad s$ induit σ

$E_\ell \to E_\ell^\sigma \xrightarrow{\varphi_\ell^{-1}} E_\ell$

$PSl_2(\mathbb{F}_\ell) \to PGl_2(\mathbb{F}_\ell) \xrightarrow{\det} \{\pm 1\} \to 0.$

$\delta(\rho) : G_k \longrightarrow \{\pm 1\}$ $\qquad \ell^* = (-1)^{\frac{\ell-1}{2}}\ell$

$\mathbb{Q}(\sqrt{\ell^*}) \subset \mathbb{Q}(\zeta_\ell)$

unique s/corps quadratique de $\mathbb{Q}(\zeta_\ell)$.

Théorème

① Si $\left(\frac{N}{\ell}\right) = 1$, alors

$\delta(\rho) = \varepsilon_\ell.$

Notons $\varepsilon_\ell : G_k \to \{\pm 1\}$ qui donne l'action de G_k sur $k(\sqrt{\ell^*})$

② Si $\left(\frac{N}{\ell}\right) = -1$ alors

$\delta(\rho) = \varepsilon_\ell \, \varepsilon_{K/k}$

$\varepsilon_{K/k} : G_k \to \{\pm 1\}$ noyau G_K

Démonstration

$\Lambda^2 E_\ell \simeq \mu_\ell$ ⁎ $E = \mathbb{C}/L$ $E_\ell = L/\ell L$ $\Lambda^2 L = \mathbb{Z}$

choix du signe μ_ℓ $\Lambda^2 E_\ell \simeq \mathbb{Z}/\ell\mathbb{Z} = \underbrace{\mu_\ell}_{e^{2\pi i/\ell}}$

$\alpha : E \to F$

$\alpha_\ell : E_\ell \to F_\ell$

$\Lambda^2 \alpha_\ell : \mu_\ell \to \mu_\ell$ multipl. par degré

En fait

$E_\ell = H_1(E, \text{mod } \ell)$

$\mu_\ell = H_2(E, -)$.

$s \in G_k$ PE_ℓ.

ⓐ Si $s \in G_K$ $\delta(\rho)(s) = \varepsilon_\ell(s)$

$E_\ell \xrightarrow{s} E_\ell$

dét mod □

ⓑ Si $s \in G_k - G_K$

$E_\ell \xrightarrow{s} E_\ell^\sigma \xrightarrow{\varphi_\ell^{-1}} E_\ell$ $N^{-1}\chi_\ell(s) \in \mathbb{F}_\ell^* / \square = \{\pm 1\}$

$\mu_\ell \xrightarrow{\chi_\ell(s)} \mu_\ell \xrightarrow{N^{-1}} \mu_\ell$ d'où le théorème.

On va supposer $\left(\frac{N}{\ell}\right) = -1$ dans la suite

$\delta(\rho) = \varepsilon_\ell \, \varepsilon_{K/k}$

Étape suivante : choix de k, K, E.

$X_0(N)$ classifie les isogénies de degré n

corps de fonctions $\mathbb{Q}(j, j_N)$

$j = \frac{1}{q} + 744 + 196884q + \ldots$ $j(z)$ $q = e^{2\pi i z}$

$j_N(z) = j(Nz) = \frac{1}{q^N} + 744 + 196884q^N + \ldots$

On prendra $K = \mathbb{Q}(j, j_N)$

Il existe une involution σ (w) permutant j et j_N (de Fricke) (σ, w, w_n selon auteurs).

k = corps des pts fixes $= \mathbb{Q}(j, j_N)^+$

$=$ — de fonctions de $X_0(N)^+ = X_0(N)/_{\{1, w_N\}}$

E courbe elliptique sur K d'invariant j.

$\Phi_N(j, j')$

$K \simeq \mathbb{Q}[j, j_N] / (\Phi_N(j, j_N))$.

Il est bien vrai que E^σ a comme invariant j_N et est donc N-isogène à E.

D'où un homom de $G_k \xrightarrow{\rho} PGl_2(\mathbb{F}_\ell)$ associé à k, K, E, N, ℓ.

① ρ surjectif

② $\delta(\rho) = \varepsilon_\ell \, \varepsilon_{K|k}$.

③ l'ext. coresp de $k = \mathbb{Q}(j, j_N)^+$ est rég.

$1 \to PSl_2(\mathbb{F}_\ell) \longrightarrow PGl_2(\mathbb{F}_\ell) \to \{\pm 1\} \to 1$.

image de G_K contient $PSl_2(\mathbb{F}_\ell)$, car c'est vrai sur $\mathbb{C}$.

$\mathbb{C}(j, j_N) = (\mathbb{C} \otimes K)$ frac

$\mathbb{Q}(j, j_N) = K$

$G_{\mathbb{C}(j)}$ agissant sur $T_\ell(E) \times \prod_{\ell' | N} T_{\ell'}(E)$

donne $Sl_2(\mathbb{Z}_\ell) \times \prod Sl_2$.

D'où une ext gal. régulière de $k = \mathbb{Q}(j, j_N)^+$ à groupe $PGl_2(\mathbb{F}_\ell)$.

Supposons que $N \in S = \{2,3,5,7,11,13,19,23,29,31,$
$41,47,59,71\}$

1er. $N \in S \Leftrightarrow N \mid$ Monstre,

$N \in S \Leftrightarrow$ genre de $X_0(N)^+ = 0$.

$X_0(N)$ a 2 ptes $(0, \infty)$.

Alors $k \simeq \mathbb{Q}(T)$.

<u>Théorème</u> : <u>Si ℓ premier</u> ≥ 3 <u>est tel que</u> $\left(\frac{N}{\ell}\right) = -1$
<u>pour au moins un $N \in S$</u>, <u>alors</u> $PSL_2(\mathbb{F}_\ell)$ <u>a la</u>
<u>prop. Gal_T</u>.

(vrai pour $\ell < 5329271$)

On veut PSL_2.

$K \quad \mathbb{Q}(\sqrt{\ell^*})k = \mathbb{Q}(\sqrt{\ell^*}, j, j_N)^+$

$k = \mathbb{Q}(j, j_N)^+ \xrightarrow{2} \varepsilon_\ell$, K/k : 2

$\varepsilon_{K/k} \cdot \varepsilon_\ell$

Dans le composé (biquadratique sur k), on regarde le corps intermédiaire $K_1(N, \ell)$, car associé $\varepsilon_{K/k} \cdot \varepsilon_\ell$.

D'où une ext. régulière de $K_1(N, \ell)$ à groupe de Galois $PSL_2(\mathbb{F}_\ell)$.

$$\begin{array}{ccc} X_0(N) & \longrightarrow & X_0(N)^+ / \mathbb{Q}(\sqrt{\ell^*}) \\ \{1, w_N\} \searrow & & \nearrow \\ & X_0(N^+) & \end{array}$$

$K_1(N, \ell)$ est le corps de fonctions de $X_0(N)$ tordue par le groupe d'automorphismes $\{1, w_N\}$ relativt à l'ext quad $\mathbb{Q}(\sqrt{\ell^*})/\mathbb{Q}$.

$G_\mathbb{Q} \xrightarrow{\varepsilon_\ell} \{\pm 1\} \to \mathrm{Aut}\, X_0(N)$

On appelle cette courbe $X_0(N)_\ell$.

genre $X_0(N)_\ell = 0$ si $N \in \{2, 3, 5, 7, 13\}$
(N 1er)

a 1 pt rationnel si $N \in \{2, 3, 7\}$.

Le corps $K_1(N, \ell)$ 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

$K = \mathbb{Q}(j, j_N) \subset$ séries formelles en q.

$$T = \left(\frac{\Delta(z)}{\Delta(Nz)}\right)^{\frac{1}{N-1}} = q^{-1} \prod_{\substack{m=1 \\ N \nmid m}}^{\infty} (1 - q^m)^{\frac{24}{N-1}}$$

$$\Delta = q \prod_{m=1}^{\infty} (1 - q^m)^{24}$$

$$\boxed{w_N(T) = N^{\frac{12}{N-1}} \frac{1}{T}}$$

Les pts fixes sont rationnels si ceci est $\frac{\square}{T}$ (ie $\frac{12}{N-1}$ est pair) soit $N = 2, 3, 7$. Ds les autres cas, donne équation conique.

Autre manière de procéder :

Description explicite des pts fixes de w $N = 2, 3, 7$.

$N = 2$ $\begin{cases} \text{m.c. par } \mathbb{Z}[i] \\ \text{endo } 1+i \\ \to \mathbb{Z}[\sqrt{-2}] \text{ end } \sqrt{-2}. \end{cases}$

$N=3$ 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 $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ $\sqrt{-7}$

$\mathbb{Z}[\sqrt{-7}]$ $\sqrt{-7}$.

Les pts correspdts st rationnels car nbre de classes $=1$ pour isogénie $\overline{\pi}=-\pi$ ou en tt cas $\overline{\pi}=$ unité π.

5 et 13 ne marchent pas car $h=2$.

Thme Shih si $\left(\frac{N}{\ell}\right)=-1$ pour au moins un $N\in\{2,3,7\}$ alors $PSL_2(\mathbb{F}_\ell)$ a la prop Gal_T

Premier ex ne marchant pas $p=47$.

Thme d'irréductibilité avec paramètre elliptique (Néron).

Soit $X\to S$ un revêt ramifié régulier galoisien de groupe G, S courbe de genre 1 sur Ω (c. de nbrs)

On suppose que pour tout ssgpe H de G contenant (G,G) et $\neq G$, le revêt $X/H\to S$ ~~soit~~ est ramifié en au moins un pt de S (évite d'avoir isogénie S' qui donnerait image des pts rationnels trop S grosse.

Alors pour tt $P\in S(\Omega)$, sf un nbre fini, on a $Irr(P)$ (d'où ext gal. de gpe G).

En effet X/H de genre ≥ 2 $\xrightarrow{\text{Faltings}}$ nbre fini

Néron (ignorant Faltings!) : nbre fini $\to$ mince que $S(\Omega)$.

Corollaire Si un tel revêt existe sur $\mathbb{Q}$ avec $S:\mathbb{Q}^*\mathbb{K}$,

$\exists$ cours de nbres à des ext. galois de gpe G.

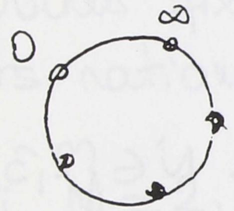
Très bon théorqt mais pas pour les calculs numériques !

Ex $\frac{\ell}{\ell} = 47$ $N = 1$

Shih $\Rightarrow$ ext galois $PSL_2(\mathbb{F}_{47})$ au-dessus de $K_1(N,\ell)$

c. des fctions de $X_0(N)_\ell$.

$X_0(11)_{47}$ a une qté de pts rationnels.



$X_0(11)$ 5 pts rationnels

$-47y^2 = f(x)$

On peut prendre $f(x) = 4x^3 - 4x^2 + 1$

(donne courbe isogène à $X_0(11)$)

$x = -2, \quad y = 1$ d'ordre ∞ (cf par réduct)

$x = -8 \quad y = 7$

$\exists$ cours de nbres possède ext gal à gpe de Galois $PSL_2(\mathbb{F}_{47})$

explicite sur $\mathbb{Q}$ par Elkies.

$N = 2, 3, 7$

$\left(\ell, \frac{N}{\ell}\right) = -1$

$$\begin{array}{c} C \\ \downarrow G = PSL_2(\mathbb{F}_\ell) \\ \mathbb{P}_1 \end{array}$$

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 $\mathbb{I} \cdot \sqrt{-7}, \mathbb{I}\sqrt{-27}\ell^*$

(pas obtenu par rigidité)