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

Problèmes Galoisiens (suite)

Cours de Jean-Pierre Serre, tome 10 (1989-1990)
<http://www.numdam.org/item?id=CJPS_1989__10_>

Cours 1989 – 1990

Problèmes Galoisiens (suite)

—

Notes de E. Bayer, complétées par C. Goldstein

Résumé des cours 1989 - 1990
Annuaire du Collège de France (1990)

Algèbre et géométrie

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

Le cours, comme celui de l'année précédente, a été consacré au « problème inverse de la théorie de Galois » : étant donné un groupe fini G, existe-t-il une extension galoisienne L de **Q** telle que le groupe de Galois Gal(L/**Q**) soit isomorphe à G ?

En fait, on s'est intéressé à la propriété plus précise suivante de G : (Gal_T). — Il existe une extension galoisienne régulière de **Q**(T) de groupe de Galois G.

Des exemples de groupes ayant cette propriété avaient déjà été donnés dans le cours de 1988-1989. La méthode suivie cette année a été basée sur la notion de « rigidité », due à Belyi, Fried, Matzat et Thompson (voir notamment B.H. Matzat, *Konstruktive Galoistheorie*, Lect. Notes in Math. n° 1284, Springer-Verlag, 1987, ainsi que l'exposé 689 du séminaire Bourbaki, 1987-1988).

Enoncé du théorème de rigidité

On considère un groupe fini G, dont on choisit des classes de conjugaison $C_1, \ldots, C_k$. On fait les deux hypothèses suivantes :

(1) (« rationalité »). Chacune des classes C_i est rationnelle sur **Q**. Cela signifie que $x \in C_i$ entraîne $x^m \in C_i$ pour tout m premier à l'ordre de x.

(2) (« rigidité »). Il existe $x_1 \in C_1, \ldots, x_k \in C_k$ tels que $x_1 \ldots x_k = 1$ et que G soit engendré par les x_i. De plus, si $x'_1, \ldots, x'_k$ est une autre famille d'éléments jouissant des mêmes propriétés, il existe $g \in G$ tel que $x'_i = g x_i g^{-1}$ pour tout i.

Théorème - *Supposons que le centre de* G *soit trivial, et que les classes* $C_1, \ldots, C_k$ *satisfassent à* (1) *et* (2). *Soit* K *un corps de caractéristique zéro, et soient* $Q_1, \ldots, Q_k$ *des points* K*-rationnels, deux à deux distincts, de la droite* *projective* $\mathbf{P}_1$. *Il existe alors une extension galoisienne régulière* L *du corps* K(T) *des fonctions rationnelles sur* $\mathbf{P}_1$ *jouissant des propriétés suivantes :*

(a) *Le groupe de Galois* Gal(L/K(T)) *est* G.

(b) *L'extension* L/K(T) *est non ramifiée en dehors des* Q_i.

(c) *Pour tout i, le groupe d'inertie en* Q_i (défini à conjugaison près) *est engendré par un élément appartenant à la classe* C_i.

De plus, une telle extension L *est unique, à isomorphisme unique près.*

Notons X la courbe algébrique, projective et lisse, dont le corps de fonctions est le corps L cherché. C'est un revêtement galoisien ramifié de $\mathbf{P}_1$. Lorsque le corps de base est le corps **C** des nombres complexes, l'existence et l'unicité de X résultent du théorème d'existence de Riemann (dont la démonstration a été rappelée dans le cours, en même temps que celle des théorèmes du type « GAGA »). On passe ensuite de **C** à K par un argument de « descente » reposant de façon essentielle sur *l'unicité* de la courbe cherchée.

Le théorème ci-dessus, appliqué avec K = **Q**, donne :

Corollaire - *Tout groupe fini* G *à centre trivial possédant des classes ayant les propriétés* (1) *et* (2) *jouit de la propriété* Gal_T. *En particulier,* G *est groupe de Galois d'une infinité d'extensions de* **Q**, *linéairement disjointes.*

Variantes du théorème de rigidité

Ces variantes visent à affaiblir les hypothèses (1) et (2), qui sont très difficiles à satisfaire. Un certain nombre d'entre elles ont été exposées dans le cours, avec applications aux groupes suivants :

— S_n, A_5, $SL_2(\mathbf{F}_8)$, J_1, J_2 ;

— $PSL_2(\mathbf{F}_p)$ pour p premier tel que $\left(\dfrac{2}{p}\right) = -1$ ou $\left(\dfrac{3}{p}\right) = -1$;

— $3{\cdot}A_6$, $3{\cdot}A_7$, $3{\cdot}M_{22}$, $3{\cdot}McL$, $3{\cdot}Suz$, $3{\cdot}O'N$, $3{\cdot}F_{22}$, $3{\cdot}F'_{24}$, d'après W. Feit ;

— $PSL_2(\mathbf{F}_{p^2})$ pour p premier $\equiv \pm 2 \pmod 5$, d'après W. Feit.

D'autres variantes, exploitant l'action du *groupe des tresses* sur les solutions de $x_1 \ldots x_k = 1$, ont été exposées dans le séminaire par G. Malle (le cours a tenté — avec un succès limité — d'en donner une interprétation géométrique).

Propriétés locales des extensions de **Q**(T) *fournies par la méthode de rigidité*

Le cas réel n'est pas difficile, mais on sait peu de choses dans le cas p-adique. Ainsi, si G satisfait aux conditions du théorème ci-dessus, avec $k = 3$, et si $X \to \mathbf{P}_1$ désigne le revêtement correspondant, est-il vrai que ce revêtement « se réduit bien mod p » pourvu que p ne divise pas l'ordre des éléments de C_1, C_2, C_3 ? (C'est vrai lorsque p ne divise pas l'ordre de G.)

Un théorème de Harbater

Il ne s'agit plus ici de rigidité, mais de la propriété Gal_T pour un groupe fini donné G. Cette propriété est relative au corps **Q**. On peut se demander si elle est déjà vraie dans le cas local, c'est-à-dire lorsque l'on remplace **Q** par $\mathbf{Q}_p$ (ou par **R**, mais ce cas est facile). Il en est bien ainsi. De façon plus précise, on a :

Théorème (Harbater) *Pour tout groupe fini* G *et tout corps local* K *de caractéristique* 0, *il existe une extension galoisienne régulière* L *de* K(T) *ayant les deux propriétés suivantes :*

(a) *Le groupe de Galois* Gal(L/K(T)) *est* G.

(b) *Il existe un point* $Q \in \mathbf{P}_1(K)$ *qui est complètement décomposé dans l'extension* L/K(T) (autrement dit, la courbe X correspondant à L possède un point rationnel sur K distinct des points de ramification).

La démonstration repose sur les théorèmes du type « GAGA formel » de Grothendieck (ou « GAGA *p*-adique rigide » de R. Kiehl et U. Köpf, cela revient au même, comme me l'a signalé M. Raynaud). On commence par vérifier que le théorème est vrai lorsque G est cyclique, ce qui peut se faire (sur tout corps de base) en utilisant des isogénies de tores. Lorsque G n'est pas cyclique on choisit des sous-groupes propres G_1 et G_2 de G engendrant G et l'on choisit dans la droite projective $\mathbf{P}_1$ deux disques fermés disjoints D_1 et D_2. Utilisant l'hypothèse de récurrence, on construit un revêtement rigide de D_i ($i = 1,2$), de groupe G, qui est trivial sur le bord de D_i et admet une « composante connexe » stable par G_i. Par recollement de ces revêtements (sur les D_i) et du revêtement trivial (sur le complémentaire de $D_1 \cup D_2$), on obtient un revêtement rigide (donc algébrique) de $\mathbf{P}_1$ ayant les propriétés voulues.

Les exemples de Mestre pour A_n *et* $\tilde{A}_n$

J.-F. Mestre a construit récemment (*J. of Algebra*, 1990) des extensions galoisiennes régulières de **Q**(T) à groupe de Galois le groupe alterné A_n jouissant de remarquables propriétés, parmi lesquelles :

(i) Les groupes d'inertie correspondant aux points de ramification sont d'ordre 3.

(ii) Il existe un « point-base » $Q \in \mathbf{P}_1(\mathbf{Q})$, i.e. un point rationnel qui est complètement décomposé dans l'extension considérée.

Supposons $n \geqslant 4$. Le groupe A_n possède alors une unique extension centrale non triviale par un groupe d'ordre 2, notée $\tilde{A}_n$ (ou $2 \cdot A_n$). Si L/**Q**(T) est une extension galoisienne à groupe de Galois A_n, on peut se demander s'il existe une extension quadratique $\tilde{L}$ de L telle que $\tilde{L}$ soit galoisienne sur **Q**(T) à groupe de Galois $\tilde{A}_n$. Ce « problème de plongement » se heurte à une obstruction qui est un élément x du groupe $H^2(\mathbf{Q}(T),\mathbf{Z}/2\mathbf{Z}) = Br_2\,\mathbf{Q}(T)$. Dans le cas des extensions de Mestre, *cet élément est* 0 (Mestre, *loc. cit.*). En effet, le fait que les groupes d'inertie soient d'ordres impairs entraîne que x est « constant », i.e. provient de $H^2(\mathbf{Q},\mathbf{Z}/2\mathbf{Z})$; comme cette constante prend la valeur 0 au point-base, elle est nulle. (La nullité de x peut aussi se prouver en utilisant l'invariant de Witt de la forme trace associée à l'extension de degré n définie par L : c'est de cette façon que procède Mestre.)

On déduit de là l'existence de l'extension $\tilde{L}$. En particulier, $\tilde{A}_n$ *a la propriété* Gal_T *pour tout* $n \geqslant 4$, ce qui complète des résultats antérieurs de N. Vila. Lorsque n est *impair*, on peut aller plus loin, et construire une extension $\tilde{L}$ ayant les propriétés supplémentaires suivantes :

— elle est non ramifiée sur la sous-extension L correspondante ;

— elle a un point-base.

On utilise pour cela le résultat suivant :

Théorème - *Soit n un entier impair > 4. Soient $x_1, \ldots, x_{n-1}$ des 3-cycles engendrant A_n et tels que $x_1 \ldots x_{n-1} = 1$. Pour tout i, soit $\tilde{x}_i$ l'unique élément d'ordre 3 de $\tilde{A}_n$ se projetant sur x_i. On a alors $\tilde{x}_1 \ldots \tilde{x}_{n-1} = 1$ dans $\tilde{A}_n$.*

La démonstration peut se faire, soit par voie combinatoire, soit en utilisant les propriétés des « thêta-caractéristiques » des courbes algébriques. Elle n'a pas été donnée dans le cours, mais elle a fait l'objet d'un exposé de séminaire à l'E.N.S.

Séminaire

G. Malle - *Braid orbit theorems* (2 exposés).

Publication

J.-P. Serre, *Rapport au Comité Fields sur les travaux de A. Grothendieck* (*K-Theory* 3 (1989), p.199-204).

Missions

Cours :

— *Topics in Number Theory and Group Theory*, Singapour, février 1990.

Exposés :

— $\tilde{A}_n$*-liftings*. Oberwolfach, octobre 1989 ;

— *Relevements dans* $\tilde{A}_n$ *et thêta-caractéristiques*. E.N.S., octobre 1989 ; Bordeaux, janvier 1990 ;

— *Spécialisation d'éléments de* Br Q(T) (2 exposés), Univ. Paris VII, octobre 1989 ;

— *Un chapitre de théorie des groupes*. E.N.S., novembre 1989 ;

— *The « Hauptmoduln » for* $X_0(N)$. Singapour, février 1990 ;

— C *is algebraically closed*. Singapour, février 1990 ;

— *Bounds for number of solutions of equations over* $\mathbf{F}_q$. Singapour, mars 1990 ;

— *Spécialisations d'éléments du groupe de Brauer*. Luminy, mars 1990 ;

— *Cohomology and Galois groups* (3 exposés). Oxford, avril 1990 ;

— *Problème inverse de la théorie de Galois : succès et échecs*. Genève, avril 1990 ;

— *Points rationnels sur les variétés algébriques* (3 exposés). E.N.S. Lyon, avril 1990 ;

— *Bornes pour les nombres de points d'hypersurfaces sur les corps finis* (2 exposés). Besançon, mai 1990 ;

— *On coverings of algebraic curves in characteristic* $p > 0$. Purdue, juin 1990 ;

— *Sur les groupes fondamentaux des courbes algébriques en caractéristique* p. Orsay, juin 1990.

Table des Matières

Serre ① 9/10/89

Problèmes galoisiens : suite

Construction d'extensions de corps de nombres à groupe de Galois donné.

$$\begin{array}{c} E \\ \Big| \, G \\ \mathbb{Q}(T) \end{array}$$

utiliser le π_1 pour fabriquer des ext. de $\mathbb{C}(T)$, puis descendre sur $\mathbb{Q}(T)$: méthode de rigidité.

topologie – str. analytique complexe – algébrique
GAGA

1) Théorèmes de finitude de cohomologie

(entraîne des théorèmes d'existence).

Thm (Cartan-Serre, 1953) : Soit X ~~une~~ une variété analytique complexe, compacte ; soit F un faisceau cohérent sur X. Alors les espaces $H^q(X, F)$ sont de dimension finie sur $\mathbb{C}$ pour tout q (nuls pour $q<0$, $q>\dim X$).

$\mathcal{D}_x \supset \mathcal{H}_x$
diff an. réel

Thm de "div. des dist"
$\mathcal{D}_x$ est plat sur $\mathcal{H}_x$.
Malgrange

On utilise un thm de Schwartz sur les appl. compl. cont. :

Thm (Schwartz) :

Soit $\varphi : E_1 \to E_2$ une application lin. cont. surjective d'espaces de Fréchet (evtlc, métrisable, complet).

Soit $u : E_1 \to E_2$ une appl. lin. complètement continue ($\exists$ vg de 0 ds E_1 dont l'image par u est rel. compacte). Alors :

$\mathrm{Im}(\varphi + u)$ est fermée, de codimension finie ds E_2.

(difficulté est de montrer que $\mathrm{Im}(\varphi+u)$ est fermée)

Ref : CRAS ~1953, Sém. Cartan (Serre)

X lisse

X rec. par des ouverts de Stein $(U^i) = \mathcal{U}$

Coh. de X ds F est celle du complexe $C(\mathcal{U}, F)$. Sur cet espace, on a une structure naturelle d'espace de Fréchet.

Plus généralement, V var. de Stein, F

$H^0(V, F) = \Gamma(F)$ top. de Fréchet

"convergence compacte"

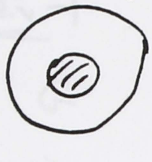
$$\mathcal{L}^n \to F \to 0$$

Rec. de Stein $(\mathcal{U}^2_i) = \mathcal{U}^2$, t.q.

$U_i^2 \subset U_i^1$.

$$C^1(\mathcal{U}, F) \xrightarrow{c.c.} C^2(\mathcal{U}, F)$$ compl. cont.

isom. sur cohomologie

Fct hol. bornées  on peut extr. conv.

$$\begin{array}{ccc} Z_1^q & \xrightarrow{i} & Z_2^q \\ & & \uparrow \delta \\ & & C_2^{q-1} \end{array}$$

$E_1 = Z_1^1 \times C_2^{q-1}$, $E_2 = Z_2^q$

$\varphi = i + \delta$ surjectif, $u = -i$

d'où : δ a image fermée de codim. finie. C'est ce qu'on voulait.

Cas particulier :

F localement libre $\Longleftrightarrow$ fibré vectoriel

Kodaira a donné une démonstration tout à fait différente de la finitude, par formes harmoniques.

Généralisations du thm de finitude.

Thm de Grauert :

Si $\pi : X \to Y$ est un morphisme propre d'espaces analytiques complexes. (réunion dénombrable de compacts ?) et si F est un faisceau analytique cohérent sur X, les images directes $R^q_\pi F$ sont des faisceaux analytiques cohérents sur Y.

Publ. IHES, 1960 (compliqué, erreurs de détail), Kiehl - Verdier, 1971 Math. Ann. (exposé ds Bourbaki par Douady) (Sém. Bourbaki 1971).

Analogue dans le cadre rigide :
Kiehl, Invent. Math. 1966
Lütkebohmert : les déf. de rigide sont équivalentes.

Théorèmes de type "GAGA"

$/\mathbb{C}$ X variété algébrique projective (en fait propre suffit)

X^h espace analytique associé.

$\mathcal{O}_x$ $x \in X$ algébrique, $\mathcal{O}^h_x$ analytique complexe

Ces 2 anneaux locaux ont le même complété :

$$\hat{\mathcal{O}}_x = \hat{\mathcal{H}}_x = \text{séries formelles sur } \mathbb{C}$$

$\mathcal{H}_x = \mathcal{O}^h_x$ est fidèlement plat sur $\mathcal{O}_x$

F faisceau algébrique cohérent $/X$

$$F^h = F \otimes_{\mathcal{O}_x} \mathcal{O}^h_x \qquad i : X^h \xrightarrow[\text{cont.}]{} X$$

$$H^q(X,F) \to H^q(X^h, F^h)$$

Théorème (GAGA).

(a) Pour tout F alg. cohérent,

$$H^q(X,F) \longrightarrow H^q(X^h, F^h)$$

est un isomorphisme

(b) $$\mathrm{Hom}_X(F,G) \xrightarrow{\sim} \mathrm{Hom}_{X^h}(F^h, G^h)$$

(c) Tout faisceau analytique cohérent sur X^h est de la forme F^h (pour un F unique, à isom. unique près)

($F \longmapsto F^h$ est une équivalence de catégories).

Théorème :

Si X est projectif, Y alg.

$$\mathrm{Mor}(X, Y) \simeq \mathrm{Mor}(X^h, Y^h).$$

$$\Updownarrow$$

Thm de Chow : ttte ssvariété anal. compacte d'une var. alg. est algébrique.

Thm de finitude intervient ds (c).

Démonstrations :

(a) $X = \mathbb{P}_r$ $r = \dim$

on prolonge le faisceau par 0.

récurrence sur r. $r=0$ est évident.

Vérifier (a) si $F = \mathcal{O}_X$, $F^h = \mathcal{O}_X^h$

$$H^q(X, \mathcal{O}_X) = 0 \quad \text{si } q \geq 1$$

$$H^0(X, \mathcal{O}_X) = \mathbb{C}$$

On doit calculer $H^q(X^h, \mathcal{O}_X^h)$

Méthodes possibles : utiliser méth. var. kählenennes

$$H^q(X^h, \mathcal{O}_X^h) = h^{0,q}$$

à voir, $h^{0,q} = 0 \quad q \geq 1$

$h^{q,0}$

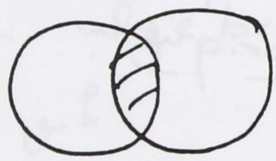
autre méthode:

recouvrement de Stein $t_i \neq 0$

(Frenkel)

$$H^1(\mathbb{P}_1(\mathbb{C}), \mathcal{H}) \overset{?}{=} 0$$

rec. $\mathbb{P}_1$ par les 2 ouverts $z \neq \infty$ et $z \neq 0$



à démontrer: toute fct holomorphe sur $\{z \neq 0, \infty\}$ est différente d'une fct. hol. sur $\{z \neq 0\}$, $\{z \neq \infty\}$.

$$f = \sum_{-\infty}^{\infty} a_n z^n$$

$$\frac{-\log |a_n|}{n} \to \infty$$

$$f = \sum_{1}^{\infty} a_n z^n + \sum_{-\infty}^{0} a_n z^n$$

Monter (a) pour $F = \mathcal{O}_X(n)$, le $n$ième tordu de $\mathcal{O}_X$.

t forme lin. $\neq 0$ section de $\mathcal{O}(1)$

$$0 \to \mathcal{O}_X(n-1) \xrightarrow{t} \mathcal{O}_X(n) \to \mathcal{O}_H(n) \to 0$$

$\mathcal{O}_H$: faisceau des fct. rég. sur H : $t = 0$.

$\mathcal{U}$: $(t_i \neq 0)$ (ouv. affines var. de Stein)

F

$$0 \to C(\mathcal{U}, F) \to C(\mathcal{U}, F^h) \to Q(F) \to 0$$

$$H_0(F) \qquad H^q(X, F) \to H^q(X^h, F^h) \to H_0^q(F) \to \dots$$

On veut montrer $H_0^q(F) = 0$.

$$H_0^q(\mathcal{O}_X(n-1)) \simeq H_0^q(\mathcal{O}_X(n))$$

indép. de n. Mais on le connait pour $n = 0$: $H_0^q(\mathcal{O}_X) = 0$. Donc $= 0$ tjs.

<u>Cas général</u> :

$$0 \to R \to L \to F \to 0$$

L somme directe de faisceaux $\mathcal{O}_X(n_i)$.

$$H_0^q(F) \cong H_0^{q+1}(R).$$

récurrence descendente sur q.

Si $q > r = \dim$, tout est 0.

$H_0^{q+1}(R) = 0$ par hyp. de réc.

b.) Tout homomorphisme

$$F^h \to G^h$$

est algébrique, i.e.

$$\underline{Hom}(F, G) \to \underline{Hom}(F^h, G^h)$$

est bijectif.

Résulte de a.), appliqué à $\underline{Hom}(F,G)$.

$$H^0(X, \underline{Hom}(F,G)) = Hom(F,G).$$

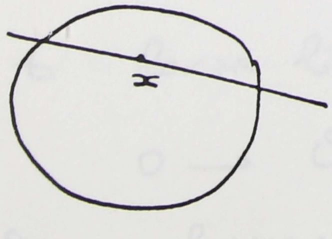
c.) Proposition:

Si F analytique cohérent sur $X = \mathbb{P}_r(\mathbb{C})$ il existe un entier n tel que $F(n)$ soit "engendré par ses sections"

$$H^0(X, F(n)) \xrightarrow{\text{surj.}} F(n)_x / m_x F(n)_x$$

Récurrence montante sur r

Suffit de montrer que pour $x \in X$, il existe un $n = n(x)$ tel que $F(n)_x$ soit engendré par les sections globales.



$t=0$

H : hyperplan défini par $t = 0$.

$x \in H$ (10)

Multiplication par t :

$$0 \to A \to F(-1) \xrightarrow{t} F \to B \to 0$$

A et B sont annulés par t.

$$0 \to A(n) \to F(n-1) \xrightarrow{t} F(n) \to B(n) \to 0$$

On suppose connu c.) pour $\mathbb{P}_{r-1}$.

Donc les $H^i(A(n))$, $H^i(B(n))$ sont

0 pour $n \geq N$.

$C = \mathrm{Im}\,(t : F(-1) \to F)$

$$0 \to A \to F(-1) \to C \to 0$$

$$0 \to C \to F \to B \to 0$$

$$0 \to A(n) \to F(n-1) \to C(n) \to 0$$

$$0 \to C(n) \to F(n) \to B(n) \to 0$$

On suppose $n > N$.

$$H^0(F(n-1)) \to H^0(C(n)) \to 0$$

$$0 \to H^0(C(n)) \to H^0(F(n)) \to H^0(B(n)) \to H^1(C(n))$$

$$\to H^1(F(n)) \to 0$$

$$H^1(F(n-1)) \xrightarrow{\sim} H^1(C(n))$$

donc $H^1(F(n-1)) \to H^1(F(n))$ est surjectif.

Donc la suite des

$$\dim H^1(X, F(n))$$

est décroissante, donc stationnaire.

Quitte à changer N,

$$\dim H^1(F(n-1)) = \dim H^1(F(n))$$

si $n > N$.

Donc $H^0(F(n)) \to H^0(B(n))$

est surjective, pour $n > N$.

Donc quitte à rechanger N,

$H^0(B(n))$ engendre $B(n)_x$

$(n > N)$.

Mais $B(n)_x = F(n)_x / t\, F_n(x)$.

Donc $H^0(F(n))$ engendre $F(n)_x \pmod t$.

$\Longrightarrow$ engendre $F(n)_x$.

(Nakayama)

$$L \longrightarrow F(n) \to 0$$

$$L = \mathcal{O}_x^h \oplus \cdots \oplus \mathcal{O}_x^h$$

L_0 : somme directe de faisceaux $\mathcal{O}^h(n_i)$

$$L_1 \xrightarrow{\partial} L_0 \longrightarrow F \longrightarrow 0$$

$(\mathrm{Coker}\, \partial)^{\sim} = F.$

(Kodaira - Spencer ~ 1953
décroissance des dim.)

Variété analytique compacte a au plus <u>une</u> structure algébrique.

GAGA est vrai pour les variétés algébriques propres (i.e. compactes) : démontré par Grothendieck, cf. Michèle Raynaud, SGA1, exposé 12, 1960/61)

GAGA rigide.

Thm de Grauert – Remmert (Ann. Math. 1958)

$$\begin{array}{c} \mathbb{P}_r \times Y \\ \downarrow \pi \\ Y \end{array}$$

Y variété analytique/$\mathbb{C}$

Faisceaux cohérents ?

<u>Thm A</u> <u>Sur tout compact de Y</u>,

$$\pi^*(R^0\pi\, F(n)) \longrightarrow F(n)$$

<u>est surjectif</u> p<u>our</u> <u>tout</u> n <u>grand</u>

(au-dessus d'un compact de Y).

Groth : espaces alg. au-dessus d'une base

(: cf. de M. Hakim.

GAGA/$\mathbb{R}$

variété projective / $\mathbb{R}$

"

variété anal. complexe, compacte, plongeable ds $\mathbb{P}_n(\mathbb{C})$ muni d'un anti-automorphisme de carré 1.

$X/\mathbb{C}$ $\quad X^\sigma$ $\qquad \mathbb{C} \xrightarrow{\sigma} \mathbb{C}$ conj. complexe

$$(X^\sigma)^h = \overline{X}^h$$

donne résultat ci-dessus.

Revêtements

X var. alg. projective / $\mathbb{C}$

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

π morphisme fini (<=> Y compacte, fibres finies).

GAGA $\Longrightarrow$ Y fini au-dessus de X analytique

$\Updownarrow$

algébrique

A démontrer : Si $Y \xrightarrow{\alpha} X^h$, α fini : analytique, il provient d'un unique Y_0 algébrique et d'un morphisme $Y_0 \xrightarrow{\alpha_0} X$

De tels Y correspondent à des faisceaux d'algèbres (comm. ass. avec 1) $\alpha_* \mathcal{O}_Y$ sur $\mathcal{O}_X$ qui sont des faisceaux cohérents sur X

Grothendieck, séminaire Cartan.

Corollaire : tout revêtement fini (non ramifié) de X (var. proj.) est algébrique (et projectif).

Plus généralement :

Théorème (Grauert - Remmert, Grothendieck).

Si X est une variété algébrique, tout revêtement fini (topologique) est algébrique.

Cas particulier

X quasi-projectif (ouvert dense dans une variété lisse projective $\overline{X}$).

$X = \overline{X} - W$

$$\begin{array}{ccc} Y & \subset & \overline{Y} \\ \downarrow & & \\ X & \subset & \overline{X} \end{array}$$

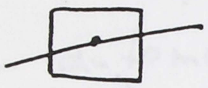
rev. non ramifié fini

$$\begin{array}{c} \overline{Y} \\ \downarrow \\ \overline{X} \end{array}$$ morphisme fini (plus étale)

Thm d'existence d'un tel $\overline{Y}$ est dû à Grauert - Remmert).

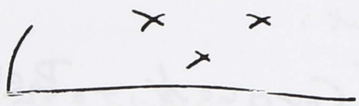
Si la sous-variété enlevée est lisse, thm. est trivial.

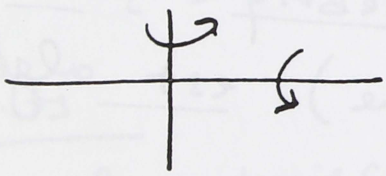
Si c'est un diviseur à croisements normaux, il est facile.

 $t=0$ disque $\times$ {disque $- pt$}

$\pi_1(\times) \cong \mathbb{Z}$

$z = t^{1/n}$

X courbe 

 $\mathbb{Z} \times \mathbb{Z}$

Résolution des singularités

<u>Surfaces</u>

$$S \xrightarrow{\text{morphisme fini}} \mathbb{P}_2$$

rev. ram. le long d'une courbe.

$$\begin{array}{ccc} S & \leftarrow & S' \\ \downarrow \pi & & \downarrow \\ \mathbb{P}_2 & \leftarrow & \mathbb{P}_2' \end{array}$$

Méthode de ~~Young~~ Jung.

Théorème d'existence de Riemann :

Une variété analytique complexe compacte de dim 1 est algébrique.

X surface de Riemann compacte.

$\dim H^1(X, \mathcal{O}_X^h) = g < \infty$

On va construire grâce à ça des fct mér. non const.

$P \in X$ choisi,

f fct holomorphe ailleurs qu'en P. avec pôle d'ordre $\leq n$ en P.

$\mathcal{L}_n$ faisceau de ces fcts.

$$0 \to \mathcal{O}^h \to \mathcal{L}_n \to Q_n \to 0$$

$Q_n = 0$ ailleurs qu'en P

$= \left\{ \frac{a_1}{t} + \cdots + \frac{a_n}{t^n} \right] \quad t$ coord. loc. $\}$

$H^0(Q_n)$ de dim n.

$$H^0(\mathcal{L}_n) \to H^0(Q_n) \to H^1(\mathcal{O}^h)$$

$\varphi : X \longrightarrow \mathbb{P}_n$ $\qquad$ $\deg(D) > 2g$

X alg. $\qquad$ série lin. définit plongement dans un $\mathbb{P}_n$).

Revêtements algébriques, analytiques et topologiques.

Conventions pour le groupe fondamental et les revêtements.

Définition par les lacets : $x_0 \in X$

$\alpha : [0,1] \longrightarrow X$, $\alpha(0) = \alpha(1) = x_0$.

$\alpha \cdot \beta$

Topologues : d'abord α, puis β.

Grothendieck, Deligne : d'abord β, puis α.

$$\begin{array}{ccc} L & & Y \\ \Big| G & & \Big\downarrow G \\ K & & X \end{array}$$

opère à gauche

$g^{-1} \longleftarrow g \in \mathrm{Aut}\, Y$

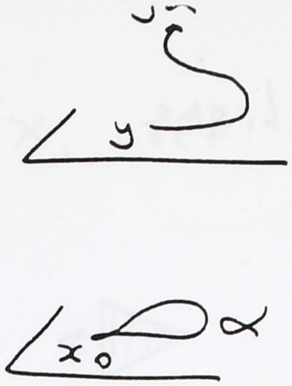
$\updownarrow$

Classification des revêtements

$$\begin{array}{c} Y \\ \downarrow \\ x_0 \in X \end{array}$$

Y_{x_0} = fibre du revêt. en x_0

espace discret



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

Class. des revêts :

X connexe (localement convenable), $x_0 \in X$

$$Y \longmapsto Y_0$$

est une équivalence de la catégorie des revêtements au-dessus de X dans celle des ens. discrets munis d'une action à droite de $\pi_1(X, x_0)$.

Gro $\begin{array}{cc} y_0 & Y \\ \downarrow & \downarrow \\ x_0 & X \end{array}$ rev. gal. de groupe G connexe

Si $\alpha \in \pi_1(X, x_0)$, le point $y_0\alpha \in Y_{x_0}$

il existe un unique $g(\alpha) \in G$ tel que $y_0\alpha = g(\alpha)y_0$

D'où un homomorphisme

$$\alpha \longmapsto g(\alpha)$$

$$\pi_1(X, x_0) \longrightarrow G$$

On obtient un homomorphisme

$$\pi_1(X, x_0) \longrightarrow G .$$

$\pi_1(X, x_0)$ "dépend" du point de base x_0.

$x_0 \longrightarrow x_1$ le choix d'un tel chemin définit un isom.

$$\pi_1(X, x_0) \xrightarrow{\sim} \pi_1(X, x_1)$$

unique à conjugaison près :

T simplement connexe, connexe

$w : T \to X$

$\pi_1(X, w)$ "a un sens" :

choisissons $t \in T$ $\quad \pi_1(X, w(t))$

$$\begin{array}{ccc} t \in T & & \pi_1(X, w(t)) \\ \alpha \swarrow & & \downarrow \simeq \\ t' \in T & & \pi_1(X, w(t')) \end{array}$$

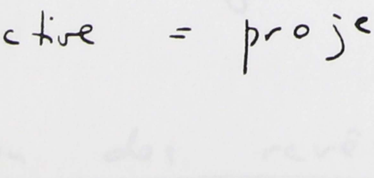
bien défini

On a un système transitif d'isom.

$\lim \pi_1(X, w(t)) = \pi_1(X, w)$

($\lim$ inductive = projective).

Deligne :



on enlève P de la variété

On voudrait prendre P pour point base

$\pi_1(X, \text{vect. tg.})$

base de filtre formé
d'espaces simplement
connexes

<u>Les surfaces et leur π_1</u>

X courbe algébrique lisse, connexe

$\pi_1(X(\mathbb{C}), x_0)$?

$\overline{X}$: courbe projective lisse $\supset X$

X dense ds $\overline{X}$

surface topologique compacte orientable.

$X = \overline{X} - \{P_1, \ldots, P_k\}$, $k \geq 0$.

<u>Classification des surfaces</u>

$k = 0$ $X = \overline{X}$ surface de genre g

($g = \frac{1}{2}$ premier nombre de Betti)

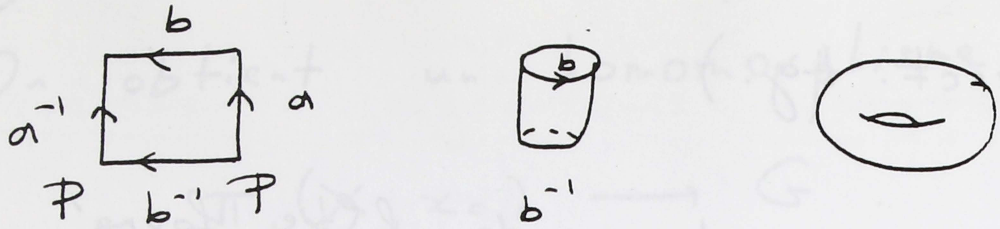
A homéom. près, une seule telle surface

$g = 0$ sphère, en général sphère

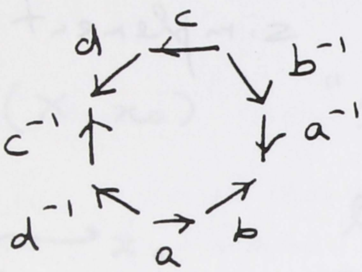
avec anses attachées.

Preuve : triangulation + réarrangement de triangles

Seifert - Threlfall



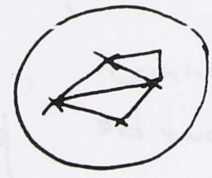
tore



$g = 2$

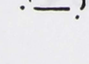
triangulation des surfaces : pas de problème ici, car

$$\begin{tikzcd} X \arrow[d, "\text{rev. ramifié}"] \\ \mathbb{P}_1 \end{tikzcd}$$



triangulation de la sphère avec la propr. que les points choisis soient des sommets

On relève la triangulation.

il faut éventuellement faire une subdivision barycentrique, si dans le relèvement on a  .

π_1(surface de genre g) $\cong$

groupe défini par $2g$ générateurs

$x_1, y_1, \ldots, x_g, y_g$

liés par la relation $(x_1, y_1) \cdots (x_g, y_g) = 1$

$(x, y) = x y x^{-1} y^{-1}$.

Théorème de van Kampen

U_1, U_2 2 ouverts, $U_1 \cap U_2$

(U_i et $U_1 \cap U_2$ connexes)

$x_0 \in U_1 \cap U_2$.

Alors $\quad \pi_1(U_1 \cup U_2) = \pi_1(U_1) \underset{\pi_1(U_1 \cap U_2)}{*} \pi_1(U_2)$

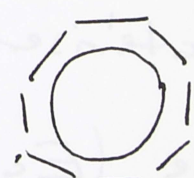
plus précisément, on a un diagramme

$$\begin{tikzcd} & \pi_1(U_1) \\ \pi_1(U_1 \cap U_2) \arrow[ur] \arrow[dr] & \\ & \pi_1(U_2) \end{tikzcd}$$

"push out"

U_1 voisinage du bord

U_2 disque intérieur



$U_1 \cap U_2$ a le type d'homotopie d'un cercle

P

π_1(voisinage du bord) $\simeq \pi_1$(bord)

= groupe libre à $2g$ générateurs

$\pi_1(U_2) = 1, \quad \pi_1(U_1 \cap U_2) = \mathbb{Z}$

$$\begin{tikzcd} & F \\ \mathbb{Z} \arrow[ur] \arrow[dr] & \\ & 1 \end{tikzcd}$$

gén $\longrightarrow \Pi(x_i y_i) = r$

$$= F/\langle r \rangle .$$

autre démonstration

van Kampen.

Comment se passer de topologie combinatoire ?

caractériser π_1(surfaces) ?

Th de (Eckmann + $\left| \begin{matrix} A \\ B \end{matrix} \right)$

caractérise le groupe fondamental d'une surface orientable de genre g

par :

| $cd\ \Gamma = 2$
| groupe à dualité
| 1er nombre de Betti $2g$.

"de type FL" : $\mathbb{Z}$ a rés. proj. de type fini.

admettons ce théorème.

On vérifie facilement le résultat précédent.

<u>parenthèse</u> :

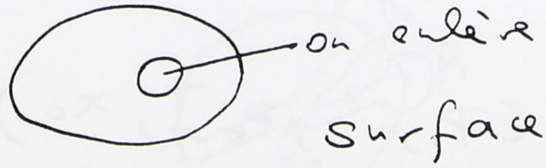
pro-p-groupe (Demushkin)

$\Longrightarrow$ Si X est une courbe proj. lisse en car $\neq p$, son pro-p-groupe fondamental est le pro-p-groupe défini par $(x_1, y_1) \cdots (x_g, y_g) = 1$ (corps algébriquement clos)

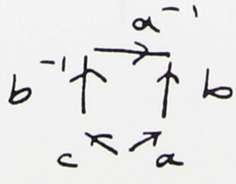
c'est une conséquence d'un thm de Grothendieck mais peut aussi se déduire de la caractérisation cohomologique.

$X = \overline{X} - \{P_1, \dots, P_k\}$, $k \geq 1$, P_i distincts

$\overline{X}$ de genre g.



surface compacte à bord.



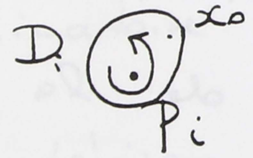
Le π_1 d'une telle surface est définie par $2g+k$ générateurs

$x_1, y_1, \dots x_g, y_g, z_1, \dots, z_k$

et la relation $(x_1, y_1) \cdots (x_g, y_g) z_1 \cdots z_k = 1$.

<u>Précision</u>:

Les z_i peuvent être choisis dans la classe de conjugaison "tourner autour de P_i" : C_i



disque D_i ne contenant pas P_j, $j \neq i$

$$\pi_1(D_i - P_i) \cong \mathbb{Z}$$

avec générateur $\circlearrowright$ "tourner autour dans le sens positif"

$x_0 \in D_i$

$$\mathbb{Z} \longrightarrow \pi_1(\overline{X} - \{P_1, \dots, P_k\}, x_0)$$

Remarque:

La position des P_i ne joue aucun rôle.

Surface orientable, contenant $\{P_1, \dots, P_k\}$ et $\{Q_1, \dots, Q_k\}$.

Il existe un homéomorphisme de la surface $P_i \mapsto Q_i$ $\forall i$.

Cas essentiel pour la suite :

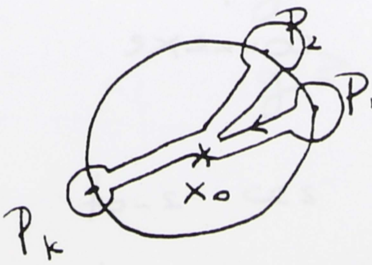
$$\overline{X} = \mathbb{P}_1(\mathbb{C}) = \mathbb{S}_2$$

$k \geq 1$, $P_1, \dots, P_k$.

$$\pi_1(\mathbb{S}_2 - \{P_1, \dots, P_k\}, x_0)$$

groupe libre à k générateurs

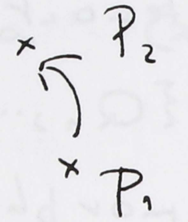
$z_1, \dots, z_k$ liés par $z_1 \cdots z_k = 1$.



$\mathbb{C} \cup \infty$

produit :

Groupe fondamental des espaces de k pts distincts : groupe de tresses.



$$z_1 z_2 z_1^{-1} z_1 z_3 \cdots z_k = 1$$

$z_1, \dots, z_k$ $\qquad \prod z_i = 1$

$z_1 z_2 z_1^{-1}, z_1, z_3, \dots, z_k$.

Lien avec les groupes fuchsiens

X surface de Riemann, connexe

$\tilde{X}$ revêtement universel

$$\begin{array}{c} \tilde{X} \\ \downarrow G \\ X \end{array} \qquad X = \tilde{X}/G$$

$\tilde{X}$ simplement connexe

$$\tilde{X} \cong \begin{cases} S_2 \\ \mathbb{C} \\ \frac{1}{2} \text{ plan} = \text{disque ouvert.} \end{cases}$$

S_2 n'a pas d'automorphisme opérant librement.

$\overline{X} = S_2$ possible seulement si $X \simeq S_2$

Sur $\mathbb{C}$: groupe discret opérant librement : 0, $\mathbb{Z}$, $\mathbb{Z} \oplus \mathbb{Z}$

$\mathbb{C}$ $\quad \mathbb{C}^* = S_2 - \{0, \infty\}$ $\quad$ courbe elliptique $g = 1$

Autres cas : s/g discrets (sans torsion) de $PSL_2(\mathbb{R})$

$X = \overline{X} - \{P_1, \dots, P_k\}$

g

cas triviaux : $g = 0$, $k = 0$ ou 1

$g = 1$, $k = 0$ $\Longrightarrow$ $\overline{X} = \mathbb{C}$, $g = 0$, $k = 2$, $\overline{X} = \mathbb{C}$

Autres cas : $\left.\begin{array}{l} g = 0, \ k \geq 3 \\ g = 1, \ k \geq 1 \\ g \geq 2 \end{array}\right\}$

dans tous ces cas, $G \subset PSL_2(\mathbb{R})$ discret.

" Groupe fuchsien de 1ère espèce"

$\Gamma \subset PSL_2(\mathbb{R})$, Γ discret,

$\quad\quad\ \ \wr\wr$

$Aut(D)$ $\quad$ D disque

$D/\Gamma \cup$ "pointes" compacte.

(s/g paraboliques de Γ

$\cong \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$

fixateurs des points du bord)

Soit Q un point de ∂D = bord du disque.

fixateur de Q dans $PSL_2(\mathbb{R})$

(radical unipotent du Borel. on pourrait avoir $\mathcal{O}$ $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$).

unipotent

$\simeq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

$$\partial D_\Gamma = \{ Q \mid \Gamma \cap (\text{fixateur de } Q) \text{ soit infini} \}.$$

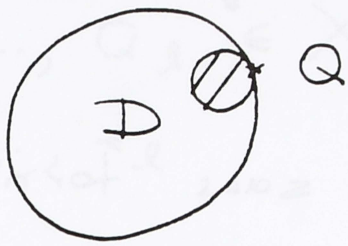
$$\wr\wr$$

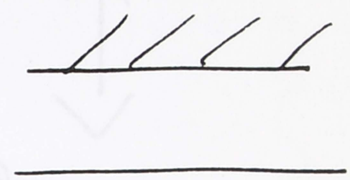
$$\mathbb{Z}$$

un tel Q est appelé une <u>pointe</u> de Γ.

Réf. Shimura, ou séminaire Cartan 60-61.

$D_\Gamma := D \cup$ (ensemble des pointes)





Action de Γ sur D_Γ.

D_Γ/Γ a une structure naturelle de surface de Riemann.

(sém. Cartan pour détails)

contient la surface ouverte D/Γ.

On dit que Γ est <u>fuchsien de 1ère espèce</u> si D_Γ/Γ est compacte.

<u>Siegel</u> ceci est équivalent à D/Γ de volume fini.

<u>Théorème</u> (Siegel):

<u>Si</u> Γ <u>discret</u> $\subset PSL_2(\mathbb{R})$, <u>alors</u>:

Γ <u>fuchsien de</u> 1<u>ère</u> espèce

$\Updownarrow$

aire $(D/\Gamma) < \infty$ ($\Longleftrightarrow$ $PSL_2(\mathbb{R})/\Gamma$ est de volume fini).

$(\overline{X}, P_1, \dots, P_k)$ $g=0,\ k\geq 3$

$g=1,\ k\geq 1$

$g\geq 2$

$\Big\Updownarrow$

groupes fuchsiens sans torsion

de $1^{\text{ère}}$ espèce.

$S_2 - \{0, 1, \infty\}$.

$\Gamma \subset PSL_2(\mathbb{Z})$

<u>Uniformisation avec ramification</u>.

(pas de bonne référence, sauf (peut-être) livre de Farkas - Kra)).

$\overline{X}$ surface de Riemann compacte.

Oubli :

$\Gamma = \pi_1 \subset PSL_2(\mathbb{R})$

topologie : eng. $x_1, \dots, y_g, z_1, \dots, z_k$

relation : $\prod_i (x_i, y_i) \cdot z_1 \cdots z_k = 1$

$\Longrightarrow$ z_i paraboliques (unipotents)

x_i, y_i hyperboliques?

$\overline{X}$ compacte, $P_1, \dots, P_k$

$X = \overline{X} - \{P_1, \dots, P_k\}$

$Q_1, \dots, Q_\ell \in X$

$e_1, \dots, e_\ell$ $\qquad e_i \geq 1$

$e(P_i) = \infty \quad \forall i.$

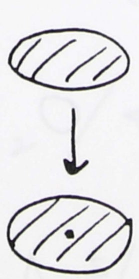
"signature"

On s'intéresse à

$$\begin{array}{c} Y \\ \downarrow \\ X \end{array} \qquad \text{surface de Riemann}$$

revêtement en dehors de $Q_1, \dots, Q_\ell$

Ramification divisant e_i au dessus de Q_i. Plus précisément :



Q_i

$$\begin{array}{c} z \\ \downarrow \\ z^\alpha \end{array}$$

$\alpha \mid e_i$

(α variable)

Il existe un revêtement universel pour la signature donnée.

Il est simplement connexe, galoisien, groupe G, de présentation :

$$\begin{cases} (x_1, y_1) \cdots (x_g, y_g)\, z_1 \cdots z_k\, q_1 \cdots q_\ell = 1 \\ q_i^{e_i} = 1 \quad , \quad i = 1, \dots, \ell \end{cases}$$

Cas dégénérés :

$g = 0$, $k = 0$, $\ell = 1$

$k = 0$ $\ell = 2$, $e_1 \neq e_2$

On les élimine.

Théorème :

Sauf dans les cas "dégénérés", l'ordre de q_i dans G est égal à e_i.

Le revêtement universel est un disque (cas "fuchsien") si

$$A = 2g - 2 + k + \sum_{i=1}^{\ell} \left(1 - \frac{1}{e_i}\right) > 0$$

(ce revêtement est S_2 si $A < 0$
$\mathbb{C}$ si $A = 0$)

Dans le cas $A > 0$, G est un groupe fuchsien de 1ère espèce, et on les trouve tous ainsi.

les points elliptiques $\to e_i$

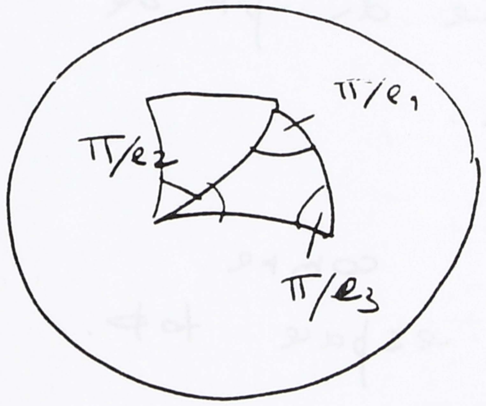
Cas fuchsien : Aire $(D/G) = 2\pi A$.

$A < 0$, $g = 0$, $k = 0$,

$$\sum \left(1 - \frac{1}{e_i}\right) < 2 .$$

$l \geq 3$, $e_i \geq 2$

$$\Longrightarrow \quad l = 3, \quad \frac{1}{e_1} + \frac{1}{e_2} + \frac{1}{e_3} > 1$$



triangle sphérique

pavage de la sphère

G' engendré par les symétries

$\cup$

G s/g respectant l'orientation

$$S_2 / G \simeq \text{surface de Riemann}$$

G s/g$^{\text{fini}}$ (non cycliques) de $PGL_2(\mathbb{C})$

de $SO_3(\mathbb{R})$

liste : $(e_1\ e_2\ e_3)$

$(2,2,n)$	diédral D_n	groupe de rotation
$(2,3,3)$	A_4	
$(2,3,4)$	S_4	(Schwartz)
$(2,3,5)$	A_5 .	

Présentation de A_5 :

t_1, t_2, t_3 $\quad t_1^2 = 1, \ t_2^3 = 1, \ t_3^5 = 1$

$t_1 t_2 t_3 = 1$.

Oubli :

$X \subset \overline{X}$ compacte

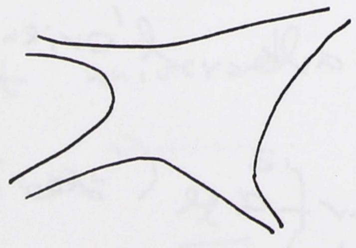
$\overline{X} - X =$ fini.

compactification est unique du pt de vue analytique complexe.

1.) top. de $X \longrightarrow \overline{X}$ comme espace top.

Espace des bouts (compl. de compacts)

$\in$ bouts



"compactification par les bouts.

$\overline{X} = X \cup$ bouts de X.

Fct hol. sur ouvert de $\overline{X}$: cont et restriction à X est holomorphe.

donc str. analytique déterminée.

Tout isom. (anal. complexe) entre c. alg. affines lisses sur $\mathbb{C}$ est algébrique.

(si on supprime lisse, l'énoncé devient faux).

Prochaine fois : $x_1 \cdots x_k = 1$

les compter ? rigidité ...

23/10/89

Formules d'intégration

Groupes compacts

G avec mesure de Haar de masse 1.

$\int_G f(x)\,dx$ définie au moins si f continue...

" $\int_{x\in G} f(x) = \int_x f(x)$ ... selon le cas.

Représ. irréductible ρ de G

$\chi =$ caractère de ρ

$\int_{t\in G} \rho(txt^{-1}) = \lambda . 1$ (lemme de Schur)

Trace $\Rightarrow$ $\int_{t\in G} \chi(x) = \chi(x) = \lambda\chi(1)$

d'où $$\boxed{\int_{t\in G} \rho(txt^{-1}) = \frac{\chi(x)}{\chi(1)} . 1}$$

$$\int_{t\in G} \rho(txt^{-1})\rho(y) = \frac{\chi(x)}{\chi(1)}\rho(y)$$

Trace $\Rightarrow$ $$\boxed{\int_t \chi(txt^{-1}y) = \frac{\chi(x)\chi(y)}{\chi(1)}}$$

Par récurrence : x_i $i = 1, \dots, k$ $x_i \in G$

$t_i x_i t_i^{-1}$

$$\boxed{\int_{t_1}\dots\int_{t_k} \chi(t_1x_1t_1^{-1}.\, t_2x_2t_2^{-1} \dots t_kx_kt_k^{-1}.\, y) = \frac{\chi(x_1)\dots\chi(x_k)\chi(y)}{\chi(1)^k}}$$

$$\int_{t,x} \rho(txt^{-1}x^{-1}) = \int_x \frac{\chi(x)\rho(x^{-1})}{\chi(1)} = \frac{1}{\chi(1)^2}$$ 38

(car c'est une constante – commute à tout ce qu'on veut !, donc Schur – et la trace sort du calcul ci-dessous)

$$\int_{t,x} \chi(txt^{-1}x^{-1}) = \int_x \frac{\chi(x)\chi(x^{-1})}{\chi(1)} = \frac{1}{\chi(1)}$$

D'où :

$$\int_{t,x} \chi(txt^{-1}x^{-1}y) = \frac{\chi(y)}{\chi(1)^2}$$

$$\boxed{\int_{\substack{t_1 \dots t_g \\ x_1 \dots x_g}} \chi((t_1,x_1)\dots(t_g,x_g)\cdot y) = \frac{\chi(y)}{\chi(1)^{2g}}}$$

$z_1, \dots, z_k \in G$ fixés

$$\int_{\substack{u_1 \dots u_g \\ v_1 \dots v_g \\ t_1 \dots t_k}} \chi\left(\prod_{i=1}^{g} (u_i, v_i) \cdot \prod_{j=1}^{k} t_j z_k t_j^{-1} y\right) = \frac{\chi(z_1)\dots\chi(z_k)\chi(y)}{\chi(1)^{2g+k}}$$

On en déduit des formules pour f = fction centrale sur G,

$$f = \sum c_\chi \chi \qquad \left(\text{avec } \sum |c_\chi|\,\chi(1) < \infty \text{ par exemple}\right)$$

$$\boxed{\int_{u,v,t} f\left(\prod (u_i, v_i) \prod_{j=1}^{k} t_j z_j t_j^{-1} y\right) = \sum_\chi c_\chi \frac{\chi(z_1)\dots\chi(z_k)\chi(y)}{\chi(1)^{2g+k}}}$$

Groupes finis (39)

$$f = \text{"Dirac"} = \begin{cases} 1 \text{ en l'élément neutre} \\ 0 \text{ ailleurs} \end{cases}$$

$$f = \sum_{\chi \text{ irred}} \frac{\chi(1)}{|G|}\chi$$

$N = N(g, z_j, y)$ = nbre des (u_i, v_i, t_j) pour lesquels

$$\prod_i (u_i, v_i) \prod_j t_j z_j t_j^{-1} = y^{-1}$$

Alors $\quad N = |G|^{2g+k} \int_{u,v,t} f(\quad)$

$$\boxed{N = |G|^{2g+k-1} \sum_{\chi \text{ irred}} \frac{\chi(z_1) \dots \chi(z_k)\chi(y)}{\chi(1)^{2g+k-1}}}$$

<u>Cas particulier</u>

Le nombre des (u_i, v_i) $(1 \leq i \leq g)$ tels que

$$y = \prod_{i=1}^{g} (u_i, v_i)$$

est égal à $\quad |G|^{2g-1} \sum_{\chi \text{ irred.}} \frac{\chi(y)}{\chi(1)^{2g-1}}$.

En particulier y est un produit de g commutateurs si et seulement si $\sum_{\chi \text{ irred}} \chi(y)/\chi(1)^{2g-1} \neq 0$;

<u>y est un commutateur ssi</u> $\sum_{\chi \text{ irred.}} \chi(y)/\chi(1) \neq 0$.

Théorem (...) : G simple non abélien ; tout élément de G est un commutateur. (40)

(à partir de la table des caractères)

Monstre $\quad \Sigma\, \chi(y)/\chi(1) = 1 + \sum_{\chi \neq 1} \frac{\chi(y)}{\chi(1)}$

~180 classes

$$y \neq 1 : \left|\frac{\chi(y)}{\chi(1)}\right| < \frac{1}{200} \quad (\text{à 2 exceptions près})$$
$\chi \neq 1$

donc $1 + \sum_{\chi \neq 1} \frac{\chi(y)}{\chi(1)} \neq 0$!

$g = 0 \qquad k$ quelconque $\qquad y = 1$

$z_1, \dots, z_k$ donnés

$N =$: nbre de $t_1, \dots, t_k$ tels que $\prod_{j=1}^{k} t_j z_j t_j^{-1} = 1$

$$N = |G|^{k-1} \sum_{\chi} \frac{\chi(z_1) \dots \chi(z_k)}{\chi(1)^{k-2}}$$

Appelons C_j la classe de conjugaison de z_j.

$M = M(C_1, \dots, C_k) =$ nbre des $(c_1, \dots, c_k)$ dans $C_1 \times \dots \times C_k$

avec $c_1 \dots c_k = 1$.

$Z_j =$ centralisateur de $z_j \qquad C_j = G/Z_j \qquad |C_j| = |G|/|Z_j|$

$$M = N / \prod_{j=1}^{k} |Z_j|$$

Formule pour M :

$$M = \frac{|G|^{k-1}}{\pi |Z_j|} \sum_{\chi} \frac{\chi(z_1) \dots \chi(z_k)}{\chi(1)^{k-2}}$$

$$\boxed{M = \frac{1}{|G|} \prod_{j=1}^{k} |C_j| \sum_{\chi} \frac{\chi(z_1) \dots \chi(z_k)}{\chi(1)^{k-2}}}$$

Variante

On donne $g, k, C_1, \dots, C_k$.

$M = M(g, C_1, \dots, C_k) =$ nbre des u_i, v_i $(1 \leq i \leq g)$

et $c_j \in C_j$ avec $\prod_{i=1}^{g} (u_i, v_i)\, c_1 \dots c_k = 1$

avec $M = |G|^{2g-1} \prod |C_j| \sum_{\chi} \dfrac{\chi(z_1) \dots \chi(z_k)}{\chi(1)^{2g+k-2}}$ $z_j \in C_j$

X surface de Riemann

$= \overline{X}_{\text{compacte}} - \{P_1, \dots, P_k\}$

x_0 point de X

$\pi_1(X, x_0)$ est présenté par $2g+k$ générateurs $\tilde{u}_i, \tilde{v}_i, \tilde{c}_j$ avec la relation usuelle

"Un lacet autour de P_i" définit une classe de conjugaison $\tilde{C}_j$ bien déterminée dans le π_1.

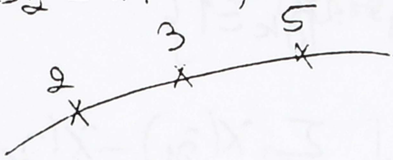
G, u_i, v_i, c_j $=$ se donner un homomorphisme de $\pi_1(X; x_0)$ dans G appliquant $\tilde{C}_j$ dans C_j.

Malheureusement, comment calculer le nbre des u_i, etc. donnant homom ~~des~~ sur G ? On peut tjrs dans la pratique calculer les nbres associés aux ss-gpes de G et conclure...

La table des caractères de G permet de calculer le nombre des sgpes de G isomorphes à A_5.

En effet A_5 a une présentation $x^2=1$ $y^3=1$ $z^5=1$ $xyz=1$

$S_2 = P_1(\mathbb{C})$ on enlève 3 pts



$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5} > 1$$

Le revêtement associé est P_1

gpe $A_5 \hookrightarrow PGL_2(\mathbb{C})$

On choisit ds G (quelconque) C_1, C_2, C_3 avec des élts d'ordre resp. 2, 3, 5 et on calcule le nbre des (g_1, g_2, g_3) dans $C_1 \times C_2 \times C_3$ avec $g_1 g_2 g_3 = 1$ par une formule précédente.

Idem pour A_4, S_4, diédral.

Rigidité

G gpe fini

On suppose le centre $Z(G)$ de G trivial.

Soient $C_1, \dots, C_k$ des classes de conjugaison

$$\overline{\Omega} = \{ z_1 \in C_1, \dots, z_k \in C_k \ ; \ z_1 \cdots z_k = 1 \}$$

$$\overset{\shortparallel}{\overline{\Omega}}(C_1, \dots, C_k)$$

$|\overline{\Omega}|$ calculé par $\dfrac{1}{|G|} |C_1| \cdots |C_k| \displaystyle\sum_\chi \frac{\chi(z_1) \cdots \chi(z_k)}{\chi(1)^{k-2}}$

Ω ss-ensemble de $\overline{\Omega}$ formé des élts $z_1, \dots, z_k$ qui engendrent G

$$G = \langle z_1, \dots, z_k \rangle.$$

G opère par automorphismes intérieurs sur $\overline{\Omega}$ et Ω.

$$s \in G, \quad (z_1, \dots, z_k) \longmapsto (s z_1 s^{-1}, \dots, s z_k s^{-1}).$$

opère librement sur Ω ;

si s commute à tous les z_i, il commute à G or $Z(G) = \{1\}$.

Définition $(C_1, \dots, C_k)$ est rigide si $\Omega \neq \emptyset$ et G opère transitivt sur Ω $\iff |\Omega| = |G|$.

strictt rigide si rigide (et si $\overline{\Omega} = \Omega$.

rigide $\Rightarrow |\overline{\Omega}| \geq G$

st rigide $\Rightarrow |\overline{\Omega}| = |G|$.

Dans la plupart des applications $k = 3$ ($k = 1$ ou 2 trivial !)

Rigidité du problème des revêtements

$$S_2 \left(= \mathbb{P}_1(\mathbb{C})\right) - \{P_1, \dots, P_k\} \qquad P_i \neq P_j \quad \text{si } i \neq j$$

X — revêt galoisien à gpe G

$\downarrow G$ — X projective lisse, connexe

$\mathbb{P}_1$ — G opère sur X fidèlement $X/G = \mathbb{P}_1$

librement en dehors des fibres au-dessus de P_i

On demande que la classe de conjugaison dans G de "tourner autour de P_i" soit C_i.

<u>Remarque</u> : le groupe d'inertie d'ordre $e \hookrightarrow \mu_e$ a un générateur canonique (ds $\mathbb{C}$)

Avec les conventions choisies, identif "générateur inertie et "tourner autour de P_i" donne le signe $-$.

<u>Théorème</u> – Si $(C_1, \dots, C_k)$ est rigide, il <u>existe un</u> <u>G-revêtement</u> X <u>du type ci-dessus</u> <u>et un seul</u> <u>à</u> isom près.

Il s'agit d'<u>isom</u> de G-<u>revêt</u> : $\exists!\ \varphi : X \to X'$ commute à l'action de G

$$\begin{tikzcd} X \arrow[rr, "\varphi"] \arrow[dr, "G"'] & & X' \arrow[dl, "G"] \\ & \mathbb{P}_1 & \end{tikzcd}$$

(Si le centre $\neq 1$ (était), automorph. du revêt non trivial.)

iso de G-revêt X et X' $\Leftrightarrow$ $\begin{cases} \cdot\ G\text{-isom de } X \text{ et } X' \\ \cdot\ \forall\ G\text{-auto de } X \text{ est trivial.} \end{cases}$

Ceci traduit en fait exactement la rigidité.

Idée de démonst : $x_0 \in \mathbb{P}_1(\mathbb{C}) - \{P_1, \dots, P_k\}$.

$$\begin{array}{cccc} x_1 \in & X_1 & X_2 & \ni x_2 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ x_0 & \mathbb{P}_1 & \mathbb{P}_1 & x_0 \end{array}$$

$\pi_1 \xrightarrow{\theta_1} G$ associé à X_1, x_1

$\pi_1 \xrightarrow{\theta_2} G$ " X_2, x_2.

Il existe $s \in G$ $\quad \theta_2(x) = s\,\theta_1(x)\,s^{-1}$.
Quitte à chger le pt x_2, on peut supposer que $\theta_2 = \theta_1$

Rationalité dans un groupe fini

G gpe fini
N tq $s^N = 1$ pour tout $s \in G$
$\Gamma_N = (\mathbb{Z}/N\mathbb{Z})^*$ opère sur G (comme ensemble)
$\alpha \in \Gamma_N \quad s \in G \longmapsto s^\alpha \in G$

$Cl(G)$ = cl. de conjugaison de G
Γ_N agit sur $Cl(G)$
Une classe $C \in Cl(G)$ est dite $\mathbb{Q}$-rat. (ou rat.) si elle est fixe par Γ_N
(i.e. si $s \in C$, tt générateur du gpe cyclique $\langle s \rangle$ appartient à C.)

Si k est un corps, notion de k-rationalité
$$\mathrm{Gal}(k(\mu_N)/k) \subset \Gamma_N$$
$$\parallel$$
$$\Gamma_N(k)$$
Une classe $C \in Cl(G)$ est dite k-rationnelle si elle est fixée par $\Gamma_N(k)$

k car 0, $\bar{k}$ = cl. alg.
$X(G)$ = ens. des caractères irréduct de G sur $\bar{k}$
Proposition Une classe de $C \in ClG$ est k-rationnelle si et seulement si pour $c \in C$ et $\chi \in X(G)$, $\chi(c)$ appartient à k.

En particulier C est rationnelle (sur $\mathbb{Q}$) $\Leftrightarrow \chi(c) \in \mathbb{Q}$ pour tout χ $\Leftrightarrow \chi(c) \in \mathbb{Z}$ pour $\forall \chi$.

Démonstration: $\alpha \in \Gamma_N(k) \simeq \mathrm{Gal}(k(\mu_N)/k) \Rightarrow \sigma_\alpha$

$\sigma_\alpha(z) = z^\alpha$.

$$\boxed{\sigma_\alpha \chi(c) = \chi(c^\alpha)}$$

car $\chi(c)$ est la Σ des val. propres

Si C k-rationnelle, c^α est un conjugué de c

$\chi(c^\alpha) = \chi(c)$, donc $\chi(c) \in k$.

Récipt: deux élts non conjugués st séparés par un caractère.

Γ_N agit sur $Cl\, G$ et $X(G)$

Est-ce que $Cl(G)$ et $X(G)$ sont isomorphes comme Γ_N-ensembles? (Non: chercher de Thompson)

Réinterprétation en termes d'algèbres étales:

$Cl(G) \longmapsto \mathbb{Q} \otimes R(G)$, où $R(G)$ = anneau des caractères de G.

$X(G) \longmapsto Z\mathbb{Q}[G]$, centre de $\mathbb{Q}[G]$

La question équivaut à celle-ci: est-ce que les $\mathbb{Q}$-algèbres commutatives étales $\mathbb{Q} \otimes R(G)$ et $Z\mathbb{Q}[G]$ sont isomorphes? (Non, en général.)

Par contre $Cl(G)$ et $X(G)$ sont "faiblement" isomorphes, i.e les représentations linéaires de Γ_N associées sont isomorphes.

Exemples

1) $G = S_m$ ttc classe est rationnelle

2) $G = A_5$ 1, 2, 3, 5A, 5B ("2 classes d'élts d'ordre 5).

si $s \in 5A$ $s^{-1} \in 5A$ mais $s^2, s^3 \in 5B$

5A et 5B ne sont pas rationnelles (le sont sur $\mathbb{Q}(\sqrt{5})$)

critère pour distinguer 5A et 5B

$s \in A_5$ (1, 2, 3, 4, 5) d'ordre 5

$X_1 \dots X_5$ 5 var indépendantes.

on pose : $D = \prod_{i<j} (x_j - x_i)$ D inv. par A_5

$$\prod_{1 \le i < j \le 5} (s^j x_j - s^i x_i) = \varepsilon(s) D \qquad \varepsilon(s) = \pm 1$$

$\begin{cases} \varepsilon(s) = 1 & \text{pour l'une des 2 classes} \\ -1 & \text{pour l'autre} \end{cases}$

Ceci intervient ds des calculs de J. Buhler

$$\begin{array}{c} K \\ A_5 \,| \\ \mathbb{Q} \end{array} \qquad Cl(\mathrm{Frob}_p) \; ?$$

$\uparrow$ non ramifié

si la classe est d'ordre 5 ; comment la déterminer

$x_1, \dots x_5 \in \overline{\mathbb{F}}_p$

$\downarrow$

$$\prod_{1 < i < j \le 5} (x_j^{p^j} - x_i^{p^i}) \equiv \pm D \mod p$$

Rationalité des groupes d'inertie dans le cas local

$$\begin{array}{ccc} \ell & & L \\ | & & | \\ k & & K \end{array}$$

extension galois G de corps locaux. modérément ramif. I = gpe d'inertie ($|I|$, car rés) = 1

Proposition Les classes de conjugaison dans G des élts de I sont rationnelles sur k.

(en particulier, si $k = \mathbb{Q}$, elles sont rationnelles)

Conséquence:

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

ram. rationn. sur $\mathbb{Q}$ $\Rightarrow$ inertie correspdte rationn. / $\mathbb{Q}$

en appliq^{r} la prop au gpe de décomp.

Idée de la preuve.

Si π est une uniformisante de L, et si $s \in I$, l'image ds l de $\frac{s\pi}{\pi}$ ne dépend pas du choix de π, c'est une racine de l'unité et l'on obtient ainsi un isomorphisme $\theta : I \xrightarrow{\sim} \mu_e(\ell)$, avec $e = |I|$.

Cette identification θ est compatible à l'action de G

$x \in G$ $\quad \theta(x s x^{-1}) = \sigma_x \theta(s)$ $\quad \sigma_x$: autom de l/k défini par x.

$\alpha \in Gal(k(\mu_e)/k)$

$\theta(x s x^{-1}) = \theta(s^{\alpha})$ et θ injectif $\Rightarrow$ $x s x^{-1} = x^{\alpha}$

la proposition en résulte.

...rre 30/10/89.

Rigidité (...compléments) $\Omega(C_1, \dots, C_k)$ $\quad \Omega \subset \overline{\Omega}$

$\overline{\Omega}(C_1, \dots, C_k)$ $\quad (x_1, \dots, x_k)$ eng. G

C_i cl. de conj. G

$x_1, \dots, x_k \quad x_i \in C_i$

$x_1 \cdots x_k = 1$

centre $G = 1$

G opère transitivt sur Ω, $\Omega \neq \phi \Rightarrow |\Omega| = |G|$.

Remarques 1) $|\Omega(C_1, \dots, C_k)| = |\Omega(C_{\sigma_1}, \dots, C_{\sigma_k})|$.

idem sur $\overline{\Omega}$

rigidité.

En effet si $x_1, \dots, x_k$ $\quad x_i \in C_i \quad x_1 \dots x_k = 1$

on cherche $y_j \in C_{j+1}$

$y_{j+1} \in C_j$

la formule $x_1 \cdots x_k = 1$ s'écrit $x_1 \dots x_{j-1} \cdot x_j x_{j+1} x_j^{-1} \cdot x_j x_{j+1} \dots x_k = 1$.

d'où
$$y_j = x_j x_{j+1} x_j^{-1}$$
$$y_{j+1} = x_j$$
$$y_i = x_i \qquad \text{si } i \neq j, j+1$$

Donc résultat marche sur transpositions, donc sur $\mathfrak{S}_n$ qui est engendré par transp.

Action du gpe des tresses, cf exposé de G. Malle bientôt.

2) N $\quad \Gamma_N = (\mathbb{Z}/N\mathbb{Z})^\times$ opère sur l'ensemble G et aussi sur $\mathcal{C}\ell G$

On a : $|\Omega(C_1^\alpha, \dots, C_k^\alpha)| = |\Omega(C_1, \dots, C_k)|$, $\alpha \in \Gamma_N$.

idem pour $\overline{\Omega}$

rigidité.

$\alpha = -1$: $x_1 \dots x_k = 1 \Rightarrow x_k^{-1} \cdots x_1^{-1} = 1$ et on peut "remettre ds l'ordre par ce qui précède

(Le cas général)

(Résulte des formules sur les caractères (50)

(évident pour $\bar{\Omega}$, par récurrence sur sous-gpes pour Ω)

Se fait aussi par méthode géométrique:

Théorème : Soit F le groupe libre présenté par k générateurs $x_1, \dots, x_k$ avec relation $x_1 \cdots x_k = 1$.

Soit $\hat{F}$ son complété profini

Soit $\alpha \in \hat{\mathbb{Z}}^* = \prod_p \mathbb{Z}_p^*$

Il existe un automorphisme θ de $\hat{F}$ tel que $\theta(x_i) \in$ cl. de conjugaison de x_i^α.

ou encore:

$\Leftrightarrow$ il existe ds $\hat{F}$ des y_i, conjug. de x_i^α, $y_1 \cdots y_k = 1$, et $\hat{F}$ eng (top.) par $y_1 \cdots y_k$

De tels y définissent en effet $\hat{F} \xrightarrow[\text{surj}]{} \hat{F}$, or surj $\Rightarrow$ bij sur gpes profinis, topol. engendrés par un ensemble fini d'éléments.

cf la dém. la semaine prochaine

Exemples ds S_n, A_5, $PSL_2(\mathbb{F}_p)$, $SL_2(\mathbb{F}_8)$, J_1, J_2, M.

1. S_n

C_1, C_2, C_3 $\quad$ $n \geq 3$

$C_1 = Cl(12)$
$C_2 = Cl(12 \dots n-1)$
$C_3 = Cl(12 \dots n)$
| cycles

Prop. (C_1, C_2, C_3) est (strict.) rigide.

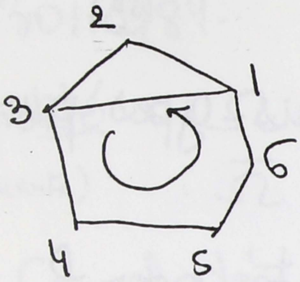
Principe (caractères): χ irréductible de S_n de degré > 1.

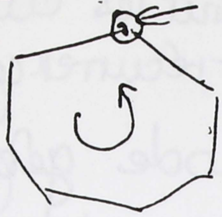
on a $\chi((1 - n-1))$ ou $\chi((1 \dots n)) = 0$ (disent les spécialistes ...)

$$|\bar{\Omega}| = \frac{|G|^2}{|Z_1||Z_2||Z_3|} \sum_\chi \frac{\chi(z_1)\chi(z_2)\chi(z_3)}{\chi(1)}$$

$$= |G| = n!$$

Méthode unicité





1er point rencontré (d'où unicité).

Il y a un revêtement non galoisien :

$$\begin{array}{ccc} x & & X \\ & & \Big|\, n \\ T & & \mathbb{P}_1 - \{3 \text{ pts}\} \end{array}$$

$n-1 \quad n$

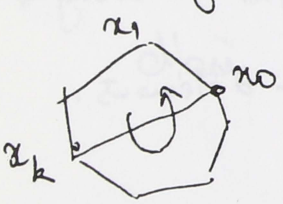
$0, \lambda, \infty$

$T = X^n + X^{n-1}$

C_2 remplacé par $(1 \ldots k)(k+1 \ldots n)$

avec $(k, n) = 1$. $\quad k < n/2$.

aussi rigide



Il faut prendre cette fois des pts distincts de k.

Si $(k, n) \neq 1$ $\quad |\Omega| = G$ mais les élts n'engendrent pas le groupe.

② A_5 $\quad$ 1A $\quad$ 2A $\quad$ 3A $\quad$ 5A $\quad$ 5B

$(1) \quad (12)(34) \quad (123) \quad (12345) \quad (13524)$

	1A	2A	3A	5A	5B
χ_1	1	1	1	1	1
χ_2	3	-1	0	z	z'
χ_3	3	-1	0	z'	z
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

$z = \dfrac{1+\sqrt{5}}{2}$

$z' = \dfrac{1-\sqrt{5}}{2}$

$\chi_5 : A_5 \hookrightarrow A_6$

Ordre des centralisat. resp $60, 4, 3, 5, 5$.

Triplets rigides dans A_5

Remarque : Si $C_1, \dots, C_k$ est rigide et si σ est un automorphisme externe du groupe G, on a $\sigma(C_i) \neq C_i$ pour au moins un i

$x_1, \dots, x_k \quad \sigma x_1, \dots, \sigma x_k = \mathrm{Int}(g)\,(x_1, \dots, x_k)$

$\Rightarrow \sigma = \mathrm{Int}\, g$ (car les x_i eng le gpe et le centre est trivial)

impossible.

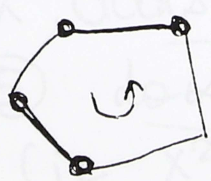
donc triplet rigide contient 5A ou 5B

On a rigidité pour :

2	3	5
3	3	5
2	5A	5B
3	5A	5B
3	5A	5A
5A	5A	5A.

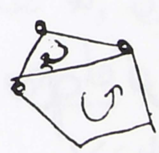
(On peut vérifier par la formule des caractères).

Se voit aussi sur dessins

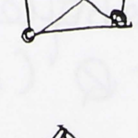


(2, 3, 5)

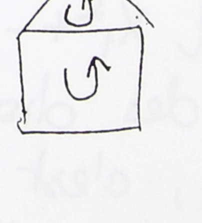
<– 1 seul pt exclus fixe la situation !



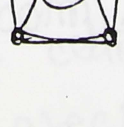
3 3 5



2 5A 5B



3 5A 5B



3 5A 5A

Revêtements associés

2, 3, 5A non réalisable sur $\mathbb{Q}$
car les 3 pts de ramif seraient rationnels
mais "5" ne peut l'être
$\mathbb{P}_1 / \mathbb{Q}(\sqrt{5})$.

On a X de genre 0. $A_5 \hookrightarrow PGL_2(\mathbb{C})$ donc opère sur dte proj.

$$S_5 \left(\begin{array}{c} X \\ |A_5 \\ \mathbb{P}_1/\mathbb{Q}(\sqrt{5}) \\ | \\ \mathbb{P}_1/\mathbb{Q} \end{array} \right. \qquad \begin{array}{c} K \\ | \\ \mathbb{Q}(T, \sqrt{5}) \\ | \\ \mathbb{Q}(T) \end{array}$$

$$\begin{array}{ccc} X & & \mathbb{P}_1 \\ \downarrow & \Longrightarrow & \downarrow \\ \mathbb{P}_1 \ / \mathbb{C} & & \mathbb{P}_1 \simeq \mathbb{P}_1/A_5 \end{array}$$

X n'a pas de pt rationnel $/ \mathbb{Q}(\sqrt{5})$
élt d'ordre 2 de $Br(\mathbb{Q}(\sqrt{5})) \to (-1,-1)$.
$\Updownarrow$
inv. locaux 0 sauf aux 2 places ∞ l'∞.

Construction de X :

$\mathbb{P}_4$ $\begin{cases} X_1 + \dots + X_5 = 0. \\ X_1^2 + \dots + X_5^2 = 0. \end{cases}$ quadrique ds $\mathbb{P}_3$

Courbe des droites de cette quadratique (2 courbes sur $\mathbb{C}$), c'est X ; irréductible sur $\mathbb{Q}$ (et pas abst irréd), avec action de S_5.

Autre construction : corps des fonctions modulaires de niveau 5

$C_2 \subset GL_2(\mathbb{F}_5)/\{\pm 1\}$ $\qquad PGL_2(\mathbb{F}_5) \simeq S_5$
centre

lien avec la "résolution" de l'équation du 5^e degré.

équation sur k $k \ni \sqrt{5}$

à groupe de Galois A_5 $\quad$? $\quad X \xrightarrow{A_5}$

$t \mapsto$ algèbre étale de $d^o\ 5$ $\quad$ $t \in \mathbb{P}_1 / k$

(GO si on veut galoisien)

Pb: si $K|k$ est de degré 5, à discriminant carré, (et $\sqrt{5} \in k$) à quelle cond $K|k$ provient-il du revêtement "de Klein" ?

Thme Les propriétés suivantes sont équivalentes

① $K|k$ est du type de Klein

② On peut définir K par une équation de la forme $X^5 + a_2 X^2 + a_1 X + a_0 = 0$.

③ Il existe $x \in K$, $x \neq 0$ avec $\mathrm{Tr}\, x = 0$ et $\mathrm{Tr}\, x^2 = 0$.

④ L'invariant de Witt de la forme $\mathrm{Tr}\, x^2$ associé à K, dans le groupe de Brauer de k, est $(-1,-1)$.

⑤ La forme $\mathrm{Tr}(x^2)$ est isomorphe à $\langle 1\rangle \oplus \langle 1\rangle \oplus \langle 1\rangle \oplus \langle -1\rangle \oplus \langle -1\rangle$ (ie $X^2+Y^2+Z^2-U^2-V^2$).

Dém. • (2) $\Leftrightarrow$ (3) $\Rightarrow$ 4) $\Rightarrow$ 5)

• $k.1 \oplus \{\mathrm{Tr} = 0\} = K$

$$\mathrm{Tr}\, x^2 = \langle 1 \rangle \oplus \underbrace{\mathrm{Tr}_0\, x^2}$$

(5 est un $\square$)

discriminant 1

4 variables

donc cette forme doit être hyperbol., inv de Witt $= (-1,-1)$

• lien avec (1)

$\underbrace{K^{gal} / k}_{A_5}$ $\quad$ X tordue par $K|k$ a des pts rationnels $\Leftrightarrow$ $K|k$ Klein

inv. de cette tordue $(-1,-1) + w_2(\mathrm{Tr}\, x^2)$

<u>Corollaire</u> : Quitte à faire une extension quadratique de k, V_1/k est du type de Klein. "akzessorische Irrat."

(On "tue" l'élt de Brauer, ou on donne un pt à la quadrique).

En résumé : $\sqrt{5} \in k$, $\sqrt{d} \in k$ + "irrationalités accessoires" servant à tuer un élt du gpe de Brauer.
disc

Table des caract. de J_1 en entrocte

J_1	175560.	120	30	30 ← central.	
	1	2	5A	5B	
	1	1	1	1	
	76	4	1	1	$b = \frac{-1+\sqrt{5}}{2}$
	76	-4	1	1	$b' = \frac{-1-\sqrt{5}}{2}$
	77	5	2	2	
	77	-3	b	b'	
	77	-3	b'	b	
	133	+5	-2	-2	
	133	-3	$-b$	$-b'$	
	133	-3	$-b'$	$-b$	
	209	1	-1	-1	

<u>Retour sur A_5</u>, suite et fin

2, 5A, 5B

$A_5 \subset S_5$

X courbe de Bring de genre 4

$$\begin{cases} \Sigma x_i = 0 \\ \Sigma x_i^2 = 0 \\ \Sigma x_i^3 = 0 \end{cases}$$

$$\begin{array}{c} X \\ A_5 \big| \\ P_1 \\ \big| \\ P_1/Q \end{array} \quad S_5$$

genre

2	3	5	0	0
~~2~~ 3	3	5	0	5
2	5A	5B	1	4
3	5A	5B	1	9
3	5A	5A	1	9.
5A	5A	5A	2	13

$K|k$ ext de degré 5 type Bring ⟺ obt par une équation $X^5+aX+b=0$.

Thme Après ext quadratique et cubique, tte équation de d^o 5 se ramène à cette forme

Thme Tte courbe de genre 4 a des pts rationnels après ext quad. et cub. convenables.

Si courbe de genre 4 hyperelliptique, c'est un revêtt double de $\mathbb{P}_1$

sinon intersection d'une quadrique et d'une cubique on trouve des dtes de la quad après exts quadr.; ces dtes coupent la cubique sur de ext. cubiques.

On arrive à $\boxed{J_1}$: gpe sporadique $|G|=175560$.

15 classes de conjug

la table écrite + ht est partielle (on a éliminé les cas où le produit des X est nul entre autres)

On trouve $N = |G|\,\frac{5}{2}$ (2, 5A, 5B) n'est pas strict rigide

ds A_5, il y a 2, 5A, 5B $A_5 \subset J_1$

Plus précisément il y a 2 classes de A_5 ds J_1

Dans l'une de ces classes ; centralisateur $= C_2 = \{1,-1\}$
l'autre, — $= \{1\}$

le nbre des A_5 du 1er type est $|G| / \underbrace{2.A_5}_{|\text{normalisateur}|}$

2e type est $|G| / \widehat{A_5}$

Chaque A_5 donne $|A_5|$ triplets $(x,y,z) \in \overline{\Omega}$ avec $\langle x,y,z\rangle = A_5$

soit $|G|/2A_5 \times |A_5| + \dfrac{|G|.|A_5|}{|A_5|} = |G|\dfrac{3}{2}$

Reste donne $|G|$ triplets ; ils engendrent G (sinon $\subset$ ss gpes max ; on regarde ds carte : seules possibilités $C_2 \times A_5$, déjà considéré ou $PSL_2(\mathbb{F}_{11})$ et il faut étudier ce cas. les 2 classes de $\hat{A}_5$ contenues dedans ont en fait été déjà traitées) d'où la rigidité.

Référence : [Ho] J. of Algebra

J_2 y est aussi traité

$\boxed{J_2}$: 604800 5A 5B 7

	7	300	300
604800			
1	7	5B	5A
1	1	1	1
36	1	-4	-4
90	-1	5	5
160	-1	-5	-5
288	1	3	3

$N = |G|$

les ss gpes max de G ne st pas d'ordre divisible par 35.

Tout ceci fait partie d'un vaste programme de Matzat et ses élèves.

Par ex $2A$, $3B$, $29A$ classes "rigide" du monstre
Difficulté car on ne dispose pas de la liste des ss-gpes max du monstre. On doit étudier struct du gpe engendré et la classific. des gpes simples.

$\boxed{PSL_2(\mathbb{F}_p)}$

Ici, la rigidité donne un peu moins que le modulaire
p premier $\neq 2,3$

$2A$ ordre 2
$3A$ ordre 3
$\left.\begin{matrix} pA \\ pB \end{matrix}\right\}$ ordre p

En relevant à $SL_2(\mathbb{F}_p)$ $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \sim pA$

$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \sim pB$ si $\left(\frac{\lambda}{p}\right) = -1$

Thme: Les triplets suivants sont strictement rigides:
$(2A, 3A, pA)$
$(2A, pA, pB)$ si $\left(\frac{2}{p}\right) = -1$.
$(3A, pA, pB)$ si $\left(\frac{3}{p}\right) = -1$.

Le 1e cas ne donne pas des ext rationnelles à cause de pA
2e et 3e cas oui car classes pA, pB non conjug, mais on retrouve extensions de Shih de niveau resp 2 et 3.

Preuve: $x = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ $y = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ $z = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
$xyz = 1$.

A montrer x', y', z' ds G chacun conjugué de ce qu'il faut
$$x'y'z' = 1.$$
alors (x', y', z') est G-conj de (x, y, z)

z' unipotent $\qquad z' = z \qquad$ ~~dte x(droite)~~

$$x' = \begin{pmatrix} 0 & \lambda \\ -\lambda^{-1} & 0 \end{pmatrix} \qquad z' = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} = z \qquad \mu = \square$$

On peut se ramener à $\mu = 1$.
Le produit de x et z est d'ordre 3. $\quad \mathrm{Tr}(x'z) = \lambda^{-1} = \pm 1$
d'où $x' = x$ de départ. $\quad \Rightarrow \lambda = \pm 1$

<u>Cas</u> 2A, pA, pB

$$x = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} \qquad y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad z = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \quad \in \Gamma_0(2)$$

$\qquad\qquad pA \qquad\qquad pB$) conjug.

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \qquad \left(\frac{2}{p}\right) = -1$$

$xyz = 1.$

A conj près, il n'y a là encore que cela.
x', y', z' $\qquad$ y' et z' unipotents, fixent 2 dtes $\neq$
on les prend comme coordonnées

$$y' = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \qquad z' = \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix}$$

$\mathrm{Tr}(x'y'z') = 0 \Rightarrow \lambda\mu = -2$
$\lambda = \square$ (on peut conjuguer pour avoir $\lambda = 1$)
d'où $\mu = -2$ cqfd.

Même raisonnement <u>pour</u> 3A, pA, pB.

2A, 3A, pA correspond au corps de fctions modulaires de niveau p.
On reconnait la ramif habituelle 3 en 0, 2 en 1728, p en ∞. Le corps de base est $\mathbb{Q}(\sqrt{\pm p})$, signe selon que $p \equiv 1, 3 \mod 4$.

Hecke $/\mathbb{C}$

$$\begin{array}{c} PSL_2(\mathbb{Z}) \\ \downarrow \\ PSL_2(\mathbb{Z}/p\mathbb{Z}) \end{array}$$

Prop : unicité de ce revetᵗ par essentiellᵗ rigidité

$\boxed{SL_2(\mathbb{F}_8)}$ 504

9A 9B 9C

Cartan non déployé (ordre $q+1=9$)
Corps de rationalité sur le corps cubique $\mathbb{Q}(\cos\frac{2\pi}{9})$.
Elles forment un triplet strict rigide.

6.III.99

Revêtements

Revêt topolog (finis) $\Longleftrightarrow$ revêtements algébriques / sur $\mathbb{C}$

$$\widehat{\pi}_1 = \varprojlim_{\substack{H \text{ indice} \\ \text{fini normal}}} \pi_1/H$$

Rappel $\Gamma = \pi_1(X_g - \{P_1, \dots, P_k\}) = \text{Aut}(\text{S. de P. simpl. connexe})$

sf cas triviaux $\quad \Gamma \subset PSL_2(\mathbb{R}) \hookrightarrow SL_3$

Γ a une rep. linéaire fidèle

Thme (Malcowski–Selberg) : si Γ de type fini a une rep linéaire $\Gamma \to GL_N(k)$, k quelconque, fidèle, alors Γ est séparé pour la topologie des ss gpes d'indice fini.

On peut supposer $\Gamma \subset GL_n(\Lambda)$ où Λ est une $\mathbb{Z}$-algèbre de type fini ; on choisit $\underline{m}$ idéal maximal ; $\Lambda/\underline{m} = \tilde{k}$ fini

$$\Gamma \subset GL_n(\Lambda) \longrightarrow GL_n(\hat{\Lambda} = \varprojlim \Lambda/\underline{m}^N)$$

$\Lambda \longrightarrow \hat{\Lambda}$ injectif par Krull

donc $\Gamma \hookrightarrow GL_n(\hat{\Lambda})$ qui est profini.

Sur $\mathbb{R}$ idem

Etape suivante : passage à un corps de base algébriqt clos de car. 0.

k alg clos de car 0 $\qquad$ V var alg$/k$

k'/k ______ $\qquad$ $V_{k'}$ ext des scalaires

① en termes de revêtts

Le foncteur qui à un revêtement fini W de V (non ramifié!) associé $N_{/k'}$ revêtt fini de $V_{/k'}$ est une équivalence.

Tt revêtt de $V_{/k'}$ provient de manière unique d'un revêt de $V_{/k}$.

③ En termes de gpes fondamentaux. (algébriques, cf Grothendieck).

$$\pi_1(V, x) \quad x \in V(k)$$

$\downarrow$ isomorph.

$$\pi_1(V', x)$$

2 faux en caractéristique p pour le cas général (marche par ex si on rajoute hyp. "projective").
cf plus loin.

En particulier, s'applique avec $k = \overline{\mathbb{Q}}$, $k' = \mathbb{C}$.

la pleine fidélité (vraie en tte car): si W_1, W_2 sont deux revêtements de V devenant isomorphes sur k', ils le sont sur k.

$$\mathrm{Mor}_{/k}(W_1, W_2) \xrightarrow{\sim} \mathrm{Mor}_{k'}(W_1, W_2)$$

$\varphi : W_1 \to W_2 \qquad \varphi \overset{?}{=} \varphi^\sigma \qquad \sigma \in \mathrm{Aut}(k'/k)$

On peut supposer que V est connexe, φ déterminé par son action sur un pt d'où OK.

W'
$|$ provient d'un revêtt de $V_{/k}$?
V/k'

On peut supposer $\deg_{\text{tr}} k'/k = 1$

W' est alors définissable sur un corps k'_1 de k' contenant k, de type fini sur k.

ie $W' = W'_1/_{k'}$ $\quad W'_1$ revêt de $V/_{k'_1}$

k'_1/k = corps de fonctions d'une courbe irréductible C/k.

$$\begin{array}{c} C \times V \\ \downarrow \\ V \end{array} \qquad V_{k'_1} = \text{fibre générique de la projection } \begin{array}{c} C \times V \\ \downarrow \\ C \end{array}$$

W'_1 s'étend en un revêtement de $C \times V$ (quitte à remplacer C par un ouvert).

$$\begin{array}{ccc} W_c & \longrightarrow & C \times V \\ & & \downarrow \pi \\ & & C \end{array} \qquad c \in V \quad \pi^{-1}(c) \simeq V_{/k(c)}$$

W_c revêt de $V_{/k(c)}$.

Thme : (Sur un corps de base Ω algt clos de car 0)
Soit W_c un revêtement d'un produit de variétés $\underset{\downarrow}{C \times V}$ avec C connexe. Alors les revêtements $W_c \to V_{/\Omega}$ obtenus à partir des pts $c \in C(\Omega)$, sont isomorphes entre eux.

On applique cela à $k' = \Omega$ en prenant c = pt générique, puis c = pt rationnel$/_k$.

Contre exemple standard en car p

$V =$ dte affine $\qquad C =$ dte

$T \quad k[T] \qquad U \quad k[U]$

$C \times V$ plan

revêt d'Artin Schreier $\quad Z^p - Z = UT$

(non ram, cyclique de d° p)

$U \to u \qquad Z^p - Z = uT$ revêt de la droite

$u = 1$ non trivial

$u = 0$ trivial

<u>En topologie</u> (avec hyp de régularité, par ex. localt contractiles), l'analogue est vrai et résulte de

$$\boxed{\pi_1(C \times V) = \pi_1(C) \times \pi_1(V)}$$

W est un revêtement de $C \times V$, il existe C' un revêtement de C tel que, après chgt de base,

$C' \times V \to C \times V$

W provienne d'un revêt de V.

Critère pour qu'un revêt provienne de V

Si $W \quad C \times V$ est un revêt connexe qui est trivial sur $C \times v$ pour un $v \in V$, alors W provient de V, ie $W \simeq C \times V'$.

$\pi_1 = \pi_1(C) \times \pi_1(V)$

$W \leftrightarrow \pi_1$ - ens. X

avec action transitive.

$\pi_1(C)$ fixe un pt de X $\to$ $\pi_1(C)$ fixe X (65)

Donc X provient d'un $\pi_1(V)$-ensemble, ie W provient d'un revett de V.

[Attention : Il n'est pas vrai qu'un (revêtement d'un) produit soit un produit de revêtements des facteurs ...]

Le thme est donc vrai en topologie.
En général : on peut supposer que

$\Omega \subset \mathbb{C}$

et même $\Omega = \mathbb{C}$

Alors on connaît le résultat par la topologie.

La méthode est un peu marteau pilon. Autre piste :
Proposition. Revett de degré donné d'une var. alg/k (alg. clos car 0) sont en nbre fini
(topol π_1 est de type fini
probablt dém. algébriques).
d'où le thme, peut-être ...

Cas de car p

① Le thme sur les revetts de $C \times V$ reste vrai en car p si V est une variété projective
(cf Serre + Lang, Amer. Journal.)
Ceci équivaut grosso modo à $\pi_1(C\times V) = \pi_1(C) \times \pi_1(V)$
C, V connexes non vides.

Idée : $W_c \to V$ revêts, famille paramétrée par $c \in C$.

Lemme : Si ~~[illegible]~~ W_c ${}^{\text{nt}}$ trivial pour une valeur de c, il l'est pour c générique.

Thme connexion de Zariski $\Rightarrow$ nbre composantes connexes de W_c, c rat, est $\leq$ nbre composantes connexes de W_c, c générique.

Corollaire Si V projective (k alg. clos et si k' ext. de k), les revêts de $V_{/k'}$ proviennent de ceux sur k.

($\cap$ démonstration qui précéd.)

Remarque : Supposons que V soit une courbe non singulière, $V = \overline{V} - \{P_1, \dots, P_k\}$, $\overline{V}$ projective.
Un revêtement $W \to V$ est dit modéré à l'infini si l'ext de corps corresp. est modérée aux valuations associées $= P_i \Leftrightarrow$ (si W galoisien de groupe G), les groupes d'inertie au-dessus des P_i st d'ordre 1^{ers} à p, i.e. les elts d'ordre p de G opèrent librement sur le revêtement.

Thme (Abhyankar) Si on se borne à de tels revêtements, les énoncés précédents restent valables.

revêtt galoisien d'ordre np^{d} + é ; $(n, p) = 1$
en cherchant un $V' \to V$
revêtt ramifié aux P_i
et aussi peut-être
(ailleurs) avec gpe de ram modéré
d'ordre multiple de ~~[illegible]~~ n.

$$W \to V' \to V$$

$$\begin{array}{ccc} W' & \longrightarrow & W \\ \downarrow & & \downarrow \\ V' & \longrightarrow & V \end{array}$$ après chgt de base normalisé.

Alors $\overline{W'} \to \overline{V'}$ n'est pas ramifié. (lemme d'Abhyankar)

Remarque Vrai pour dimensions >1 avec hyp.
$V = \overline{V} - D$ $\overline{V}$ normal proj
(d'après ce que dit Gabber).

Nous savons donc passer de $\mathbb{C}$ à $\overline{\mathbb{Q}}$.

Structure de $\pi_1(\mathbb{P}_1 - \{P_1, \ldots, P_k\})$ (corps de base algt clos de car 0), $k \geq 2$

Ce π_1 est le complété profini du gpe discret correspondant ie le gpe libre engendré par k générateurs $c_1, \ldots, c_k$ liés par $c_1 \ldots c_k = 1$

F_k gpe discret $c_1, \ldots, c_k \mid c_1 \ldots c_k = 1$
$\hat{F}_k$ complété
Il existe un isomorphisme $\pi_1 \simeq \hat{F}_k$

On aura besoin de préciser les classes de conj où vont les c_i:

G
$\Big|$
K
$\Big|$
$k(T)$ Galois

v_i valuation attachée à P_i

w_i
$\Big|$
$\Big|$ I_{w_i} gpe d'inertie

c_i = ordre de I_{w_i}

$I_{w_i} \simeq \mu_{c_i}(k)$ (k alg. clos).

de $I_{w_i} \xrightarrow{\sim}$ $st_i/t_i \in$ corps res. t_i uniformisante en P_i.

On choisit une trivialisation ζ des racines de 1, ie un choix cohérent

pour tte une racine primitive de 1, ζ_e

avec $(\zeta_{ee'})^{e'} = \zeta_e$

ou encore $\mathbb{Z}(1) \simeq \mathbb{Z}$ fixé.

le groupe d'inertie I_i de π_1 en P_i a 1 générateur canonique $s_{\zeta,i}$

$$I_i \simeq \hat{\mathbb{Z}}$$

(I_i est défini à conjugaison près)

C_i = classe de conjugaison de $s_{\zeta,i}$

Thme Il existe un isomorphisme

$$\pi_1 \longleftrightarrow \hat{F}_R$$

tel que $c_i \in \hat{F}_R$ tombe dans la classe C_i.

Démonstration. On peut supposer que k est de type d° tr fini sur $\mathbb{Q}$ (à savoir d° de trans du corps de P_i)
Il existe un plongement $k \to \mathbb{C}$ transformant ζ_e en $e^{2\pi i/e}$

Sur $\mathbb{C}$, résulte de la comparaison avec topologie (avec choix usuel du signe)

$\zeta \quad \zeta^\alpha \quad \alpha \in \hat{\mathbb{Z}}^* = \prod \mathbb{Z}_\ell^\times$

Thme $\Rightarrow$ <u>existence d'un automorphisme</u> $\sigma_\alpha : \hat{F}_k \to \hat{F}_k$ <u>transformant les classes</u> C_i <u>en</u> C_i^α.

$$\begin{array}{l} K \\ \big|\,\pi_1 \\ k(T) \end{array} \qquad c_1 \quad c_i \quad \zeta \text{ fixé alors } \mathrm{set}_\zeta \simeq \hat{\mathbb{Z}}$$

$P_1 \ldots P_k$ $\qquad$ $s_1 \ldots s_k = 1$ seule relat. et engendrent

Complexité sur C non (néc.) algébr. clos

$\mathbb{P}_1 - \{P_1, \ldots, P_k\}$

les P_i st rationnels sur $\bar{k}$, ens. stable par conjugaison

L corps $k(T)$. Soit K = plus grande extension algébr. de $\bar{k}(T)$ non ramifiée en dehors des P_i

$$\begin{array}{lll} & K & \\ & \big|\ \pi^{\text{géom}} & \pi^{\text{géo}} \ (\simeq \hat{F}_k) \\ \pi & \bar{k}(T) & \\ & \big| & \Gamma = \mathrm{Gal}(\bar{k}/k) \\ & k(T) & \end{array}$$

(*) $1 \to \pi^{\text{géo}} \to \pi \to \Gamma \to 1$ $\qquad$ (Valable pour tte var alg.)

$\Gamma \to \mathrm{Out}(\pi^{\text{géom}}) = \mathrm{Aut}(\ )/\mathrm{Int}(\ )$

$k = \mathbb{Q}$ $\qquad$ $P_1 \ldots P_k$ rat/$\mathbb{Q}$

$\alpha \in \Gamma \qquad \zeta \mapsto \zeta^\alpha$

A un pt rationnel de V (i.e. à un relevé de ce pt ds K) est associé un scindage de la suite exacte (*)

π = produit semi direct de Γ par π_1^{geom}.

Shafarevich
Grothendieck → | Que peut-on dire de
$\Gamma \longrightarrow Out(\widehat{F_k})$?

cf Ihara, Deligne.

$\mathbb{P}_1 - \{0, 1, \infty\}$

$\widehat{F_k}^{ab} \simeq \widehat{\mathbb{Z}} \oplus \widehat{\mathbb{Z}}$ Γ agit par caract cyclotom.

suite centrale descendante

$\widehat{F_k} /$ i-ème terme de la suite $=$

partie ℓ-adique de cela $=$ gpe de Lie ℓ-adique nilpotent

muni d'une action (à autom près) de $\Gamma = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$

sur les quotients successifs, on n'a que l'action cyclotom.

Vrai phénomène de non semi simplicité

On cherche noyau, etc...

Pb aussi de l'indépendance par rapport à ℓ

Serre 13/11/89

$\overline{K}$ cl. alg.

$|$

K car 0 $\quad V/K \; (= \mathbb{P}_1 - \{P_1, \dots, P_k\})$

(71) $\quad \pi \begin{cases} \frac{E}{K(V)} \; \pi^{\text{géom}} \text{ ext. max. non ram.} \\ \big| \Gamma = \mathrm{Gal}(\overline{K}/K) \\ K(V) \end{cases}$

$\pi^{\text{geom}} \simeq (\pi_1^{\text{top}})^{\wedge}$ complété profini

$K \hookrightarrow \mathbb{C} \quad \pi_1^{\text{top}} = \pi_1(V(\mathbb{C}))$

$$1 \to \pi^{\text{geom}} \to \pi \to \Gamma \to 1.$$

$$\Gamma \longrightarrow \mathrm{Out}(\pi^{\text{geom}}).$$

(1) ne provient pas en général d'un homom.
$\Gamma \to \mathrm{Out}(\pi_1^{\text{top}})$.

ex $\quad \mathbb{P}_1 - \{0, \infty\} \qquad \pi_1^{\text{top}} \simeq \mathbb{Z} \qquad \pi^{\text{geo}} \simeq \hat{\mathbb{Z}} = \prod \mathbb{Z}_\ell$

$K = \mathbb{Q} \qquad \Gamma = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow[\chi]{} \mathrm{Aut}(\hat{\mathbb{Z}}) = \prod \mathbb{Z}_\ell^*$

caract cyclot

(2) Même sur K alg^t clos.

π_1^{top} dépend du choix de $K \hookrightarrow \mathbb{C}$.

<u>Exemple</u> : V courbe elliptique à mult. cplxe $/\overline{\mathbb{Q}} \overset{i}{\hookrightarrow} \mathbb{C}$

$R = \mathrm{End}\, V$.

$\pi_1^{\text{top}} V \simeq \mathbb{Z} \oplus \mathbb{Z} \qquad R$-module projectif de rang 1.

En variant i, on trouve ts les modules proj de rg 1

$(\pi_1^{\text{top}})^{\wedge} \simeq \hat{R}$ (indépt du plgt)

ex $h = 3 \quad \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$ on trouve 3 modules $\neq$

plgt réel $\Longleftrightarrow$ module libre

cf Note aux CRAS (Serre), t. 258 (1964), 4194-4196.

On peut introduire un fibré un produit de courbes elliptiques à CM de base une variété de $\pi_1 \simeq C_{23}$.

$$\begin{array}{ccc} \mathbb{Z}[\zeta_{23}] & \tilde{W} & A = \underbrace{E \times \_ \times E}_{\frac{p-1}{2}} \\ \Big| 11 & \Big| & \\ R & W & \end{array}$$

V fibré
$\Big| A$
W

réseau $\Lambda \simeq \mathbb{Z}^{22}$

$\pi_1(V)$ extension de C_{23} par Λ.

(3) Le groupe discret attaché à $k = \mathbb{R}$

$$\begin{array}{ccccccccc} 1 & \to & \pi^{geom} & \to & \pi & \to & \{1,-1\} & \to & 1 \\ & & \uparrow & & & & \Vert & & \\ & & & & & & \Gamma & & \\ 1 & \to & \pi_1^{top} & \to & \pi^? & \to & \Gamma & \to & 1 \end{array}$$

<u>Revêtement d'une</u> $\mathbb{R}$-<u>variété</u> V : couples (V' <u>revt</u> de $V(\mathbb{C})$, involution σ' de V' relevant l'involution naturelle $P \mapsto \bar{P}$ de $V(\mathbb{C})$)

(cf terminologie Atiyah : "$\mathbb{R}$-esp topol = esp muni d'une involution.)

(1) Cas élémentaire

X connexe $\quad \sigma x = x \quad$ pour un $x \in X$

i.e $V(\mathbb{R}) \neq \emptyset$.

$\pi_1^{top} = \pi_1(X, x)$

σ définit un automorphisme de ce π_1, $\sigma^2 = 1$.

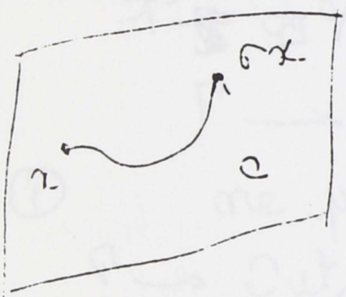
$G \simeq \pi_1^{top} \rtimes \{1,-1\}$.

catégorie des revêtements $\simeq$ G-ensembles.

② Cas où X a 2 composantes connexes échangées par σ

$G = \pi_1(X_1, x)$ $\quad x$ choisi quelconque

③ X connexe $\quad x \in X$ ... σx pas nécessairt x



on choisit c allant de x à σx

$\pi_1^{top}(X, x)$ autom.

"en composant" $\pi_1^{top}(X,x) \xrightarrow[\sigma]{\sim} \pi_1^{top}(X,\sigma x) \xrightarrow[c]{\sim}$

$\theta(\alpha) = c\,\sigma(\alpha)\,c^{-1}$

$\theta^2 = \mathrm{Int}\, a$

$a = c\,\sigma(c)$

G contenant π_1^{top} $\quad \tau$

$\tau^2 = a$

$\tau \alpha \tau^{-1} = \theta(\alpha) \qquad \alpha \in \pi_1^{top}$

$1 \to \pi_1 \to G \to \{\pm 1\} \to \underline{1}$.

Remarque (Gabber): Si $\{1,\sigma\}$ opère librement sur X

$G \simeq \pi_1(X / \{1,\sigma\})$

Thme de rigidité ; le cas "rigide rationnel"

Données $\quad K$ car 0

$P_1, \ldots, P_k$ pts rationnels de $\mathbb{P}_1/K$, distincts.

G gpe fini à centre trivial

$C_1, \dots, C_k$ classes de conjugaison

$C_1 - C_k$ $\mathbb{Q}$-rationnelles

$(C_1 - , C_k)$ rigide

$x_1, \dots, x_k = 1$ $\quad x_i \in C_i$ $\quad \langle x_1, \dots, x_k \rangle = G$

Th [Shih, Belyi, Fried, Matzat, Thompson]

Il existe un G-revêtement irréductible de $P_1 - \{P_1, \dots, P_k\}$ où les gpes d'inertie au-dessus des P_i ont des générateurs $\in C_i$. Il est unique à isomorp. unique près.

En fait vrai avec C_i K-rationnelles (après choix de racines de 1)

Corollaire: Le groupe G vérifie Gal_T.

(On applique le thme en prenant $K = \mathbb{Q}$.)

1ère démonstration (par descente)

sur $\mathbb{C}$ résulte de la struct du π_1^{top}

sur $\bar{K}$ en résulte par équiv de catégories (si K: d° tr.)

sur K descente à la Weil.

F_k $\quad x_1 - x_k \quad x_1 - x_k = 1$

$g_i \in C_i \quad g_1 - g_k = 1 \qquad \langle g_1, \dots, g_k \rangle = G$

$F_k \to G \quad g_i \in C_i$

descente: $V / \bar{K}$ écrivt sur K

V doit être isomorphe à ses conjugués

$$\begin{matrix} L \\ | H = \mathrm{Gal}(L/K) \\ K \end{matrix}$$

V déf $/L$

$V^\sigma_L \xleftarrow{f_\sigma} V_{/L}$

$$\begin{tikzcd} V \arrow[r, "f_\sigma"] \arrow[dr, "f_{\sigma\tau}"'] & V^\sigma \arrow[d, "(f_\tau)^\sigma"] \\ & V^{\sigma\tau} \end{tikzcd}$$

diagr. commutatif

Récipr : si on se donne V quasi projective avec les f_σ formant diag commutatif, il existe V_0 définie sur K et $(V_{0/K})_L \xrightarrow[\sim]{\varphi} V$ faisant commuter les diagramme

$$\begin{tikzcd} V_0 \arrow[r, "\varphi"] \arrow[dr, "\varphi^\sigma"'] & V \arrow[d, "f_\sigma"] \\ & V^\sigma \end{tikzcd}$$

Ici : V G-revêtement ayt les propriétés voulues sur L/K assez grand.

$V \to V^\sigma$ (V^σ ayt les mêmes prop) existe par unicité et est unique

<u>Remarque</u> : les classes étant rationnels, dire que les gpes d'inertie ont un générat ds C_i ou ts les générat revient au même.

Ceci fournit les propriétés souhaitées de V^σ.

<u>Variante</u> : G avec un centre non trivial $Z(G)$.

C_i rationnelle sur $\mathbb{Q}$ et $(C_1, -, C_k)$ rigides.

Le thme en général est faux.

Mais supposons $H^2(\Gamma_K, Z(G)) = 0$ (ex: $\mathrm{cd}\, K \leq 1$
ex $K = \mathbb{Q}^{cycl}$).

alors l'assertion d'existence est vraie.

En effet:
diag Weil $\to$ 2-cocycle de Γ_K dans $Z(G)$.

$2^{\text{ème}}$ <u>démonstration</u> (style galoisien)

$$\begin{tikzcd} 1 \arrow[r] & \pi^{geom} \arrow[r] \arrow[dr, "\varphi"'] & \pi \arrow[r] \arrow[d, dashed, "?"] & \Gamma \arrow[r] & 1 \\ & & G & & \end{tikzcd}$$

$\Gamma = \mathrm{Gal}(\bar{K}/K)$

Σ hom $f : \pi^{geom} \to G$ caract par | surjectif
| généri. inertie $\to C_i$

Si $\sigma \in \pi$ $\quad x \mapsto \varphi(\sigma x \sigma^{-1}) \in \Sigma$

$\varphi_* \sigma$

On a donc $\varphi_* \sigma \in \Sigma$
d'où un élément $g_\sigma \in G$

$(\varphi * \sigma)(x) = g_\sigma x g_\sigma^{-1}$

$\sigma \in \pi \mapsto g_\sigma \in G$

hom Si $\sigma \in \pi^{geom}$ $\quad \varphi * \sigma(x) = \varphi(\sigma x \sigma^{-1}) = \varphi(\sigma) \varphi(x) \varphi_\sigma^{-1}$

soit $g_\sigma = \varphi(\sigma)$

(10/11/89)

Exposé de Malle — **Braid orbit theorems**

G finite group

$Z(G) = \{1\}$. $C_1, \ldots, C_s$ conj. classes de G

$|\Omega(C_1, \ldots, C_s) / G| = \ell(\Sigma)$ $\quad \Sigma = (C_1, \ldots, C_s)$.

$\to \exists\ N_\sigma / k_\sigma$ $\quad k_\sigma, k^{\mathcal{C}}$ number fields, $[\sigma] \in \Omega/G$

$Gal(N_\sigma / k_\sigma(t)) = G$, $\quad (k_\sigma : k^{\mathcal{C}}) \leq \ell(\Sigma)$

$k^{\mathcal{C}} / \mathbb{Q}$ abelian

Many finite simple groups with $\ell(\Sigma) = 1$, $s = 3$
(but not for ? $B_2(32) = S_2(32)$)

for $s \geq 4$ almost no examples exist
(ie $\ell(\Sigma) >> 1$)

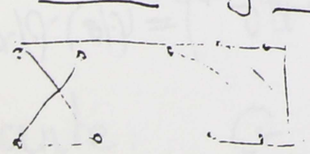
Thompson has indeed found ex of $\ell(\Sigma) = 1$ for some $Sl_3(p)$, $s = 4$.

What is generally the degree of the field of definition k_σ?

Are there any special choices of ram. points such that $(k_\sigma : \mathbb{Q})$ becomes smaller?

Instead study action of the Braid group.
Fried, Matzat.

1- Braid groups.



$\mathbb{R}^3$

$\tilde{B}_n$ Artin braid group

Nalle (?)

β_i | | | [diagram: strands i, $i+1$ crossing]

Prop. $\tilde{B}_r = \langle \beta_i \mid 1 \le i \le r-1 \;\; \beta_i\beta_j = \beta_j\beta_i \;\; |i-j| \ge 2, \;\; \beta_i\beta_{i+1}\beta_i = \beta_{i+1}\beta_i\beta_{i+1} \rangle$

is a presentation of $\tilde{B}_r$

$g : \tilde{B}_r \longrightarrow S_r \quad \beta_i \mapsto (i, i+1)$ surjectif.

$Ker(g) = B_r$ pure Artin Braid group.

Prop. $B_r = \langle \beta_{ij} \mid 1 \le i < j \le r \rangle$

$\beta_{ij} = (\beta_i^{\,2})^{\beta_{i+1}^{-1} \cdots \beta_{j-1}}$

$\beta_{i\,i+1} = (\beta_i^{\,2})$

Prop. $F_{r-1} = \langle \gamma_1, \ldots, \gamma_{r-1} \rangle$ is a free normal subgroup of B_r ($\gamma_i = \beta_{ir}$)

B_r is a semi direct product $B_r = F_{r-1} \rtimes B_{r-1}$

and $(\gamma_1, \ldots, \gamma_{r-1})^{\beta_{i\,i+1}} = (\gamma_1, \ldots, \gamma_{i-1}, \gamma_i\gamma_{i+1}\gamma_i\gamma_{i+1}^{-1}\gamma_i^{-1}, \gamma_i\gamma_{i+1}\gamma_i, \gamma_{i+2}, \ldots, \gamma_{r-1})$.

Motivation

$\beta_1 \ldots \beta_{r-1}$: |

$\beta_{r-1} - \beta_r$ ~~| |~~ .

$\beta_1 - \beta_{r-1}\;\; \beta_{r-1} - \beta_r$ ~~| |~~ |

N_r is a normal subgroup of B_r ~~B_r~~

79

generated by $\beta_1 - \beta_{r-1}\beta_{r-1} - \beta_r$

$\mathcal{H}_r = \tilde{B}_r / N_r$ Hurwitz Braid group

$\varphi : \hat{\mathcal{H}}_r \to S_{r\,\alpha r}$ $\ker(\varphi) = \mathcal{H}_r$ pure Hurwitz braid group

<u>Thm</u> $\mathcal{G}_{r-1} = \langle \gamma_1, -, \gamma_{r-1} \mid \gamma_1 - \gamma_{r-1} = 1 \rangle$ <u>is</u> <u>a free normal subgroup of $\mathcal{H}_r$ of rk $r-2$,</u>

$\mathcal{H}_r = \mathcal{G}_{r-1} \rtimes \mathcal{H}_{r-1}$

(the action of $\mathcal{H}_{r-1}$ on $\mathcal{G}_{r-1}$ can be read off from a preceeding proposition).

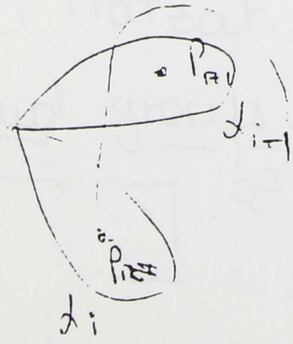
$\mathcal{X}_r^{\circ} = \mathbb{P}_1(\mathbb{C})^r - \{x \mid x_i = x_j \text{ for some } i \neq j\}$

finite group $\quad \mathcal{C} = (C_1, -, C_r)$

$H(\mathcal{C})$ = set of Galois extensions of $\mathbb{C}(t)$ belonging to $\mathcal{C}$.

Projection from $H(\mathcal{C})$ to $\mathcal{X}_r^{\circ}$: to Galois extensions attached ~~to triples~~ uplets of ram. pts.

Topology on $H(\mathcal{C})$: $H(\mathcal{C})$ is a covering of $\mathcal{X}_r^{\circ}$



What happens if one moves P_i around P_{i+1}?

$(\alpha_1, -, \alpha_r) \mapsto (\alpha_1, -, \alpha_{i-1}, \alpha_i \alpha_{i+1} \alpha_i \alpha_{i+1}^{-1} \alpha_i^{-1}, \alpha_i \alpha_{i+1} \alpha_{i+1}^{-1}, -, \alpha_r)$

(exp: Cartier)

Theorem: (Fadell, Fox, Neuwirth, von Bourbaki)

(a) the fundamental group of $\mathbb{A}^1(\mathbb{C})_r^\cdot = \mathbb{A}^1(\mathbb{C}) - \{z \mid z_i = z_j, i \neq j\}$ is the pure Artin Braid group (pb of base pts)

(b) The fundamental group of $\mathbb{P}_1(\mathbb{C})_r^\cdot$ is the pure Hurwitz braid group (same remark)

By factoring $\mathbb{A}^1(\mathbb{C})_r^\cdot$ or $\mathbb{P}_1(\mathbb{C})_r$ by the action of S_r we also get $\tilde{B}_r$, $\tilde{\mathcal{H}}_r$ as fundamental groups.

2 Profinite braid groups.

H_r = profinite completion of $\mathcal{H}_r$ with normal subgroups of finite index.

Thm $G_{r-1} = \langle \gamma_1 \ldots \gamma_{r-1} \mid \gamma_1 \ldots \gamma_{r-1} = 1 \rangle^\wedge$ is a free (profinite) normal subgroup of H_r, of rk $r-2$ and $H_r = G_{r-1} \rtimes H_{r-1}$, with the action of $\beta_{i,i+1}$ as in Prop. Moreover $\mathcal{H}_r \to H_r$ is injective (Matzat, to appear).

Theorem (Abhyankar) Let M_r be the max. field extension of $\mathbb{C}(t_1 \ldots t_s)$ unramified over $\mathbb{P}_1(\mathbb{C})_r^*$. Then $M_r / \mathbb{C}(t)$ is Galois and $\mathrm{Gal}(M_r/\mathbb{C}(t)) \cong H_r = \hat{\mathcal{H}}_r$

Let D_{ij} be the hyperplane $\{x \mid x_i = x_j\}$ in $\mathbb{P}^1(\mathbb{C})^r$.

$D_{ij} = (t_i - t_j)$

Thm: Let Π_r as above, Then there exists $\hat{D}_i$ in Π_r and $G_{\mathbb{I}}(\hat{D}_{ij} / D_{ij}) = \langle B_{ij} \rangle^\wedge$.

$M_r / \mathbb{C}(t_1, \dots, t_r)$ max. non ram. / $\mathbb{P}_1(\mathbb{C})^{\bullet}_r$

Gal $\simeq$ $\hat{H}_r$ complétion du g. des tresses

$H_r = G_{r-1} \rtimes H_{r-1}$ $\qquad G_{r-1} = \langle \gamma_1, \dots, \gamma_{r-1} \mid \gamma_1 \cdots = 1 \rangle$

D_{ij} $(t_i - t_j)$ $\langle \beta_{ij} \rangle$

$\boxed{r \geq 4}$ <u>Th.</u> $M_r^{G_{r-1}} = M_{r-1}(t_r)$. De plus M_{r-1} est alg. fermé ds M_r.

S = div au dessus des $t_i - t_j$ et c'est ext. maximale non r. en dehors de S.

M_r
$|G_{r-1}$
$M_{r-1}(t_r)$
$\mathbb{C}(\underline{t})$ H_{r-1}

Bien sûr, vrai sur $\overline{\mathbb{Q}}$. Il écrit $\overline{M}_{r-1}, \overline{M}_r \dots$

$s = r-1$, $t = t_r$

$$\begin{array}{c} \overline{M}_r \\ | \\ \overline{M}_s(t) \\ / \\ \overline{\mathbb{Q}}(t) \\ / \\ \mathbb{Q}(t) \quad \Lambda = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \end{array}$$

$\overline{M}_r$ est galoisien sur $\mathbb{Q}(t)$; gr. de Galois $H_r \rtimes \Lambda$.

<u>Corp de déf.</u> G fini, $Z(G) = 1$. $C_1, \dots, C_s$ classes rat. (pour simplifier).

$\Omega(C_1, \dots, C_s)$; G agit librement ; $\Sigma = \Omega / G$ $(= \Sigma(\underline{c}))$; $\sigma \in \Omega$.

Si on se donne $[\sigma] \in \Sigma$, il y a $\overline{N}_\sigma / \overline{M}_s(t)$ de g. de Galois G.

Action de $\Delta = H_s \rtimes \Lambda$ sur $\Sigma(\underline{c})$; (action de Λ probt. pas canonique ?)

Il appelle Δ_σ le stab. de $[\sigma]$ ds Δ ; $K_\sigma = \overline{M}_s^{\Delta_s}$. Alors $K_\sigma(t)$ "est un corp de déf." de $\overline{N}_\sigma / \overline{M}_s(t)$.

Prop. Si $(H_s : H_{s\sigma}) = (\Delta : \Delta_\sigma)$, $\mathbb{Q}$ est alg. fermé ds K_σ.

<u>Exemple</u> $G = P\Sigma L_2(\mathbb{F}_{25})$, ext. ~~de~~ de PSL_2 par l'involution de conj.

G agit sur $\mathbb{P}_1(\mathbb{F}_{25})$, ordre 26. Classes $2A = (2)^{12}$ $\quad 2C, 2D$ $\quad (2)^{10}$

Rationnel grâce à l'invol. $\qquad$ ATLAS

$c = (2A, 2C, 2D, 12A)$. Par machine $|\Sigma(c)| = 12$. $\qquad 12A \quad (12)^2$

Action du groupe des tresses H_4 ; une seule orbite.

$\overline{N}_r$
$|G$
$\overline{M}_s(t)$
M

Th. de rigidité (Matzat) $r \geq 4$; $[\sigma] \in$ orbite esp. de G_{s-1} (longueurs $\neq$ autres)

Alors $\mathbb{Q}(t_1, \dots, t_{s-1})$ alg. fermé ds K_σ et l'ext. $K_\sigma / \mathbb{Q}(t_1, \dots, t_{s-1})$ a un <u>genre</u> <u>calculable</u>.

Si $g = 0$ et si σ un β_{1s} il y a ~~un cycle ...~~ une longueur de cycle appt. avec un nbre impair de fois, $K_\sigma \simeq \mathbb{P}_1$.

Serre 20/11/89

Rigidité "simple"

. K car. 0

$\mathbb{P}_1$ $P_1, \dots, P_k \in \mathbb{P}_1(K)$, distincts

G groupe centre trivial

$C_1, \dots, C_k$ classes rationelles

$(C_1, \dots, C_k)$ rigide

$$\begin{array}{c} X \\ \downarrow G \\ \mathbb{P}_1 - \{P_1, \dots, P_k\} \end{array}$$

G-revêtement unique $/K$.

Variantes

1.) "Même énoncé" en supposant seulement les classes K-rationelles

On se donne un choix cohérent de racines de 1 dans $\bar{K}/K$.

$$\begin{tikzcd} 1 \arrow[r] & \pi^{geom} \arrow[r] \arrow[d, "\varphi"] & \pi \arrow[r] & \Gamma \arrow[r] & 1 \\ & G & & \mathrm{Gal}(\bar{K}/K) \arrow[u, phantom, "\parallel"] & \end{tikzcd}$$

K-rationnelle :

$Gal(K^{cycl}/K) \subset \hat{\mathbb{Z}}^*$ agit sur G
et sur $cl(G)$

K-rationnelle : fixe comme point
de $cl(G)$

$s \in \Gamma \longrightarrow \chi(s) \in \hat{\mathbb{Z}}^*$

$c^{\chi(s)} = c \quad \forall s$

χ caractère cyclotomique.

Unicité après choix de facteur irréd.
du pol. cycl.

S'applique aux corps $\mathbb{Q}^{ab}$, car toutes
les classes sont rationnelles sur $\mathbb{Q}^{ab}$.

$\Rightarrow$ Si G a un système de classes
rigides, il y a une extension
galoisienne régulière de $\mathbb{Q}^{ab}(T)$
à groupe de Galois G.

——— de $\mathbb{Q}(\zeta_n)(T)$ ———

(Belyi)

Amélioration (Belyi)

$C_1, \dots, C_k$ classes de G "rigide" s'il existe $x_i \in C_i$ avec $x_1 \cdots x_k = 1$

$G = \langle x_1, \dots, x_k \rangle$ et toute autre telle famille (x_i') est conjuguée de la première.

Théorème :

Supposons $\operatorname{cd} K \leq 1$, et $K \supset \mathbb{Q}^{ab}$.

Si G (à centre non nécessairement 1) possède un système rigide de classes, alors il y a une extension galoisienne régulière de $K(T)$ à groupe de Galois G.

élém. de $Z(G)$ définissent autom. non trivial de

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

$$\begin{tikzcd} X^\sigma \arrow[dr] & X \arrow[l, "\sim"'] \arrow[dl] \\ & \mathbb{P}_1 \end{tikzcd}$$

$f_{\sigma\tau} = {}^\sigma f_\tau f_\sigma$?

on a

$f_{\sigma\tau} = z_{\sigma\tau}\, {}^\sigma f_\tau f_\sigma$

donne 2-cocycle sur le groupe

$\mathrm{Gal}(\bar{K}/K)$ à valeurs ds $Z(G)$.

Ce cocycle peut être trivial si $cd\, K \leq 1$.

Ceci s'applique à $\mathbb{Q}^{ab}$ lui-même.

On peut en déduire que $GL_n(\mathbb{F}_q)$ est groupe de Galois sur $\mathbb{Q}^{ab}$.

Plus petit groupe simple dont on ne sache pas s'il est groupe de Galois

sur $\mathbb{Q}^{ab}(T)$: $S_z(32)$

sur $\mathbb{Q}(T)$: $SL_2(\mathbb{F}_{16})$.

Autre variante :

Points de ramification irrationnelles.

2 cas particulier : $P_1, P_2, P_3 \in \mathbb{P}_1$

avec P_1 rat $/\mathbb{Q}$, P_2, P_3 rat. $/\mathbb{Q}(\sqrt{d})$

et conjugués entre eux.

G $Z(G) = 1$, C_1, C_2, C_3 rigides.

C_1 rationnelle, C_2, C_3 rat. sur $\mathbb{Q}(\sqrt{d})$

et conj. entre elles.

Il existe alors un revêtement

$$\begin{array}{c} X \\ \downarrow G \\ \mathbb{P}_1 \end{array} \quad /\mathbb{Q}$$

ramifié aux points ... P_1, P_2, P_3

groupes de ramification C_1, C_2, C_3

(racines de 1 aussi échangés)

P_1, P_2, P_3 sur corps cubique abélien

C_1, C_2, C_3 —— conjugués sur ce corps.

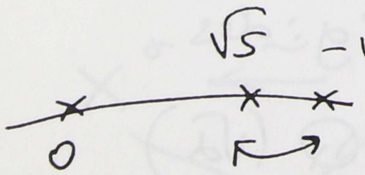
<u>Exemple :</u> $G = A_5$

pas de système de classes rigides, rat.

$(3A, 5A, 5B)$ rigide

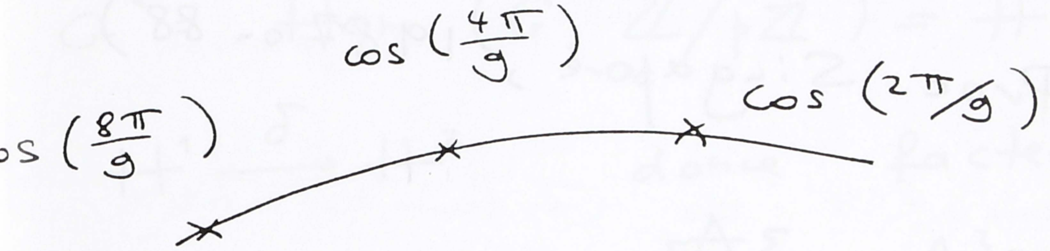
$$\begin{array}{c} \vert \quad \vert \\ \mathbb{Q}(\sqrt{5}) \end{array}$$

$G = A_5$:



$G = SL_2(\mathbb{F}_8)$

$(9A, 9B, 9C)$ — C cubique cyclique ramifié seulement en 3 : $\mathbb{Q}\left(\cos \frac{2\pi}{9}\right)$.



Variante :

Si G_1 est un groupe ayant un s/g G d'indice 2, et si G_1 a 3 classes rat. rigides, alors (si $Z(G_1) = 1$) G a la propriété Gal T.

$$\begin{tikzcd} & X_1 \arrow[dl, "G"'] \arrow[d, "G_1"] \\ X \arrow[r] & \mathbb{P}_1 \end{tikzcd}$$

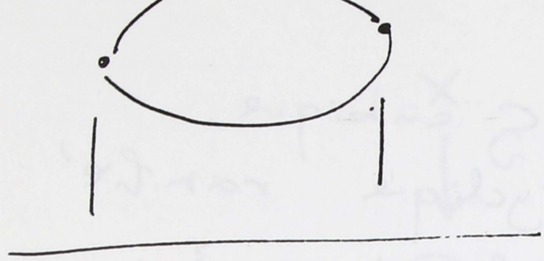
ramifié en 3 pts.

/$\mathbb{Q}$.

$$\begin{tikzcd} X \arrow[d, "2"] \\ \mathbb{P}_1 \end{tikzcd}$$

$x_1 x_2 x_3 = 1$
eng. G_1

G_1/G 2 élé'
→ ram. en 2 pts.



$g = 0$, pts :

$\Rightarrow X \simeq \mathbb{P}_1$

W. Feit (Proc. Singapore, 1987 ou 88)

G : $3A_6$, $3A_7$

ont la propriété Gal_T.

Schur : A_6, A_7 possèdent essentiellement une extension centrale par C_3, non scindée.

Plus précisément, $H^2(A_n, C_3) \simeq C_3$ $n = 6, 7$

$$1 \longrightarrow C_3 \longrightarrow 3A_n \to A_n \to 1.$$

$$H^i(G) := H^i(G, \mathbb{Z}/3\mathbb{Z}).$$

Dém : $H^i(A_6)$, $i = 2$

: 3-Sylow 123 456

$\cong C_3 \times C_3$

(90)

$$H^2(A_6) \hookrightarrow H^2(S)$$

invariant par le normalisateur.

si G de type $(p, \dots, p)$, $p \neq 2$, rappelons que :

$$H^2(G, \mathbb{Z}/p\mathbb{Z}) \simeq G^* \oplus \Lambda^2 G^*$$

$$G^* = \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z}) = H^1(G)$$

$H^1 \xrightarrow{\delta} H^2$ donc facteur G^*

cup produit : donc Λ^2.

u, v base de H^1.

$\delta u, \delta v$, $u \wedge v$ base de $H^2(S)$

Normalisateur du sylow : on peut permuter les paquets.

$(u, v) \longmapsto (-u, -v)$

$(u, v) \longmapsto (-v, u)$

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

$H^2(S)^{\text{inv. par norm.}}$ dim 1 $(u \wedge v)$

$$H^2(A_6) \longrightarrow H^2(S)^{\text{inv. norm}}$$

en fait, c'est un isom.

Thm général pour Sylows abéliens.

Analogie : G groupe de Lie

T tore maximal

$$H^*(B_G) \cong H^*(B_T)^W \qquad W : \text{groupe de Weil}$$

Autre vérification :
critère de stabilité de Cartan-Eilenberg.

$\alpha \in H^i(S)$

pour que α provienne de $H^i(G)$
$\iff$ α stable, i.e.

$$P \xrightarrow[\text{conj}]{} S$$

p-groupe

α_P indépendant de la conjugaison.

$P = S$: inv. par normalisateur.

$P = (1)$, P cyclique d'ordre p, ok

P Sylow : par hypothèse.

De plus, ds $3A_6$ le 3-Sylow est un groupe de Heisenberg d'exposant 3

$3A_7$: même démonstration.

$A_6 \hookrightarrow PGL_3(\mathbb{C})$ groupe de Valentiner.

Fricke, Algebra, Bd. II, p. 263 - ...)

$$\begin{tikzcd}
 & 1 \arrow[d] \\
 & C_3 \arrow[d] \\
3A_6 \arrow[r, hook] \arrow[d] & SL_3(\mathbb{C}) \arrow[d] \\
A_6 \arrow[r, hook] & PGL_3(\mathbb{C}) \arrow[d] \\
 & 1
\end{tikzcd}$$

$\{\pm 1\} \times 3A_6$ groupe engendré par 3 symétries (complexes).

"Système de racines complexes".

S_6 renverse $H^2(A_6)$

$3A_6 \subset 3'S_6$

extension non centrale de S_6

par C_3 (action par

signature).

Le groupe $3'S_6$ a un centre trivial.

De même, $3A_7 \subset 3'S_7$

Le critère précédent s'applique :

on montre que $3'S_6$ et $3'S_7$

possèdent des triplets rationnels

rigides.

(prochaine fois), donc ont la

propriété Gal_T.

$6A_6$, $6A_7$: la construction

de Feit ne marche pas.

Mestre : autre méthode, qui donne

$6A_6$.

27/11/89

Pour obtenir la propriété Gal_T pour $3A_6$ et $3A_7$, on va utiliser un théorème de "relèvement de la rigidité", dû à Feit (Proc. Conf. Singapore "Group Theory", W. de Gruyter, 1989).

<u>Théorème de relèvement</u>

Soit $1 \to \Phi \to G \xrightarrow{\pi} \overline{G} \to 1$ une suite exacte de groupes finis. On suppose :

a) Centre de $G = 1$.

b) Φ est contenu dans le s/groupe de Frattini de G, i.e. tout sous-groupe H de G tel que $\Phi . H = G$ est égal à G.

On se donne 3 classes de conjugaison C_1, C_2, C_3 de G, et on note $\overline{C}_1, \overline{C}_2, \overline{C}_3$ leurs images dans $\overline{G}$. On suppose :

c) $C_1 \to \overline{C}_1$ est bijectif.

d) $C_2 = \pi^{-1}(\overline{C}_2)$ et $C_3 = \pi^{-1}(\overline{C}_3)$ (i.e. $\Phi . C_i = C_i$ si $i = 2, 3$)

<u>Théorème</u> – <u>Supposons en outre que</u> $(\overline{C}_1, \overline{C}_2, \overline{C}_3)$ <u>soit un triplet rigide dans</u> $\overline{G}$. <u>Alors</u> (C_1, C_2, C_3) <u>est un triplet rigide dans</u> G.

(L'énoncé de Feit, <u>loc. cit.</u>, utilise une hypothèse moins forte que c) ; il est incorrect.)

<u>Démonstration</u> – Soient $\overline{x}_1, \overline{x}_2, \overline{x}_3 \in \overline{C}_1, \overline{C}_2, \overline{C}_3$ tels que $\overline{x}_1 \overline{x}_2 \overline{x}_3 = 1$ et que $\overline{G} = \langle \overline{x}_1, \overline{x}_2, \overline{x}_3 \rangle$. Choisissons

$x_1 \in C_1$ relevant $\overline{x}_1$, et $x_2 \in C_2$ relevant $\overline{x}_2$; il y a alors un choix unique d'un relèvement x_3 de $\overline{x}_3$ tel que $x_1 x_2 x_3 = 1$, et l'on a $x_3 \in C_3$ d'après d). De plus, l'hypothèse b) entraîne que G est égal à $\langle x_1, x_2, x_3 \rangle$.

Reste à montrer que un tel système x_1, x_2, x_3 est unique, à G-conjugaison près. Il suffit pour cela de les compter. leur nombre est visiblement $|\Phi|$ fois celui des systèmes analogues dans $\overline{G}$, lequel est $|\overline{G}|$. On trouve donc $|G| = |\Phi| . |\overline{G}|$ tels systèmes, et comme G opère librement sur ces systèmes (grâce à a), cela montre bien qu'il n'y a qu'une seule orbite, cqfd.

<u>Remarques</u>. 1) la condition c) équivaut à dire que, si $x_1 \in C_1$, et $g \in G$, alors $g x_1 g^{-1} x_1^{-1} \in \Phi \Rightarrow g x_1 g^{-1} x_1^{-1} = 1$. En particulier, Φ et x_1 commutent.

2) Si $x_2 \in C_2$, l'automorphisme $\varphi \mapsto x_2 \varphi x_2^{-1}$ de Φ est "sans points fixes", i.e. $x_2 \varphi x_2^{-1} = \varphi \Rightarrow \varphi = 1$. En effet, si φ commute à x_2, et si $x_1 x_2 x_3 = 1$, $x_i \in C_i$, $G = \langle x_1, x_2, x_3 \rangle$, alors φ commute à x_1 (par la remarque ci-dessus), donc à x_3 et à G, d'où $\varphi = 1$ par a).

Inversement, si $\varphi \mapsto x_2 \varphi x_2^{-1}$ est "sans point fixe", Tout élément de Φ peut s'écrire comme commutateur $\varphi^{-1} x_2 \varphi x_2^{-1}$ et on en déduit facilement que $\Phi . C_2 = C_2$.

Aussi la condition d) équivaut à dire que les automorphismes $\varphi \longmapsto x_i \varphi x_i^{-1}$ $(i = 2,3)$ de Φ sont "sans points fixes".

On a besoin pour la suite de propriétés de rationalité:

Théorème – Sous les hypothèses ci-dessus

e) Si $\overline{C}_2$ et $\overline{C}_3$ sont rationnelles, il en est de même de C_2 et C_3. (sur $\mathbb{Q}$)

f) Supposons que les éléments de C_1 et $\overline{C}_1$ aient le même ordre, et que cet ordre soit premier à l'ordre de Φ. Alors, si $\overline{C}_1$ est rationnelle, il en est de même de C_1.

Si $x_2 \in C_2$ et si α est premier à l'ordre de x_2, x_2^{α} a pour image dans $\overline{G}$ la puissance α-ème de l'image de x_2, donc appartient à $\overline{C}_2$. Vu c), on a donc $x_2^{\alpha} \in C_2$ et de même pour C_3. Cela démontre b).

On raisonne de même pour f), en remarquant que C_1 est formé des éléments de G relevant les éléments de $\overline{C}_1$ avec même ordre.

—

On peut maintenant revenir à $3A_6$ et $3A_7$.

Commençons par $3A_6$.

On plonge $3A_6$ dans le groupe $G = 3'S_6$; on prend pour Φ le sgroupe distingué d'ordre 3 de G, de sorte que $G/\Phi = \overline{G}$ n'est autre que S_6. Du fait que l'action de S_6 sur Φ est non triviale (donnée par $S_6 \to \{\pm 1\}$), le centre de $3'S_6$ est $\{1\}$. On choisit alors pour $\overline{C}_1, \overline{C}_2, \overline{C}_3$ les classes de S_6 suivantes :

$\overline{C}_1$ = classe de la permutation circulaire (12345) d'ordre 5

$\overline{C}_2$ = classe de la transposition (12)

$\overline{C}_3$ = classe de la permutation circulaire (123456) d'ordre 6.

Les éléments de $\overline{C}_2, \overline{C}_3$ opèrent non trivialement sur $\Phi \simeq \mathbb{Z}/3\mathbb{Z}$. D'où, par image réciproque, des classes C_2, C_3 dans $G = 3'S_6$ satisfaisant à d). D'autre part, l'ordre des éléments de $\overline{C}_1$ est premier à 3. D'où un unique relèvement de $\overline{C}_1$ en C_1, classe de conjugaison de G formée d'éléments d'ordre 5. D'après le th. ci-dessus ces classes sont rationnelles. D'autre part, le triplet

$(\overline{C}_1, \overline{C}_2, \overline{C}_3)$ de S_6 est connu pour être rigide (et même strictement rigide). On en conclut que le triplet (C_1, C_2, C_3) de $G = 3' S_6$ est <u>rationnel</u> et <u>rigide</u>. D'où, par la "variante" (7.88) de la fin du cours précédent, <u>le fait que</u> $3A_6$ <u>a la propriété</u> Gal_T (puisque c'est un sous-groupe d'indice 2 de $3' S_6$).

Le <u>cas de</u> $3 . A_7$

L'argument est le même, en prenant pour $\overline{C}_1, \overline{C}_2, \overline{C}_3$, les classes des cycles (1234567), (12), (123456) respectivement.

<u>Application aux groupes sporadiques ayant un multiplicateur de Schur d'indice divisible par 3</u>

Les groupes sont : M_{22}, $J3$, McL, Suz, $O'N$, F_{22}, F_{24}.

Dans chaque cas, le groupe Out est d'ordre 2, et opère non trivialement sur le sous-groupe $\mathbb{Z}/3\mathbb{Z}$ du multiplicateur de Schur. Si l'on note S le groupe simple en question, on a donc à la fois un groupe $3 S$ et un groupe ($G=$) $3'\overline{G}$, où $\overline{G} = S \cdot 2$ (notation de ATLAS). On peut donc espérer appliquer la méthode ci-dessus.

On doit d'abord trouver un triplet rationnel rigide dans $\overline{G} = S.2$. Cela a été fait dans chacun de ces cas :

Auteurs	Groupe	pages ATLAS	Classes $\overline{C}_1, \overline{C}_2, \overline{C}_3$
Hunt	M_{22}	39-41	11 A, 2 B, 4 C
Pahlings	J_3	82-83	3 B, 2 B, 8 B
Pahlings	McL	100-101	3 A, 2 B, 10 B
Hunt	Suz	128-131	3 B, 2 C, 28 A
den-Siedersleben et Matzat	O'N	132-133	4 A, 2 B, 22 A
Pahlings	F_{22}	156-163	2 A, 18 E, 42 A
Hunt	F'_{24}	200-207	29 A, 2 C, 8 D

Dans chaque cas, <u>excepté celui de J_3</u>, on constate que ces classes se relèvent en des classes C_1, C_2, C_3 rationnelles de $G = 3'S2$ satisfaisant à a), b), c), d). On en déduit <u>que les groupes 3S correspondants ont la propriété</u> Gal_T ; seul le cas de $3.J_3$ reste ouvert.

Autre variante du théorème de rigidité.

La variante de la Séance précédente (p. 88) concernait des sous-groupes d'indice 2. On va maintenant s'occuper du cas de sous-groupes d'indices plus grands.

Théorème (d'après W. Feit, Proc. Rutgers 1983-1984, Cambridge U. Press, 1984, p. 286). Soit G un groupe fini à centre trivial, et soit I un sous-groupe normal de G tel que G/I soit abélien de type $(2,2)$. Soit (C_1, C_2, C_3) un triplet rationnel rigide de G. Supposons que, pour $x_1 \in C_1$, on ait $N_G(\langle x_1 \rangle) . I \neq G$. Alors I a la propriété Gal_T.

(Notes : ① Il y a un énoncé analogue lorsque le quotient G/I est diédral. ② Feit ne fait pas d'hypothèse sur $N_G(\langle x_1 \rangle)$ mais sa démonstration est insuffisante, comme le lui a fait remarquer Matzat.)

Démonstration - Soit $\begin{array}{c} X \\ \downarrow G \\ \mathbb{P}_1 \end{array}$ le G-revêtement de $\mathbb{P}_1$, ramifié en P_1, P_2, P_3, points rationnels de $\mathbb{P}_1$, fourni par le théorème de rigidité.

Le revêtement $X/I \longrightarrow \mathbb{P}_1$ est de type $(2,2)$ et ramifié (au plus) en P_1, P_2, P_3. Il est facile de voir qu'il est de genre 0 [de façon générale, un revêtement de $\mathbb{P}_1$ à groupe de type $(2,\dots,2)$ a pour genre la somme des genres des revêtements quadratiques qu'il contient — ici ceux-ci sont visiblement de genre 0]. Si l'on prouve que X/I a un point rationnel, il en résultera $X/I \simeq \mathbb{P}_1$ et le revêtement $X \xrightarrow{I} X/I$ montrera que I a la prop. Gal_T.

Pour cela, choisissons un point fermé Q_1 de X au-dessus de P_1 et appelons In_1 et Dec_1 ses groupes d'inertie et de décomposition dans G. On a $In_1 = \langle x_1 \rangle$, avec $x_1 \in C_1$ et $Dec_1 \subset N_G(\langle x_1 \rangle)$ puisque In_1 est un sous-groupe normal de Dec_1. Notons $\overline{In_1}$ et $\overline{Dec_1}$ les images de ces groupes dans $\overline{G} = G/I$; ce sont les groupes d'inertie et de décomposition de l'image $\overline{Q_1}$ de Q_1 dans X/I.

Comme G est engendré par x_1, x_2, x_3 avec $x_1 x_2 x_3 = 1$, l'image de x_1 dans G/I est non triviale. D'où $|\overline{In_1}| = 2$.

D'autre part, l'hypothèse faite sur $N_G(\langle x_1 \rangle)$ entraîne que $|\overline{Dec_1}| < 4$ d'où $\overline{Dec_1} = \overline{In_1}$. Mais le groupe quotient $\overline{Dec_1} / \overline{In_1}$ est le groupe de Galois de l'extension résiduelle $\mathbb{Q}(\overline{Q}_1)/\mathbb{Q}$. Cette extension est donc triviale, ce qui montre que $\overline{Q}_1$ est un point rationnel de X/I, cqfd.

Application (Feit, Rutgers, p. 351-356).

Théorème – Si $p > 2$ est un nombre premier tel que $p \equiv \pm 2 \pmod 5$, le groupe $PSL_2(\mathbb{F}_{p^2})$ a la propriété Gal_T.

On applique le théorème précédent en prenant pour G le groupe $\mathrm{Aut}\, I$, où $I = PSL_2(\mathbb{F}_{p^2})$. Le quotient G/I est de type $(2,2)$, engendré par a) l'automorphisme de I donné par la conjugaison $x \mapsto x^p$ du corps $\mathbb{F}_{p^2}$; b) un automorphisme de I induit par un élément de $PGL_2(\mathbb{F}_{p^2})$ n'appartenant pas à $PSL_2(\mathbb{F}_{p^2})$.

Feit prouve que l'on obtient un triplet rationnel rigide du groupe G de la forme C_1, C_2, C_3, où C_1 est la classe de l'automorphisme τ, et C_2, C_3 sont des classes bien choisies d'ordre 4 et 10. Le centralisateur de τ est égal à $PGL_2(\mathbb{F}_p).\{1,\tau\}$. Du fait que $PGL_2(\mathbb{F}_p)$ est contenu dans $PSL_2(\mathbb{F}_{p^2})$ on déduit que ce centralisateur a une image dans G/I d'ordre 2. On peut alors appliquer le théorème. (Je renvoie à Feit pour les définitions de C_2 et C_3 et la vérification de la rigidité.)

<u>Note</u> – Le même résultat a été obtenu par Mestre, par une méthode différente (utilisation d'une famille de courbes de genre 2 à mult. réelles par $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$).

<u>Un théorème de rigidité de Belyi</u>

Ce théorème a l'avantage de s'appliquer à des groupes pouvant avoir un centre non trivial (et pouvant même être infinis, ce qui a un intérêt pour la monodromie des équations différentielles, cf. semaine prochaine).

Soit V un espace vectoriel de dimension finie m sur un corps k (non nécessairement fini). Soient $x, y, z \in GL(V)$ tels que

a) $xyz = 1$;

b) $\langle x, y, z\rangle$ est irréductible ;

c) $\operatorname{rang}(x-1) = 1$, i.e. x est une pseudo-réflexion.

Soient $x', y', z' \in GL(V)$ satisfaisant aux mêmes propriétés.

Théorème. Si x' est conjugué de x, y' conjugué de y et z' conjugué de z, alors il existe $g \in GL(V)$ tel que

$$x' = gxg^{-1}, \; y' = gyg^{-1} \text{ et } z' = gzg^{-1}.$$

Démonstration (d'après Belyi – on donnera la semaine prochaine une démonstration plus simple) –

On peut évidemment supposer $y = y'$.

Lemme – On a $\mathrm{Tr}(xy^n) = \mathrm{Tr}(x'y^n)$ pour tout $n \in \mathbb{Z}$.

Notons d'abord que si $\alpha \in \mathrm{End}\, V$ est tel que $\mathrm{rang}(\alpha) \leq 1$, on a $\det(1+\alpha) = 1 + \mathrm{Tr}(\alpha)$.

Appliquons ceci à $\alpha = \sum_{n=0}^{\infty} (x-1) T^n y^{-n}$, où T est une indéterminée. On obtient

$$\det(1+\alpha) = \det\left(1 + \sum_{n=0}^{\infty} (x-1) T^n y^{-n}\right) = 1 + \sum_{n=0}^{\infty} T^n \,\mathrm{Tr}((x-1)y^{-n}).$$

Or $1 + \alpha = 1 + (x-1)\dfrac{1}{1-Ty^{-1}} = (xy - T)(y-T)^{-1} = (z^{-1} - T)(y-T)^{-1}$.

On obtient donc

$$1 + \sum_{n=0}^{\infty} T^n \,\mathrm{Tr}((x-1)y^{-n}) = \det(z^{-1} - T)\det(y-T)^{-1},$$

et un résultat analogue avec x' à la place de x et z' à la place de z. Mais z et z' sont conjugués, donc $\det(z^{-1} - T) = \det(z'^{-1} - T)$.

On en conclut que

$$\mathrm{Tr}((x-1)y^n) = \mathrm{Tr}((x'-1)y^n) \quad \text{pour } n \leq 0.$$

On passe de là à $n \in \mathbb{Z}$, en remarquant que, par Hamilton-Cayley, y^n est combinaison linéaire des y^q, $q < n$.

On a donc $\mathrm{Tr}((x-1)y^n) = \mathrm{Tr}((x'-1)y^n)$ pour tout $n \in \mathbb{Z}$, d'où aussi $\mathrm{Tr}(xy^n) = \mathrm{Tr}(x'y^n)$.

Ceci fait, soit D la droite de V image de $x-1$. Si $v \in D$, $v \neq 0$, on peut écrire $x-1$ sous la forme $x - 1 = v \otimes \lambda$, avec $\lambda \in V^*$ (dual de V), autrement dit $(x-1)(w) = \lambda(w).v$ pour tout $w \in V$.

L'espace vectoriel engendré par les $y^n D$ $(n \in \mathbb{Z})$ est stable par x et y, donc aussi par le groupe $\langle x, y, z \rangle$. Vu l'hypothèse d'irréductibilité, cet espace est égal à V.

Ainsi V est un $k[y]$-module <u>monogène</u>, de générateur l'élément v. Si $\mathfrak{a} \subset k[T]$ est son annulateur, on a $V \simeq k[T]/\mathfrak{a}$. Pour la même raison, si on écrit $x'-1 = v' \otimes \lambda'$ avec $\lambda' \in V^*$, le vecteur v' est un générateur de V (comme $k[y]$-module). Il y a donc un élément inversible de $k[y]$ qui fait passer de v à v'. Quitte à conjuguer par cet élément (ce qui ne change pas y), on peut donc supposer que $v = v'$.

La démonstration sera achevée si l'on prouve que $\lambda = \lambda'$.

Or un petit calcul montre que

$$\lambda(y^n v) = \mathrm{Tr}\big((x-1)y^n\big) \quad , \ n \in \mathbb{Z}$$

et de même $\quad \lambda'(y^n v) = \mathrm{Tr}\big((x'-1)y^n\big) \quad , \ n \in \mathbb{Z}$

D'après le lemme, on a $\lambda(y^n v) = \lambda'(y^n v)$ pour tout $n \in \mathbb{Z}$.

Comme les $y^n v$ engendrent V, cela montre bien que $\lambda = \lambda'$, cqfd.

<u>Exemple</u> (Belyi). Soit ρ un générateur du groupe multiplicatif $\mathbb{F}_q^*$. Si $m \geq 3$, définissons $x, y, z \in GL_m(\mathbb{F}_q)$ par

$$x = \begin{pmatrix} 1 & 1 & & \\ 0 & 1 & & 0 \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ \pm\rho & 0 & 0 & \cdots & 0 \end{pmatrix}, \text{ avec } \underset{\det y = \rho}{\pm = (-1)^{m-1}},$$

et $z = y^{-1}x^{-1}$. On peut alors montrer que les hypothèses du théorème sont satisfaites, et que le groupe $\langle x, y, z \rangle$ est $GL_m(\mathbb{F}_q)$ tout entier. D'où le fait que $GL_m(\mathbb{F}_q)$ satisfait Gal_T <u>sur le</u>

Corps cyclotomique $\mathbb{Q}^{ab}$. (Pour $n = 2$, cela marche aussi, avec un choix différent de x, y.)

Des arguments du même goût s'appliquent aux autres groupes classiques (toujours sur $\mathbb{Q}^{ab}$).

—

4/12/89

(108)

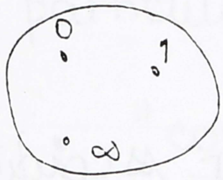
Rigidité

F. Beukers
G. Heckman Inv. Math. 95 (1989), 325-...

via équation hypergéométrique Ref à la thèse de Levelt, Indigat. ~1962

$$f = \sum_{k=0}^{\infty} \frac{(\alpha_1)_k \cdots (\alpha_n)_k}{(\beta_1)_k \cdots (\beta_{n-1})_k \, k!} z^k ,$$

$$(\alpha)_k = \alpha(\alpha+1)\cdots(\alpha+k-1)$$



action de $\pi_1(\mathbb{P}_1(\mathbb{C}) - \{0,1,\infty\})$ sur l'espace des solutions

$\gamma_0 \, \gamma_1 \, \gamma_\infty = 1$

γ_1 pseudo réflexion (équa dif plus "gentille" en 1...)

d'où 3 matrices dans $Gl_n(\mathbb{C})$.

Esquisse de démonst.

$xyz = 1$ $\quad GL_n(k)$ $\quad \langle x, y, z\rangle$ irréduct.

x pseudo réflexion

Si x', y', z' conjugués à x, y, z resp.

Alors il y a un élt de Gl_n conjuguant x à x', y à y', z à z'

Il faut construire une base de l'espace mettant en évidence les polynômes caractéristiques

$\mathrm{Ker}(x-1) = H$ hyperplan

$H, y^{-1}H, \ldots, y^{-(n-2)}H$ $\quad n-1$ hyperplans

On choisit $e \neq 0$, $e \in \bigcap_{i=0}^{n-2} y^{-(i)} H$

$y^i e \in H \quad (x-1)\, y^i e = 0 \quad i = 0, \ldots, n-2$

irréductibilité $\Rightarrow e, ye, \ldots, y^{n-1} e$ base de $k^n = V$

$y\, y^{n-1} e = \alpha_0 e + \ldots + \alpha_{n-1} y^{n-1} e$

$xyz = 1 \Rightarrow z^{-1} e = \ldots\ldots$

(y, z^{-1}) ont des matrices dans cette base déterminées par les polynômes caractéristiques de y, z d'où le résultat.

En plus, on peut se donner librement les polynômes caractéristiques de y et z (pourvu qu'ils soient 1^{ers} entre eux).

$$y = \begin{pmatrix} 0 & 0 & * \\ 1 & 0 & * \\ 0 & 1 & * \end{pmatrix} \qquad \begin{matrix} z \, ? \\ z^{-1} \end{matrix} = \begin{pmatrix} * & 1 & 0 \\ * & 0 & 1 \\ * & 0 & 0 \end{pmatrix}$$

$xyz = 1$ $\qquad x$ de rg 1. Irréductib. à vérifier. ss condition

Propriétés des extensions de $\mathbb{Q}(T)$ obtenues par rigidité

Cas simple : 3 classes rationnelles rigides
G centre trivial.

$0, 1, \infty$.

$$\begin{array}{ccc} E & & X \\ \downarrow G & & G \downarrow \\ \mathbb{Q}(T) & & \mathbb{P}_1 \end{array}$$

1° question

Pts de ramification ?

0	1	∞
ou P_1	P_2	P_3
C_1	C_2	C_3

$e_i \geq 2$.

P_1. Q_1 pt fermé (= val. discrète) au-dessus de P_1, d'où gpes de décomp D_1 et d'inertie I_1

Par hypothèse $\quad I_1 = \langle x_1 \rangle, \quad x_1 \in C_1$
gpe cyclique

$$D_1 / I_1 = \mathrm{Gal}(\text{extension résiduelle})$$
$$\mathbb{Q}(Q_1)/\mathbb{Q}$$

Q_1 = orbite de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ agissant sur les $\overline{\mathbb{Q}}$-pts au-dessus de P_1.

En particulier $D_1 = I_1 \Leftrightarrow Q_1$ rationnel sur $\mathbb{Q}$.
On sait :

- $D_1 \subset N_G(I_1)$
- $D_1 | I_1 \longrightarrow \mathrm{Aut}(I_1)$
  est surjective

car $e_1 = |I_1|$. $\mathbb{Q}(Q_1) \supset \mu_{e_1}$

d'où $D_1/I_1 \xrightarrow{\text{surj}} \mathrm{Gal}(\mathbb{Q}(\mu_{e_1})/\mathbb{Q}) = \mathrm{Aut}\, I_1$

En particulier $D_1 \neq I_1$ s.f peut-être $e_1 = 2$.

- "conjugaison complexe" $\in D_1$.
  peut être calculée.

Ex. $G = M$ $\quad C_1, C_2, C_3 \quad 2A, 3B, 29A$.
$e_1 = 2 \quad I_1 = \{1, x_1\}$

$N_G\, I_1 / I_1 = BM$ ("Babymonster")

$\{1\} \subset D_1 / I_1 \subset BM$

à cause de conj complexe $\neq \{1\}$
en fait D_1 contient une involution de type $2B$. Mais sinon ?

Conjecture (fausse en général) $D_1 = N_G(I_1)$

Ex. $\quad G = S_n \quad C_1 = (12) \quad C_2 = (12 \dots n-1) \quad C_3 = (12 \dots n)$

$$\begin{array}{ccc} S_{n-1} & E & \\ & E_n & \\ & \Big| \, G = S_n & \\ n & \mathbb{Q}(T) & \end{array} \qquad \begin{array}{c} X_1 \simeq \mathbb{P}_1 \\ \Big\downarrow n \\ \mathbb{P}_1 \end{array} \qquad \begin{array}{l} Z \text{ paramètre} \\ T = \varphi(Z) \end{array}$$

$\varphi(Z) = Z^n + Z^{n-1}$

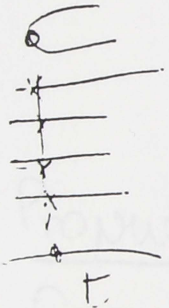
E_n = ext. de $\mathbb{Q}(T)$ engendré par une solution de $Z^n + Z^{n-1} - T = 0$.

$$N_{S_n}(I_1) = I_1 \times S_{n-2}$$

$D_1 / I_1 \subset S_{n-2}$

$Z = -\frac{n-1}{n}\, P_1 \qquad T(P_1) = \left(-\frac{n-1}{n}\right)^n + \left(-\frac{n-1}{n}\right)^{n-1}$

Pour cette valeur t de T, $Z^n + Z^{n-1} - t = (Z-\alpha)^2\, \phi_{n-2}(Z)$



$X_1 \simeq P_1$
$\Big\downarrow n$
P_1

ϕ_{n-2} donne les pts où le revêtement est étale

Image de D_1 / I_1 ds S_{n-2} = gpe de Galois du polynôme ϕ_{n-2}

A un changement de paramètres près,

$$\phi_{n-2} = X^{n-2} + 2X^{n-3} + 3X^{n-4} + \dots + n-1.$$

irréduct. sur $\mathbb{Q}$? (on ne le sait pas).

réduction modulo $p \Rightarrow$ Frobenius

si suffisamment $\Rightarrow$ Gal $= S_{n-2}$

Pour $n \leq 14$ sf $n = 8$ on trouve S_{n-2}

$n = 8$ on trouve $S_5 \subset S_6$ transitif (action de S_5 sur ses 6 5-Sylow par ex).

Pour $n = 18, 19, 49, 50, \dots$ Gal $\subset A_{n-2}$

(le discriminant est un carré)

Montre d'ailleurs que la conjecture + ht est fausse.

$$\begin{array}{c} X \\ \big\downarrow G \\ \mathbb{P}_1 \end{array} \qquad (0 \quad 1 \quad \infty)$$

K corps local.

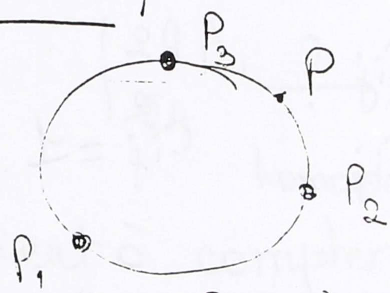
$\mathbb{P}_1(K)$ – ramification

$= \bigcup U_i$ disjointes fini

U_i ouvert fermé avec rev alg étale.

On ne sait pas grand chose sur les U.

Cas $K = \mathbb{R}$



$\mathbb{P}_1(\mathbb{R})$

algèbre sur $\mathbb{R}$

$P \longleftrightarrow$ classe de c_P conjugaison d'elt de G d'ordre 1 ou 2 ("conjugaison complexe au-dessus de P").

ie Q pt fermé au-dessus de P

D_Q gpe de décomposition ($I_Q = 1$)

$= \mathrm{Gal}(\mathbb{R}(Q)/\mathbb{R}) \subset G$

au plus 2 élts.

ou encore $\quad X(\mathbb{C})$

$\downarrow$

$\mathbb{P}_1(\mathbb{C}) \ni P$

$(P \in \mathbb{P}_1(\mathbb{R}))$.

F_P fibre de P est muni de l'action de G qui en fait un espace principal homogène muni aussi de conjug cplexe et les 2 commutent.

d'où classe de conj ds G (on prend pt origine et on trivialise l'esp. homogène)

Il s'agit de trouver c_P selon P: par continuité ne dépend que de la comp. connexe où se trouve P

Rigidité

$X_1\ X_2\ X_3 = 1 \qquad x_i \in C_i$ (113)

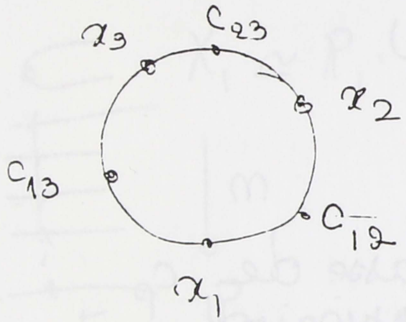
$X_1^{-1} X_2^{-1} = (X_2 X_3^{-1} X_2^{-1})^{-1}$ d'où $x_1^{-1} x_2^{-1} (x_2 x_3^{-1} x_2^{-1}) = 1$

$x_1^{-1} x_3^{-1} x_2^{-1} = 1 \qquad x_1^{-1} \in C_1,\ X_2^{-1} \in C_2,\ X_2 X_3^{-1} X_2^{-1} \in C_3$

d'où par rigidité il existe un unique $c_{12} \in G$ tq

$$x_1^{-1} = c_{12} x_1 c_{12}^{-1}$$
$$x_2^{-1} = c_{12} x_2 c_{12}^{-1} \qquad c_{12}^2 = 1$$

(car c_{12}^2 fixe x_1, x_2)



$$c_{ij}\, x_i = x_i^{-1} c_{ij}$$
$$c_{ij}\, x_j = x_j^{-1} c_{ij} \qquad c_{ij}^2 = 1$$

Thme Les c_{ij} sont les conjugaisons complexes associées aux pts réels de l'intervalle $]P_i, P_j[$

<u>Proposition</u> <u>Si l'ordre de x_1 est impair</u>, c_{12} <u>et</u> c_{13} <u>appartiennent à la même classe de conjugaison ds G.</u>

Identités

$$c_{23} = c_{12}\, x_2 = x_2^{-1} c_{12} \qquad x_2 = c_{12} c_{23}$$
$$c_{13} = c_{23}\, x_3 = x_3^{-1} c_{23} \qquad x_3 = c_{23} c_{13}$$
$$c_{12} = c_{13}\, x_1 = x_1^{-1} c_{13} \qquad x_1 = c_{13} c_{12}$$

$D_1 = \langle c_{12}, x_1 \rangle$ diedral et contient c_{13}

~~Si~~ c_{12}, c_{13} sont conjugués ds D_1 si e_1 est impair.

Si 2 des trois ordres sont impairs, c_{12}, c_{23}, c_{13} sont dans la même classe de conjugaison

Exemples

- $G = M$ $2A, 3B, 29A$

D'où 1_c bien définie ds M.

3 possibilités a priori $1, 2A, 2B$.

. 1 éliminé dès que les x ne st pas ts d'ordre 2 (car les renverse).

. 2A éliminé M contient un gpe diédral D_{29} dont c est une involution.

$$\left| \begin{matrix} 29A \\ 2A \end{matrix} \xrightarrow[\cdot]{?} M \right. \qquad x^2 = 1 \quad y^2 = 1$$
homomorph. $\qquad z^{29} = 1 \quad xyz = 1$

revient à compter le nbre d'élts ds $2A \times 2A \times 29A$ de produit 1 : on trouve 0, paraît-il.

d'où 2B.

- $S_n : X^n + X^{n-1} - T = 0$.

revient à discuter nbre de racines réelles de cette équation

que:

A part le cas $G = S_3$ on a $c_{ij} \neq 1$.

Pas d'extensions totalt réelles par la méthode de rigidité.

Si $c_{ij} = 1$ $\quad x_i$ et x_j sont d'ordre 2

$\Rightarrow G$ est diédral

$\Rightarrow G \simeq D_2, D_3, D_4$ ou D_6

centre trivial

$\Rightarrow D_3$ $(= S_3)$.

Remarque : Pour S_n, on sait qu'il existe des ext totalt réelles à gpe de Galois S_n.

$$X(X-1)-(X+n-1)=0$$

et on déforme ce polynôme

Pour A_n, OK par la méthode de Mestre.

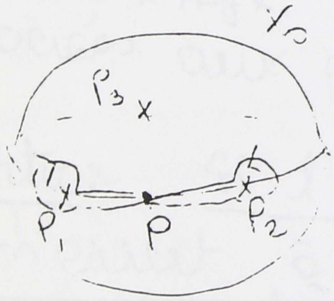
$$\begin{tikzcd} X \arrow[r, "\sigma"] \arrow[d, dashed] & X \arrow[d] \\ \mathbb{P}_1(\mathbb{C}) \arrow[r, "\sigma"] & \mathbb{P}_1 \end{tikzcd}$$

$p \in$ $\mathbb{P}_1(\mathbb{C})$, $\sigma P = P$

x_0

$$\pi_1(X_0, P) \xrightarrow{\sigma} \pi_1(X_0, P)$$

automorphisme d'ordre 1 ou 2.



Par σ : les 2 hémisphères se renversent

$x_2 \longrightarrow x_2^{-1}$

$x_1 \longrightarrow x_1^{-1}$

Cas p-adique

Thm (Raynaud) Supposons $|G|$ premier à la caractéristique résiduelle du corps local K.
Alors tout G-revêtement (étale) d'un polydisque fermé sur K au sens rigide est constant.

Sens : polydisque $A = K\{\{x_1, \dots, x_n\}\}$ séries à coeff tendant vers 0

$E_{/K}$ G-alg étale

$E \otimes_K A$

$$\begin{tikzcd} X \arrow[d, "G"] & E \arrow[d] \\ (\text{polyd}) \arrow[r] & pt_{/K} \end{tikzcd}$$

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

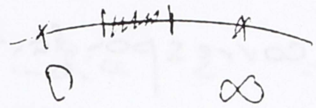
(11)

Ces polydisques "stabilisent" l'algèbre du revêtement

polydisque ne rencontrant pas la ramif.

⚠ $y=\sqrt{x}$

Sur tt polydisque ne contenant pas $0, \infty$



1 branche analyt de la racine carrée.

Corollaire Si une série $y=f(x)$ satisfait à une équation algébrique

$$y^n + a_1(x)\,y^{n-1} + \dots + a_n(x) = 0$$

et si le gpe de Galois est d'ordre $\neq$ à car résiduelle elle converge ds tt polydisque où $\Delta \neq 0$.

Pt essentiel de la démonst : en car p, $p \nmid |G|$, tt G-revêtement de l'espace affine est constant.

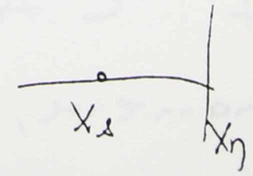
Thme "Bonne réduction" pour $p \nmid |G|$.

<u>Pb.</u> <u>Est-ce vrai avec seulement</u> $p \nmid$ <u>ordre des gpes d'inertie</u> ?

En car p, $p \nmid |G|$.
il existe un G-revêtement de la droite proj avec ramif en $0, 1, \infty$; classes C_1, C_2, C_3.

$\mathbb{P}_1 - \{0,1,\infty\} = X_{\eta|k} \supset X_{s|k}$ fibre génér.

$X / \mathcal{O}_K$



11/12/89 <u>Description sur $\mathbb{C}$ et $\mathbb{R}$</u> <u>du cas rigide</u> (117)

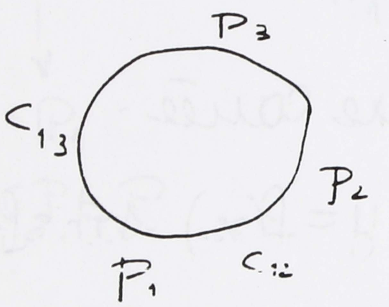
G centre trivial

C_1, C_2, C_3 rat $/\mathbb{Q}$ (sur $\mathbb{R}$ suffirait)

$P_1, P_2, P_3 \in \mathbb{P}_1(\mathbb{Q})$ distincts

Hyp. de rigidité

$$\begin{array}{l} X \\ \downarrow G \\ \mathbb{P}_1 \end{array}$$ revêtement correspondant



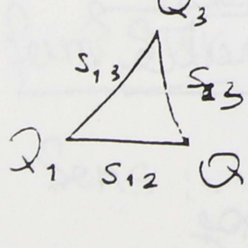
$x_1 x_2 x_3 = 1$ $\qquad$ $c_{12}^{\,2} = 1$ $\qquad$ $c_{12}\, x_1\, c_{12} = x_1^{-1}$

$c_{12}\, x_2\, c_{12} = x_2^{-1}$

m_1, m_2, m_3 ordres de x_1, x_2, x_3

pour simplifier $\frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} < 1$

Dans le plan hyperbolique H, on choisit un triangle (géodésique) d'angles $\frac{\pi}{m_1}, \frac{\pi}{m_2}, \frac{\pi}{m_3}$



Schwart (résultats généraux sur les groupes de Coxeter)

Γ : eng. par les symétries s_{ij} est un s/g discret $\subset \mathrm{Aut}(H)$

(str. Riemannienne, aut. de cette str.)

Γ présenté par les relations

$$s_{12}^2 = 1, \quad s_{13}^2 = 1, \quad s_{23}^2 = 1$$

$$(s_{12}\, s_{13})^{n_{23}} = 1, \cdots$$

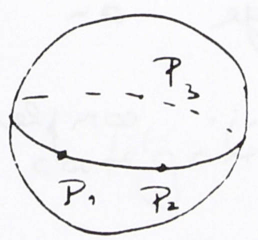
$H/\Gamma \simeq$ triangle.

Γ^+ : s/g d'indice 2 = élé de signature +1

$$1 \longrightarrow \Gamma^+ \longrightarrow \Gamma \longrightarrow \{\pm 1\} \longrightarrow 1$$

$$s_{ij} \longmapsto -1$$

$H/\Gamma^+ \simeq \mathbb{P}_1(\mathbb{C})$



triangle envoyé sur l'hémisphère nord.

x_1, x_2, x_3 choisis

$$\to N \to \Gamma \longrightarrow G \to 1 \qquad \text{surjectif}$$

$$s_{ij} \longmapsto c_{ij} \qquad\qquad N = \text{noyau}$$

$$x_1 \longmapsto c_{12}\, c_{13}$$

$$\to N^+ \longrightarrow \Gamma^+ \longrightarrow G \to 1$$

N est sans torsion, N^+ aussi (119)

(On connait les s/gs. de torsion de Γ, Γ_1 et $\Gamma \to G$ est ~~[illegible]~~ injectif sur ces s/gs.).

$X = \mathcal{H}/N_+$ — N^+ discret opère librement

$G = \Gamma^+/N^+$ opère sur X

$X/G = \mathcal{H}/\Gamma^+ = \mathbb{P}_1(\mathbb{C})$

$c \in N - N^+$: par passage au quot., c donne sur X la conj. complexe.

N ss torsion : on applique un résultat général sur les groupes de Coxeter :

Tout s/g fini de $W(S)$ est conjugué à un s/g d'un $W(\Sigma)$, $W(\Sigma)$ fini.(*)

Ici les $W(\Sigma)$ sont des groupes diédraux.]

(*) Bourbaki, ch. V, p. 130, exerc. 2 (d).

120

Description de l'utilisation du groupe des tresses (exposé de Malle).

Situation topologique:

variétés de modules pour les revêtements.

On ne veut pas d'automorphismes...

G-revêtements connexes à groupe G de centre trivial: pas d'automorphismes.

On peut $\overset{\text{donc}}{\text{espérer}}$ une variété de modules.

Topologie

Dans une catégorie où les revêtements sont décrits par le π_1 des lacets.

Par exemple, espaces localement contractiles.

X espace connexe, non vide

ensemble $\Sigma = \Sigma(G, X)$ des G-revêtements connexes de X, à isom près. (top. discrète)

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

G-revêt. connexe au-dessus de chaque $X \times \sigma$, $\sigma \in \Sigma$

$$\begin{array}{c} \tilde{X} \\ \downarrow \\ X \times \Sigma \\ \downarrow \\ \Sigma \end{array}$$

$X \simeq Y$ isom. top $\rightarrow$ $\tilde{X} \simeq \tilde{Y}$

Plus généralement, considérons une fibration :

$$\begin{array}{c} E \\ \downarrow F \\ B \end{array}$$ fibration

(thm. de relèvement des homotopies pour les polyèdres)

$b \in B \rightsquigarrow F_b$ fibre $\rightsquigarrow \Sigma_b$ discret

$$\begin{array}{c} E(B, G) \\ \downarrow G \\ B_\Sigma \\ \downarrow \\ B \end{array}$$

On veut un revêtement $B_\Sigma \to B$

t. q.

$$\begin{tikzcd} E(\Sigma, G) \arrow[d, "G"] & \\ E_\Sigma \arrow[r] \arrow[d] & E \arrow[d, "F"] \\ B_\Sigma \arrow[r] & B \end{tikzcd}$$

Fonctorialité

$$\begin{tikzcd} X \arrow[d] & \\ E' \arrow[r] \arrow[d] & E \arrow[d] \\ B' \arrow[r] & B \end{tikzcd}$$

G - rev de E' "connexe sur les fibres" image réc de $b' \in B'$ connexe.

<u>Hypothèse</u> F connexe.

Suite exacte d'homotopie

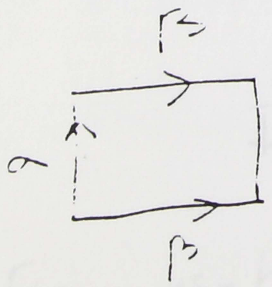
$$\begin{array}{l} x \in E \\ \downarrow \\ b \in B \end{array} \qquad F_b \text{ : fibre au-dessus de } b$$

$$\underbrace{\pi_2(B,b)}_{\text{abélien}} \xrightarrow{\partial} \pi_1(F_b, x) \to \pi_1(E, x) \to \pi_1(B, b) \to 1$$

Complément : le groupe $\pi_1(E, x)$ opère de façon naturelle sur $\pi_1(F_b, x)$

Clair si $\operatorname{Im} \partial = 1$, car alors $\pi_1(F, b)$ est un s/g invariant de $\pi_1(E, x)$.

Cas général :



$$\begin{tikzcd} I \times I \arrow[rr] & & B \\ \cup & & \\ J = \sqcup & & \\ J \arrow[rr] & & E \arrow[uuu] \end{tikzcd}$$

$I \longrightarrow B$ proj de β

relèvement des homotopies. on obtient

$$I \times I \to E$$ (124)

avec

$$\begin{tikzcd} J \arrow[d] \arrow[drr] & & \\ I \times I \arrow[rr] \arrow[drr] & & E \arrow[d, "p"] \\ & & B \end{tikzcd}$$

On obtient $\alpha * \beta$ $\qquad (\beta^{-1} \alpha \beta)$

si s/g invariant

Si l'espace fibré a une section passant par x, $\pi_2(E, x) \to \pi_2(B, b)$ est surjective donc $\partial = 0$, d'où action évidente de $\pi_1(E, x)$ sur $\pi_1(F, x)$.

On peut se ramener à ce cas.

$\Big(\pi_1(E, x) = \pi_1(F, x) \rtimes \pi_1(B, b)$

si section. $\Big)$

$$\begin{tikzcd} (x, x) \; E_2 \arrow[rr] \arrow[d, "F"] & & E \arrow[dd, "F"] \\ x \in E \arrow[u] \arrow[drr] & & \\ & & B \end{tikzcd}$$

$\pi_1(E, x)$ agit sur $\pi_1(F, x)$

description de $B_\Sigma \to B$, ... connexe.

ensemble où opère $\pi_1(B, b)$?

Soit Σ = ens. des homomorphismes surjectifs $\pi_1(F_b, x) \to G$.

L'action de $\pi_1(E, x)$ sur $\pi_1(F_b, x)$ définit une action de $\pi_1(E, x)$ sur Σ

G opère (aut. int.) sur Σ

D'où action de $\pi_1(E, x)$ sur Σ / G avec le noyau de cette action contenant l'image de $\pi_1(F_b, x)$.

D'où action de $\pi_1(B, b)$ sur Σ / G.

Le revêtement associé est B_Σ.

→ Revêtement $E(\Sigma, G)$.

($\pi_1(E, x)$ opère sur Σ).

Transposition en géométrie algébrique?

$$\begin{array}{c} X \\ \downarrow f \\ S \end{array}$$

Fibration f à fibres connexes.

$$\begin{array}{l} X \supset \Delta \\ \downarrow f \\ S \end{array}$$

f propre et lisse

Δ : ens. de ram

= diviseur

$\Delta \longrightarrow S$ lisse

fibres absolument connexes

("fibres géométriques connexes")

i.e. $f_* \mathcal{O}_X = \mathcal{O}_S$.

S localement noethérien.

G fini, centre trivial.

$(|G|$, car. rés. de $S) = 1$.

$i(S)$ = ensemble des classes d'isom. de G-revêtement de X connexes sur les fibres, rev. de $X - \Delta$. (étale en dehors de Δ)

connexe sur fibres : image réciproque d'un pt géom. de S connexe

$$\begin{array}{ccc} X' & \longrightarrow & X \\ \downarrow & & \downarrow \\ S' & \longrightarrow & S \end{array}$$

$i(s')$ est défini

<u>Théorème</u> (?)

<u>Le foncteur</u> $S \mapsto i(S)$ <u>est représentable</u> <u>par un</u> $S_\Sigma \to S$ (<u>rev. étale fini</u>)

$$\begin{array}{ccc} & \downarrow a & \\ X_\Sigma & \longrightarrow & X \\ \downarrow & & \downarrow \\ S_\Sigma & \longrightarrow & S \end{array}$$

Méthodes possibles:

1. car $= 0$
   a.) se ramener au cas où S est de type fini / $\mathbb{Q}$.
   b.) schémas de type fini / $\mathbb{C}$ on utilise la topologie.

GAGA (Grauert - Remmert) (128)

Top → Alg. / $\mathbb{C}$

puis descente de $\mathbb{C}$ à un ss/corps (à $\mathbb{Q}$).

(2) utilisation des critères de représentabilité de Grothendieck (exp. Murre, Bourbaki)

série de cond. pour qu'un foncteur soit repr. par un schéma étale

$S = \mathrm{Spec}(\Lambda)$, Λ anneau artinien.

$J \subset \Lambda$, $J^2 = 0$. Λ/J

$i(\Lambda/J) = i(S)$?

intuitivement

K local

A anneau des entiers

$$i(\operatorname{Spec} A) = i(\operatorname{Spec} K)$$

$$\begin{tikzcd} ? & \tilde{X} \arrow[d] \arrow[dl, dashed] \\ X_A \arrow[r, dash] \arrow[d, dash] & X \arrow[d, dash] \\ A & K \end{tikzcd}$$

G - rev ... abs connexe

étale en dehors de Σ

"bonne réduction" des revêtements

revêtement se prolonge à X_A

démonstration (cas particulier $\Sigma = \phi$)

On peut prolonger $\tilde{X}$ en un revêtement $\tilde{X}_A$

(a priori ramifié sur X_s (fibre spéciale)

de X_A.

Image réc. de X_s dans $\tilde{X}_A$

— géom. connexe

— div. réduit correspondant est lisse.

$\Downarrow$

géométriquement irréductible.

$\overline{}$ ss/var. lisse, géom. irréd.

$$\downarrow$$

$\overline{}\ X_s$

d'où groupe d'inertie I, et

groupe de déc $= G$

$$I \subset G \quad , \quad I \text{ distingué}$$

$$\begin{array}{c} I \\ \text{\rotatebox{90}{$\cong$}} \\ \mu_e \end{array} \qquad e = |I|$$

$\mu_e \subset k^*$ action de G est triviale sur k

$\Rightarrow I \subseteq Z(G) = \{1\}$

$\Rightarrow$ pas de ramification.

(3) Imiter la construction topologique.

$$\begin{array}{c} x \in X \\ \downarrow f \\ S \end{array} \qquad F \text{ fibre géom. de } X \text{ en } S.$$

$$\longrightarrow \pi_1(\overline{F}^{-\Delta}, x) \longrightarrow \pi_1(X^{-\Delta}, x) \to \pi_1(S, b) \to 1$$ (131)

$Gal(\overline{\mathbb{Q}}/\mathbb{Q})$

Si section, alors (sous hypothèses probablement vraies ici ...) SGA I exp. XIII, p. 420, Michèle Raynaud

Difficulté: section $\Longrightarrow$

$$\pi_1(F - \Delta_F) \longrightarrow \pi_1(X - \Delta)$$

injectif?

... alors $\pi_1(\overline{F} - \overline{\Delta}) \to \pi_1(X - \Delta)$

est injective (en car 0)

Puis on reprend la construction topologique.

W. Fulton: Annals 90 (1969)

"Hurwitz schemes"

$G = S_n$, $n \geq 3$

$$\begin{array}{ll} X & \text{fibré en} \\ \downarrow & \text{droites proj} \\ S & \end{array}$$

Méthode (2)

Schémas de Hurwitz

(132)

$X = \mathbb{P}_1$ $\quad X_k$: produit de k copies de $\mathbb{P}_1$

Δ_k = "diagonale"

$\{(x_1, \dots, x_k) \mid \exists\, i \neq j$ avec $x_i = x_j\}$.

$X_k - \Delta_k$ paramètre les familles de k points distincts (indexés) de X

$(X_k - \Delta_k)/S_k$ paramètre ss/ens. de k points de X.

$$\begin{array}{ccc} X_{k+1} & & (x_0, \dots, x_k) \\ \downarrow & & \downarrow \\ X_k & & (x_1, \dots, x_k) \end{array}$$

$$\begin{array}{c} X_{k-1} - \Delta_{k-1} \\ \downarrow \\ X_k - \Delta \end{array}$$

Fibres :

$\mathbb{P}_1 - \{x_1, \dots, x_k\}$

$$X'_{k+1} = X_{k+1} - \Delta_{k+1}$$

G à centre trivial.

On trouve ainsi

$$\begin{tikzcd}
\tilde{Z}_k \arrow[d, "G"] & \\
Z_k \arrow[r] \arrow[d] & X'_{k+1} \arrow[d] \\
Y'_k \arrow[r] & X'_k
\end{tikzcd}$$

rev. étale fini

$\tilde{Z}_k$ G-revêtement universel de Z_k

Ce sont des $\mathbb{Q}$-variétés.

"<u>Schémas de Hurwitz</u>".

On aurait pu partir de X'_k/S_k

On obtient un autre "schéma de Hurwitz".

On utilise X'_{k+1}/S_k.

Théorème : (1.4) (géom. convexe)

Pour qu'il existe un G-revêtement de $\mathbb{P}_1$ ramifié en k points rat. (resp. en k points), il faut et il suffit que Y_k' (resp. son analogue) ait un point rat. $/\mathbb{Q}$

$G \,\|\,$ a Gal_T

(II)

pour un k le schéma de H a un pt$/\mathbb{Q}$

$$\begin{array}{ccc} \vdots & & \\ \downarrow G & & \\ \text{fibre}: (\mathbb{P}_1 - \{k \text{ pts}\}) & \longrightarrow & X'_{k+1} \\ \downarrow & & \downarrow \\ \operatorname{Spec} \mathbb{Q} & \longrightarrow & X'_k \end{array}$$

On aurait pu fixer certains points et laisser d'autres mobiles.

Schémas de Hurwitz $\quad G$ donné

famille de k pts distincts numérotés.

(variant)

(135)

On associe classes de conj.

C_i de G.

Il faut choisir les racines de 1.

C^* = réunion des conj / $\mathbb{Q}$ de $(C_1, \dots, C_n)$.

Schémas de Hurwitz est somme disjointe d'ouverts-fermés corr. aux $C_1, \dots, C_n$.

$C = (C_1 \dots C_n)$ rat $\Rightarrow$ H_C : comp. corresp. de H.

rigidité $\Longleftrightarrow$ schéma de Hurwitz au-dessus de Spec $\mathbb{Q}$ est Spec $\mathbb{Q}$ lui-même.

$$\begin{array}{c} X'_{k+1} \\ \big\downarrow \\ X'_k \end{array}$$

$\pi_1(X'_k)$ sur ens. fini (classes d'hom. surjectifs du groupe libre $x_1, \dots x_k$, $(x_1 \cdots x_k) = 1$ sur G

ens. fini où opère $\pi_1(X_k') =$

= classes de conj. près d'éléments

$x_1, \dots, x_k \in G$, eng. G,

$x_1 \cdots x_k = 1$.

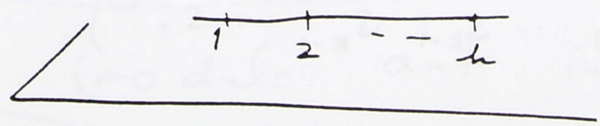
$\to \underbrace{\pi_1^{geom}(X_k)}_{\substack{\text{IIS} \\ \text{complété} \\ \text{profini} \\ \text{de } \pi_1(S_2 \times \cdots \times S_2 - \Delta)}} \to \pi_1(X_k') \longrightarrow Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to 1$

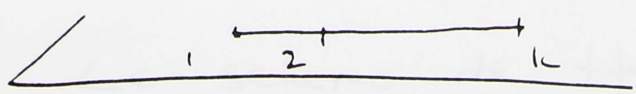
$S_2 = \mathbb{R}^2 \cup \{\infty\}$

$B_k^{pur} = \pi_1(\mathbb{R}^2 \times \cdots \times \mathbb{R}^2 - \Delta)$

= groupe des tresses pures

1, ..., k





$B_k = \pi_1(\text{——}/S_k)$ (137)

$$1 \to B_k^{\text{pur}} \longrightarrow B_k \to S_k \to 1$$

B_k présenté par $s_1, \dots, s_{k-1}$

relations $s_i s_j = s_j s_i$ si $|j-i| \geq 2$

$$s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$$

$i = 1, \dots, k-2$

s_i agit sur $(x_1, \dots, x_k)$ par

$$x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_k$$

$$\downarrow$$

$$x_1, \dots, x_{i-1}, x_i x_{i+1} x_i^{-1}, \dots, x_k$$

$\pi_1(S_2 \times \dots \times S_2 - \Delta)$: groupe de Hurwitz

= quotient de B_k

$$H_k = B_k / (s_1 \cdots s_{k-1} s_{k-1} \cdots s_1).$$

Connexion de la
(variété des modules des courbes alg ? (158)

$$g \text{ fixé} \qquad \begin{array}{c} X \\ \downarrow \\ \mathbb{P}_1 \end{array} \qquad \text{degré borné (en fonction de } g)$$

var. des modules d'un genre fixé

est connexe (Deligne-Mumford

en toute car.)

$$S_n \left(\begin{array}{c} X^{gal} \\ | \\ X \\ \downarrow \\ \mathbb{P}_1 \end{array} \right.$$

Méthode classique: type Morse

(indice de ram. 1 ou 2, pts doubles

au plus 1 pt de ordinaires

degré 2 au-dessus de pt donné

$G = S_n$, ram. par transposition

Thm (Clebsch, 1876 ?)

Le groupe des tresses agit transitivement

sur les systèmes de N transpositions

de S_n (modulo aut. int.)

de produit 1.

$\Longleftrightarrow$ Le schéma de Hurwitz correspondant

est (géom.) connexe.

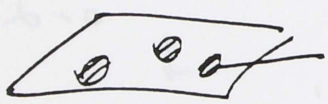
donc schéma des modules connexe

Serre
18/12/89

<u>Thm</u> de Harbater
(SLN 1240)

<u>Soit</u> p <u>un nombre premier</u>, <u>soit</u> G <u>un groupe fini</u>. <u>Il existe une extension galoisienne régulière de</u> $\mathbb{Q}_p(T)$, <u>à groupe de Galois</u> G.
(même énoncé sur $\mathbb{R}$, plus facile).

Démonstration utilise "GAGA rigide"
(cf "GAGA formel de Grothendieck)
sans utiliser structure du π_1

surface  D_i

On choisit, dans le groupe G, une collection de s/g cycliques $C_1, \dots, C_m$ engendrant G.
On choisit un petit disque D_i pour chaque i (disques disjoints)
Soit $U = S \setminus \bigcup D_i$; $S = U \cup D_1 \cup \dots \cup D_m$.
G-revêtement de S.
G-rev. de U : $U \times G$

$$\downarrow$$
$$U$$

Au-dessus de D_i, rev. ram. en 2 points.

Sur disque − 2 pts, il n'est pas affreux de fabriquer un rev. à groupe cyclique d'ordre donné, connexe, et trivial sur le bord.

On le fait sur la sphère : 

puis on enlève disque  sur lequel rev. est trivial : donc aussi sur le bord

 x, y $\quad x \to c$

$y \to c^{-1}$.

$$\begin{array}{c} D_i' \\ \downarrow C_i \\ D_i \end{array}$$

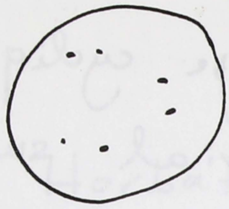
Puis : $D_i'' = D_i' \times_{C_i} G$

$$\begin{array}{c} \downarrow G \\ D_i \end{array}$$

trivial sur le bord. On recolle les revêtements. On obtient un revêtement à groupe G, connexe.

Composante connexe contenant la section : son groupe de st. de G contient les C_i, donc c'est G.

$x_1 x_1^{-1} \cdots x_n x_n^{-1} = 1$ (140)



rev. fabriqué grâce à ζ.

Structure de G ne joue pas de rôle.

Lemme :
Pour tout entier d, il existe un rev. cyclique géométriquement connexe, ramifié, du disque fermé sur $\mathbb{Q}_p$, dont la restriction au bord est triviale.

(en géom. rigide).

$|z|$ $\quad$ $|z| \leq 1$ $\quad$ $\downarrow$

disque $\nearrow$ $\quad$ couronne $|z| = 1$

Algèbre correspondante :

$K\{t\}$, séries formelles à coef $\to 0$.

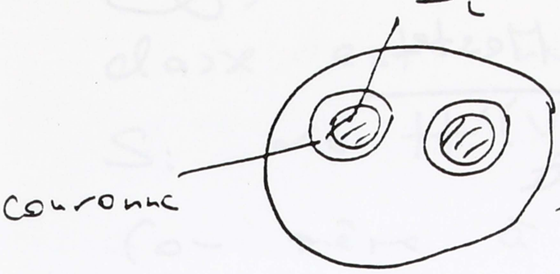
Résulte du lemme :
Il existe un revêtement cyclique de degré d donné de $\mathbb{P}_1/\mathbb{Q}$, géométriquement connexe et ayant un point non ramifié, rationel $/\mathbb{Q}$, complètement décomposé

n le montre par jacobiennes généralisées.

: $d | p-1$, 2 points $/\mathbb{Q}_p$ suffisent.

inon, ennuis de rationalité. ($2\varphi(d)$) points ?)

GAGA p-adique démontré par Kiehl. (142)



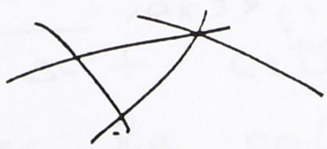
On imite la méthode

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

catégorie rigide

X est automatiquement une courbe alg. car corr. à faisceau cohérent rigide.

Harbater utilise GAGA formel :
utilise schémas formels, réduction p-adique complètement décomposé en droites



et il considère un "mock cover" relève en car 0, et il utilise Grothendieck.
Raynaud suggère d'utiliser la géométrie rigide.

Réalisation d'extensions centrales de A_n : exemples de Mestre

On se donne une suite exacte

$$\begin{array}{l} 1 \\ \downarrow \\ C \\ \downarrow \\ \tilde{\Omega} \\ \downarrow \\ \Omega \\ \downarrow \\ 1 \end{array}$$

$\tilde{\Omega}$ fini,

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

On dispose d'extensions galoisiennes de K à groupe Ω, et on aimerait en obtenir à groupe $\tilde{\Omega}$.

$K = \mathbb{Q}(T)$. On a une surjection

$$\begin{array}{ccc} & & \tilde{\Omega} \\ & \overset{\tilde{\varphi}\,?}{\nearrow} & \downarrow \\ \mathrm{Gal}(\bar{K}/K) & \xrightarrow{\varphi} & \Omega \end{array}$$

et on aimerait trouver un relèvement $\tilde{\varphi}$.

Suite exacte correspond à $c \in H^2(\Omega, C)$.

$\varphi^* c \in H^2(\mathrm{Gal}(\bar{K}/K), C)$

$\tilde{\varphi}$ existe $\Longleftrightarrow \varphi^* c = 0$.

Cohomologie étale : 

$\alpha \in H^2(U, C)$.

Suggère méthode pour montrer que la classe est nulle.

Si $\alpha \in H^2(V, C)$ se prolonge à $\mathbb{P}_1$ (ou même à $\mathbb{P}_1 - \{\infty\}$). Mais "tout ce qui est vrai sur le [T]" provient de là". Ce principe est vrai ici : donc α provient d'une classe $\in H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), C)$.

Soit $P/\mathbb{Q}$ un point. Supposons qu'en spécialisant en ce point,

$\alpha(P) \in H^2(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), C)$, $\alpha(P) = 0$.

α constant, $\alpha(P) = 0 \implies \alpha = 0$.

On suit cette méthode, mais sans utiliser la cohomologie étale.

Supposez $C \subset \Phi(\tilde{\Omega})$: s/g de Frattini, et φ surjectif. Alors tout $\tilde{\varphi}$ est surjectif. Si Ω est régulière, $\tilde{\Omega}$ l'est aussi (on utilise le même argument sur $\bar{\mathbb{Q}}$).

On en vient à un thm qui est rendu naturel par ce qui précède.

Soit k un corps de car 0.

$1 \to C \to \tilde{\Omega} \to \Omega \to 1$ suite exacte,

C central. S partie finie de $\mathbb{P}_1(\bar{k})$, stable par conjugaison et contenant $\infty \in \mathbb{P}_1(k)$.

G_S = groupe de Galois de l'extension maximale E de $k(T)$, non ramifiée en dehors de S ($\simeq \pi_1(\mathbb{P}_1 - S$, pt de base$)$)

Soit φ un homomorphisme $\varphi : G_S \to \Omega$ (cas intéressant : φ surjectif, rev. ramifié en S de $\mathbb{P}_1$).

Soit $\alpha = \varphi^* c \in H^2(G_S, C)$ l'obstruction à relever φ en $\tilde{\varphi} : G_S \to \tilde{\Omega}$.

Dans G_S, on a les groupes d'inertie I_s aux points de S. $(s \in S)$.

<u>Hypothèses</u>: <u>si</u> $s \in S - \{\infty\}$, $\varphi(I_s)$ est d'ordre premier à $|C|$, où I_s est le groupe d'inertie au-dessus de s (défini à conjugaison près).

$1 \to I \to G_S \to \Gamma \to 1$, $\Gamma = \mathrm{Gal}(\bar{k}/k)$.

$$G_S \left[\begin{array}{c} E \\ \Big| I \\ \bar{k}(T) \\ \Big| \Gamma \\ k(T) \end{array} \right.$$

Si $P_0 \in \mathbb{P}_1(k)$, $P_0 \notin S$, alors à P_0 est associé un scindage de la suite exacte

$$1 \to I \to G_S \to \Gamma \to 1.$$

Donc $G_S = I \cdot \Gamma_0$ semi-direct. ($\Gamma_0 \simeq \Gamma$)

Donc la cohomologie de Γ s'injecte dans celle de G_S :

$$H^2(\Gamma, C) \hookrightarrow H^2(G_S, C)$$

Théorème — Sous les hypothèses ci-dessus : α est constant, i.e. appartient à $H^2(\Gamma, C)$. Si en outre la restriction de φ au s/g Γ_0 est relevable dans $\tilde{\Omega}$, alors $\alpha = 0$.

$$\begin{array}{ccc} & & \tilde{\Omega} \\ & \nearrow & \\ I \cdot \Gamma_0 = G_S & \longrightarrow & \Omega \end{array}$$

relèvement de $\Gamma_0 \to \Omega$ à $\Gamma_0 \to \tilde{\Omega}$ se prolonge à $G_S \to \tilde{\Omega}$.

Exemple $\quad \Omega = A_n$, $\tilde{\Omega} = 2A_n$
$= \tilde{A}_n$

$C = \mathbb{Z}/2\mathbb{Z}$

$\varphi(I_s)$ s/g d'ordre 3.

$P_0 = 0$.

L'infini ne joue pas de rôle.
Les point ne sont pas vraiment indépendants
si

Démonstration

Structure de I : π_1 géométrique.

En topologie, $\pi_1(S_2 - S)$ = groupe libre
$(S \ni \infty)$ eng. par x_s
$x_1 \ldots x_s = 1$

= groupe libre eng. par
(produit libre complété) x_s, $s \neq \infty$

$\downarrow$

$I = \ast_{\substack{s \in S \\ s \neq \infty}} I_s$, I_s : groupe d'inertie
en un point au-dessus de s

Il existe façon de les choisir pour
que I soit le produit libre, dans
la catégorie des groupes profinis,
comme ci-dessus.

I est un groupe profini libre sur $S-\{\infty\}$, gén. eng. ds groupe d'inertie au-dessus de S.

$$\varphi_I : \varphi|I : I \to \bar{\Omega}$$

Lemme :

Il existe un unique relèvement $\tilde{\varphi}_I : I \to \tilde{\Omega}$ de φ_I tel que $\tilde{\varphi}_I(I_s)$ soit d'ordre premier à l'ordre de C pour tout $s \in S \setminus \{\infty\}$.

$I_s \simeq \hat{\mathbb{Z}}$ grâce à la théorie de la ramification.

$$I_s \equiv \hat{\mathbb{Z}} \xrightarrow[\varphi]{} \Omega$$

image de φ cyclique d'ordre premier à C

$$\tilde{\Omega} \xrightarrow{\pi} \Omega.$$

$$\pi^{-1}(\varphi(I_s)) = \varphi(I_s) \times C.$$

On relève φ_s : unique relèvement de φ_s avec propriété ci-dessus.

On demande propr. pour I_s, et aussi pour les autres groupes d'inertie. Ce sont des conjugués.

On a $\tilde{\varphi}_I : I \to \tilde{\Omega}$, propriété (149)
$\phantom{On a \tilde{\varphi}_I : } \cap$
d'unicité. $ G_S$

<u>Lemme</u> : <u>Si</u> $\sigma \in G_{\underline{S}}$, <u>et si</u> $i_\sigma \in \mathrm{Int}(\tilde{\Omega})$ <u>est l'automorphisme de</u> $\tilde{\Omega}$ <u>défini par</u> $\varphi(\sigma) \in \Omega$, <u>on a</u> $\tilde{\varphi}_I(\sigma x \sigma^{-1}) = i_\sigma(\tilde{\varphi}_I(x))$ $\forall x \in I$.

$$x \longmapsto i_\sigma^{-1}(\tilde{\varphi}_I(\sigma x \sigma^{-1}))$$

$$I \longrightarrow \tilde{\Omega}$$

au dessus de $I \longrightarrow \Omega$

$$\begin{tikzcd} I \arrow[r] \arrow[dr] & \tilde{\Omega} \arrow[d, "\pi"] \\ & \Omega \end{tikzcd}$$

cet homomorphisme a les mêmes propriétés que $\tilde{\varphi}_I$, donc ils sont égaux.

D'où la formule.

$$\begin{tikzcd}
 & 1 \arrow[d] & & 1 \arrow[d] \\
 & C \arrow[d] \arrow[rr, equal] & & C \arrow[d] \\
 & \widetilde{G}_s \arrow[d] & & \widetilde{\Omega} \arrow[d] \\
I \arrow[r] \arrow[ur, "\varepsilon"] & G_s \arrow[d] \arrow[rr, "\varphi"'] & & \Omega \arrow[d] \\
 & 1 & & 1
\end{tikzcd}$$

correspond à α.

On veut fabriquer une extension de Γ par C

$I \longrightarrow G_s$ injection

$$\begin{tikzcd}
 & \widetilde{\Omega} \\
I \arrow[r] \arrow[ur, "\widetilde{\varphi}_I"] & G_s
\end{tikzcd}$$

donc $1 \to I \to \widetilde{G}_s$

c'est un s/g normal, par l'identité du lemme précédent. Soit $\widetilde{\Gamma} = \widetilde{G}_s / I$. Alors on a :

$$1 \longrightarrow C \dashrightarrow \tilde{\Gamma} \longrightarrow \Gamma \longrightarrow 1 \, ,$$

et on a le diagramme

$$\begin{tikzcd}
C \arrow[r] \arrow[d] & C \arrow[d] \\
\tilde{G}_s \arrow[r] \arrow[d] & \tilde{\Gamma} \arrow[d] \\
G_s \arrow[r] \arrow[d] & \Gamma \arrow[d] \\
1 & 1
\end{tikzcd}$$

On combine, pour obtenir un homomorphisme $\tilde{G}_s \to \tilde{\Omega}$.

$\tilde{\varphi}_I : I \longrightarrow \tilde{\Omega}$, $I_s, s \in S, s \neq \infty$ sont envoyés ds groupes d'ordre premier à $|C|$.

Par contre, $\tilde{\varphi}_I(I_\infty)$ n'est pas tjs d'ordre premier à $|C|$.

Supposons φ, $\tilde{\varphi}$ surjectifs.

$\begin{matrix} X \\ \downarrow \Omega \\ \mathbb{P}_1 \end{matrix}$ revêtement. On a montré qu'il existe

$$\begin{tikzcd} \tilde{X} \arrow[d] \\ X \arrow[d] \\ \mathbb{P}_1 \end{tikzcd}$$

non ramifié, sauf peut-être au-dessus de $l'\infty$.

Exemple de Mestre : non ramifié à $l'\infty$.

Extensions à groupe A_n

$\tilde{A}_n = 2\,A_n$

Vila : $\tilde{A}_n$ a la propriété Gal_T

$n \equiv 0, 1 \pmod 8$

$\equiv 2, 3 \pmod 8$ + conditions.

Problème réel : $c \in A_n^+$, $c^2 = 1$

accepte-t-il de se relever ?

$$\begin{tikzcd} \tilde{A}_n \arrow[d] \\ A_n \end{tikzcd}$$

petites valeurs :

calculs de Mestre,

ne marche que pour $c = 1$...

polynômes avec toutes les racines réelles.

P polynôme de degré n sur $\mathbb{Q}$

$\neq 0$, racines rationnelles. Correspond à algèbre

al. $\mathbb{Q} \times \dots \times \mathbb{Q}$

Famille de polynômes P_T,

$T = 0 \to P$ fixé.

Marche bien pour n impair.

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

$a_i \in k$, car 0

Propriété de prolongement qui ne marche pas pour tous les a_i, mais seulement pour ceux qui ne sont pas racines d'un certain polynôme.

Propr. de $(a_1, \dots, a_n)$ est vraie en général si elle est vraie pour $(a_1, \dots, a_n) \in$ ouvert de Zariski non vide de Aff^n (i.e. pour ceux n'annulant pas un polynôme non constant).

Thm : Si P est général, il existe Q de degré $n-1$, coeff $\in k$, et R de degré $n-1$, t.q. $P'Q - PQ' = R^2$ premiers entre eux, et à P (et ils sont uniques à multiplication scalaire près)

$$T = \frac{P(x)}{Q(x)}$$ de degré n

$$\begin{tikzcd}
 & X^{gal} \arrow[d] \arrow[dd, bend right, "G"'] & \\
\mathbb{P}_1 \arrow[d, "n"] & X \arrow[d, "\varphi"] & \left\{ \begin{array}{l} Q=0 \\ \infty \end{array} \right. \arrow[d, "\text{non ramifié}"] \\
\mathbb{P}_1 & T & \infty
\end{tikzcd}$$

$t \in \mathbb{P}_1(k)$, fibre $P(x) - tQ(x) = 0$

$P_T(x) = P(x) - TQ(x)$.

(polynômes ont discriminants $\neq 0$).

dérivée : $\dfrac{dT}{dx} = \dfrac{QP' - PQ'}{Q^2} = \dfrac{R^2}{Q^2}$

a racines doubles, d'ordre exactement 2.

Donc les points de ramification sont tous d'ordre 3. Ce sont les $n-1$ zéros du polynôme R : $x_1, \dots, x_{n-1}$ $/\bar{k}$

Appelons $t_1, \dots, t_{n-1}$ les valeurs de $\frac{P}{Q}$ correspondantes. Si P est assez général, $t_1, \dots, t_{n-1}$ sont distincts.

Dans G, les groupes d'inertie correspondant aux $n-1$ points de ramification sont des 3-cycles (il y en a $n-1$ à conjugaison près). Ces groupes sont dans A_n, et le groupe qu'ils engendrent est transitif.

Lemme :

Tout s/g transitif de A_n engendré par des 3-cycles est A_n.

Groupe de Galois géométrique est A_n.

$G = A_n$ ou S_n.

Si S_n, ext. quadr. non ramifiée partout : $k(\sqrt{d})/k$.

$$\Delta(P_T) = \Delta(P) \cdot S(T)^2$$

degré $S = n-1$

racines $t_1, \dots, t_{n-1}$.

Supposons $\Delta(P) =$ carré dans k

$\Rightarrow G = A_n$.

Prenons $P = (X - \lambda_1) \dots (X - \lambda_n)$,

avec $(\lambda_1, \dots, \lambda_n) \in k^n$ assez général.

Alors $\Delta(P) = \prod_{i<j} (\lambda_i - \lambda_j)^2$ carré.

Donc on trouve une extension de $k(T)$ à groupe A_n.

Ramification d'ordre 3, premier à $2 = |\mathrm{Ker}\, \tilde{A}_n \to A_n|$.

Le point 0 se décompose complètement.

$\varphi : \Gamma \longrightarrow \Omega$ est trivial.

Il se relève. Donc il existe une extension de $k(T)$, galoisienne régulière à groupe $\tilde{A}_n$, contenant l'extension à groupe A_n construite précédemment, et avec en outre :

① 0 se décompose complètement

② ramification au-dessus de $t_1, \dots, t_{n-1}$ et ∞, est d'ordre 3 en $t_1, \dots, t_{n-1}$.

$$\tilde{A}_n \left(\begin{array}{c} \tilde{X}^{gal} \\ \downarrow \\ X^{gal} \\ \pi \downarrow A_n \\ \mathbb{P}_1 \end{array} \right.$$

— non ramifiée, sauf peut-être au-dessus de $\pi^{-1}(\infty)$.

En fait, elle n'est pas non plus ramifiée

α -dessus de ∞ (normalisée convenablement). (157)

Construction de Mestre

(méthode de Henniart).

On veut $(Q/P)'$ un carré :

$$(Q/P)' = \frac{R^2}{P^2}.$$

$$\frac{Q}{P} = \sum \frac{\lambda_i}{X-\alpha_i}, \quad \frac{R}{P} = \sum \frac{\mu_i}{X-\alpha_i}$$

$$P = \prod (X-\alpha_i)$$

$$\left(\frac{Q}{P}\right)' = -\sum \frac{\lambda_i}{(X-\alpha_i)^2} = \left(\frac{R}{P}\right)^2$$

$$= \sum \frac{\mu_i \mu_j}{(X-\alpha_i)(X-\alpha_j)}$$

$$\frac{1}{(X-\alpha_i)(X-\alpha_j)} = -\frac{1}{\alpha_j-\alpha_i} \left(\frac{1}{X-\alpha_i} - \frac{1}{X-\alpha_j}\right).$$

$$\left(\frac{R}{P}\right)^2 = \sum_{\substack{i,j \\ i \neq j}} \frac{\mu_i \mu_j}{\alpha_i-\alpha_j} \left(\frac{1}{X-\alpha_i} - \frac{1}{X-\alpha_j}\right) +$$

$$+ \sum \frac{\mu_i^2}{(X-\alpha_i)^2}.$$

$$\lambda_i = -\mu_i^2.$$

$$2\,\frac{\mu_i \mu_j}{\alpha_i - \alpha_j} \quad \text{coeff.}$$

D'où $\displaystyle\sum_{j \neq i} \frac{\mu_i \mu_j}{\alpha_i - \alpha_j} = 0$, i.e.

$$\mu_i \sum_{j \neq i} \frac{\mu_j}{\alpha_i - \alpha_j} = 0 \quad \text{pour tout } i$$

$\mu_i \neq 0$. On résoud le système

$$\sum_{j \neq i} \frac{\mu_j}{\alpha_i - \alpha_j} = 0 \quad , i = 1, \dots, n.$$

n équations, n inconnues.

La matrice est alternée, n est impair

$\Rightarrow \det = 0 \Rightarrow \exists$ solution $\neq 0$.

D'où λ_i, par $\lambda_i = -\mu_i^2$.

Pour P général, le système linéaire a le rang $n-1$. Cela se démontre en construisant ~~[illegible]~~ un exemple, bien choisi, à savoir :

$$\boxed{P = X^n - X.}$$

<u>n pair</u> : astuce :

$$\begin{array}{l} \tilde{X} \ \text{gal} \\ \big| \ \text{gal} \\ X \\ \big| \ A_{n-1} \ \text{— pair} \\ \mathbb{P}_1 = X \\ \downarrow \ n \ \text{impair} \\ \mathbb{P}_1 \end{array}$$

Non ramifié à l'infini : problème géométrique. On le fait sur $\mathbb{C}$.

Thm : Soit n impair ≥ 5. Soient $x_1, \dots, x_{n-1} \in A_n$ des 3-cycles.

On suppose $x_1 \cdots x_{n-1} = 1$, et x_i engendrent A_n

(on a besoin de $\geqslant n-1$ cycles, si on veut ces propriétés).

Soient $\tilde{X}_i$ les relèvement des x_i ds $\tilde{A}_n$ d'ordre 3.

Alors $\tilde{X}_1 \cdots \tilde{X}_n = 1$ dans $\tilde{A}_n$

(A priori, ce produit est ± 1).

('Voir exposé ENS.)

$$\tilde{A}_n \left(\begin{array}{l} \tilde{X}^{\,gal} \\ \downarrow \text{ non ramifié} \\ X^{\,gal} \\ \downarrow A_n \\ \underset{n-1}{\text{—×——×—}} \ / \ \mathbb{C} \end{array} \right.$$

marche si produit $= 1$.

Autre application du thm :

<u>Thm</u> (Mestre)
<u>Le</u> <u>groupe</u> $6A_6$ <u>a la</u> <u>propriété</u> Gal_T.

- Rappelons que l'on a déjà démontré :

<u>Thm</u> (Feit)
$3A_6$ <u>et</u> $3A_7$ <u>sont</u> Gal_T.

($6A_7$ n'est pas encore connu (il va l'être bientôt ...).)

Texel - Conf. (1989).

Même idée. ramification d'ordre 5.

D'abord, extension à groupe S_6
ramification d'ordre 2, 2, 5, 5

$$\left(\frac{Q}{P}\right)' = \frac{R^4 S}{P^2}, \quad \deg R = 2, \quad \deg S = 2.$$

2, 2 zéros de S

5, 5 " " R.

am.
,5,5,5

$$\begin{tikzcd} & X \arrow[dl, "A_6"'] \arrow[d, "S_6"] & \\ \mathbb{P}_1 \arrow[r] & \mathbb{P}_1 & \end{tikzcd}$$

gal

Point base fourni par $P = 0$
↑
degré 6
$\mathrm{disc}(P) =$ carré
On ne peut pas le prendre complètement décomposé. O.
... exemple plus compliqué! 22

On est amené à étudier la structure de $Br_2 k(T)$

Article de (D. K.) Faddeev ~ 1950 décrit $Br\, k(T)$

Problèmes : car $k \neq 2$.

- Soit $\alpha \in Br_2 k(T)$.

On suppose qu'il existe $t_0 \in k$ tel que $\alpha(t_0)$ soit défini, et soit 0 dans $Br_2(k)$. Est-ce qu'il existe un changement de variable $\varphi : \mathbb{P}_1 \to \mathbb{P}_1$ non constant, et $\operatorname{Im} \varphi \ni t_0$, $\varphi^* \alpha = 0$.

$k = \mathbb{Q}$ est un cas spécialement intéressant.

$k = \mathbb{C}(X)$.

- $SL_2(\mathbb{F}_7)$: groupe d'ordre $2 \cdot 168$

A-t-il la propriété Gal_T ?

Ce serait démontré si la réponse à la première question est "oui". [Cela a été démontré par J-P. Mestre dans le cas en question.]

$$\begin{array}{c} X \\ \downarrow \; PSL_2(\mathbb{F}_7) \\ \mathbb{P}_1 \end{array}$$

$\alpha \in Br_2\, \mathbb{Q}(T)$

il y a des t avec $\alpha(t) = 0$.

—

FIN DU COURS