JEAN-PIERRE SERRE
E. BAYER (réd.)
L. FAINSILBER (réd.)
J. COUGNARD (réd.)

Corps de fonctions et cohomologie galoisienne

Cours de Jean-Pierre Serre, tome 13 (1991-1992)
<http://www.numdam.org/item?id=CJPS_1992__13_>

Cours 1991–1992

–

Corps de fonctions et cohomologie galoisienne

–

Notes de E. Bayer
L. Fainsilber
J. Cougnard

Algèbre et géométrie

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

ANNUAIRE
DU
COLLÈGE DE FRANCE
1991 - 1992

RÉSUMÉ
DES COURS ET TRAVAUX

92e année

PARIS

11, place Marcelin-Berthelot (Ve)

Algèbre et géométrie

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

Le cours a été consacré à la cohomologie galoisienne des extensions transcendantes pures. Il a comporté deux parties.

I. Cohomologie de $k(\mathrm{T})$

Il s'agit de résultats essentiellement connus, dus à Faddeev, Scharlau, Arason, Elman,... On peut les résumer comme suit :

§1. Une suite exacte

Soient G un groupe profini, N un sous-groupe distingué fermé de G, Γ le quotient G/N, et C un G-module discret sur lequel N opère trivialement (i.e. un Γ-module). Faisons l'hypothèse :

(1.1) $\mathrm{H}^i(\mathrm{N},\mathrm{C}) = 0$ *pour tout* $i > 1$.

La suite spectrale $\mathrm{H}^{\cdot}(\Gamma,\mathrm{H}^{\cdot}(\mathrm{N},\mathrm{C})) \Rightarrow \mathrm{H}^{\cdot}(\mathrm{G},\mathrm{C})$ dégénère alors en une suite exacte :

(1.2) $\ldots \to \mathrm{H}^i(\Gamma,\mathrm{C}) \to \mathrm{H}^i(\mathrm{G},\mathrm{C}) \xrightarrow{r} \mathrm{H}^{i-1}(\Gamma,\mathrm{Hom}(\mathrm{N},\mathrm{C})) \to \mathrm{H}^{i+1}(\Gamma,\mathrm{C}) \to \ldots$

L'homomorphisme $r : \mathrm{H}^i(\mathrm{G},\mathrm{C}) \to \mathrm{H}^{i-1}(\Gamma,\mathrm{Hom}(\mathrm{N},\mathrm{C}))$ figurant dans (1.2) est défini de la manière suivante :

Si α est un élement de $\mathrm{H}^i(\mathrm{G},\mathrm{C})$, on peut représenter α par un cocycle $a(g_1,\ldots,g_i)$ qui est normalisé (i.e. égal à 0 lorsqu'un des g_j est égal à 1), et qui ne dépend que de g_1 et des images $\gamma_2,\ldots,\gamma_i$ de $g_2,\ldots,g_i$ dans Γ. Pour $\gamma_2,\ldots,\gamma_i$ fixés, l'application de N dans C définie par

$n \mapsto a(n,g_2,\ldots,g_i) \qquad (n \in \mathrm{N}),$

est un élément $b(\gamma_2,\ldots,\gamma_i)$ de $\mathrm{Hom}(N,C)$ et la $(i-1)$-cochaîne ainsi définie sur Γ est un $(i-1)$-cocycle à valeurs dans $\mathrm{Hom}(N,C)$; sa classe de cohomologie est $r(\alpha)$.

Faisons l'hypothèse supplémentaire :

(1.3) *L'extension* $1 \to N \to G \to \Gamma \to 1$ *est scindée.*

L'homomorphisme $H^i(\Gamma,C) \to H^i(G,C)$ est alors injectif, et (1.2) se réduit à la suite exacte :

(1.4) $0 \to H^i(\Gamma,C) \to H^i(G,C) \xrightarrow{r} H^{i-1}(\Gamma,\mathrm{Hom}(N,C)) \to 0.$

§2. Le cas local

Si K est un corps, on note K_s une clôture séparable de K, et l'on pose $G_K = \mathrm{Gal}(K_s/K)$. Si C est un G_K-module (discret), on écrit $H^i(K,C)$ à la place de $H^i(G_K,C)$.

Supposons que K soit muni d'une *valuation discrète* v, de corps résiduel $k(v)$; notons K_v le complété de K pour v. Choisissons un prolongement de v à K_s ; soient D et I les groupes de décomposition et d'inertie correspondants ; on a $D \simeq G_{K_v}$ et $D/I \simeq G_{k(v)}$.

Soit n un entier > 0, premier à la caractéristique de $k(v)$, et soit C un G_K-module tel que $nC = 0$. Faisons l'hypothèse suivante :

(2.1) C *est non ramifié en* v (i.e. I opère trivialement sur C).

On peut alors appliquer à la suite exacte $1 \to I \to D \to G_{k(v)} \to 1$ les résultats du §1 (les hypothèses (1.1) et (1.3) se vérifient sans difficulté). Le $G_{k(v)}$-module $\mathrm{Hom}(I,C)$ s'identifie à $C(-1) = \mathrm{Hom}(\mu_n,C)$, où μ_n désigne le groupe des racines n-èmes de l'unité (dans $k(v)_s$ ou dans K_s, cela revient au même). Vu (1.4), cela donne la suite exacte :

(2.2) $0 \to H^i(k(v),C) \to H^i(K_v,C) \xrightarrow{r} H^{i-1}(k(v),C(-1)) \to 0.$

Soit $\alpha \in H^i(K,C)$ et soit α_v son image (par restriction) dans $H^i(K_v,C)$. L'élément $r(\alpha_v)$ de $H^{i-1}(k(v),C(-1))$ est appelé le *résidu de* α *en* v, et noté $r_v(\alpha)$. S'il est non nul, on dit que α *a un pôle en* v. S'il est nul, on dit que α est *régulier* (ou « holomorphe ») *en* v ; dans ce cas, α_v s'identifie à un élément de $H^i(k(v),C)$, qui est appelé la *valeur de* α *en* v, et noté $\alpha(v)$.

§3. Courbes algébriques et corps de fonctions d'une variable

Soit X une courbe projective lisse connexe sur un corps k, et soit $K = k(X)$ le corps de fonctions correspondant. Soit $\underline{X}$ l'ensemble des points fermés du schéma X. Un élément x de $\underline{X}$ peut être identifié à une *valuation discrète* de K, triviale sur k ; on note $k(x)$ le corps résiduel correspondant ; c'est une extension finie de k.

Comme ci-dessus, soit n un entier > 0, premier à la caractéristique de k, et soit C un G_k-module tel que $nC = 0$. Le choix d'un plongement de k_s dans K_s définit un homomorphisme $G_K \to G_k$, ce qui permet de considérer C comme un G_K-module. Pour tout $x \in \underline{X}$, l'hypothèse (2.1) est satisfaite. Si $\alpha \in H^i(K,C)$, on peut donc parler du *résidu* $r_x(\alpha)$ *de* α *en* x ; on a $r_x(\alpha) \in H^{i-1}(k(x),C(-1))$. On démontre :

(3.1) *On a* $r_x(\alpha) = 0$ *pour tout* $x \in \underline{X}$ *sauf un nombre fini* (autrement dit l'ensemble des pôles de α est fini).

De façon plus précise, soit L/K une extension galoisienne finie de K assez grande pour que α provienne d'un élément de $H^i(\mathrm{Gal}(L/K),C_L)$, où $C_L = H^0(G_L,C)$. On a $r_x(\alpha) = 0$ pour tout x en lequel l'indice de ramification de L/K est premier à n.

(3.2) *On a la « formule des résidus » :*

$$\sum_{x \in \underline{X}} \mathrm{Cor}_k^{k(x)}\, r_x(\alpha) = 0 \qquad \textit{dans } H^{i-1}(k,C(-1)),$$

où $\mathrm{Cor}_k^{k(x)} : H^{i-1}(k(x),C(-1)) \to H^{i-1}(k,C(-1))$ *désigne l'homomorphisme de corestriction relativement à l'extension* $k(x)/k$.

[Précisons ce que l'on entend par Cor_E^F si F/E est une extension finie : c'est le produit de la corestriction galoisienne usuelle (correspondant à l'inclusion $G_F \to G_E$) par le degré inséparable $[F:E]_i$. Le composé $\mathrm{Cor}_E^F \circ \mathrm{Res}_F^E$ est égal à la multiplication par $[F:E]$.]

Application

Soit $f \in K^*$, et soit $D = \sum_{x \in \underline{X}} n_x x$ le diviseur de f. Supposons D disjoint de l'ensemble des pôles de α. Cela permet de définir un élément $\alpha(D)$ de $H^i(k,C)$ par la formule

$$\alpha(D) = \sum_{x \in |D|} n_x \mathrm{Cor}_k^{k(x)}\, \alpha(x).$$

On déduit de (3.2) la formule suivante :

(3.3) $$\alpha(D) = \sum_{x \text{ pôle de } \alpha} \mathrm{Cor}_k^{k(x)}\, (f(x)).r_x(\alpha),$$

où :

$(f(x))$ est l'élément de $H^1(k(x),\mu_n)$ défini par l'élément $f(x)$ de $k(x)$, *via* la théorie de Kummer ;

$r_x(\alpha) \in H^{i-1}(k(x),C(-1))$ est le résidu de α en x ;

$(f(x)).r_x(\alpha)$ est le cup-produit de $(f(x))$ et de $r_x(\alpha)$ dans $H^i(k(x),C)$, relativement à l'application bilinéaire $\mu_n \times C(-1) \to C$.

Lorsque α n'a pas de pôles, (3.3) se réduit à :

$\alpha(\mathrm{D}) = 0$,

analogue cohomologique du *théorème d'Abel.* Cela permet d'associer à α un homomorphisme du groupe des points rationnels de la jacobienne de X dans le groupe $\mathrm{H}^i(k,\mathrm{C})$; pour $i = 1$, on retrouve une situation étudiée dans le cours de 1956-1957 (cf. *Groupes algébriques et corps de classes,* Hermann, Paris, 1959).

§4. Le cas où $\mathrm{K} = k(\mathrm{T})$

C'est celui où X est la droite projective $\mathbf{P}_1$. Du fait que X possède un point rationnel, l'homomorphisme canonique $\mathrm{H}^i(k,\mathrm{C}) \to \mathrm{H}^i(\mathrm{K},\mathrm{C})$ est injectif. Un élément de $\mathrm{H}^i(\mathrm{K},\mathrm{C})$ est dit *constant* s'il appartient à $\mathrm{H}^i(k,\mathrm{C})$. On démontre :

(4.1) *Pour que* $\alpha \in \mathrm{H}^i(\mathrm{K},\mathrm{C})$ *soit constant, il faut et il suffit que* $r_x(\alpha) = 0$ *pour tout* $x \in \underline{\mathrm{X}}$ (i.e. que α n'ait pas de pôles).

(4.2) *Pour tout* $x \in \underline{\mathrm{X}}$, *soit* $\rho_x \in \mathrm{H}^{i-1}(k(x),\mathrm{C}(-1))$. *Supposons que* $\rho_x = 0$ *pour tout* x *sauf un nombre fini, et que :*

$$\sum_{x \in \underline{\mathrm{X}}} \mathrm{Cor}_k^{k(x)} \rho_x = 0 \qquad \textit{dans } \mathrm{H}^{i-1}(k,\mathrm{C}(-1)).$$

Il existe alors $\alpha \in \mathrm{H}^i(\mathrm{K},\mathrm{C})$ *tel que* $r_x(\alpha) = \rho_x$ *pour tout* $x \in \underline{\mathrm{X}}$.

On peut résumer (3.1), (3.2), (4.1), (4.2) par la suite exacte :

$$(4.3) \quad 0 \to \mathrm{H}^i(k,\mathrm{C}) \to \mathrm{H}^i(\mathrm{K},\mathrm{C}) \to \bigoplus_{x \in \underline{\mathrm{X}}} \mathrm{H}^{i-1}(k(x),\mathrm{C}(-1)) \to \mathrm{H}^{i-1}(k,\mathrm{C}(-1)) \to 0.$$

Remarque — Soit $\alpha \in \mathrm{H}^i(\mathrm{K},\mathrm{C})$, et soit P l'ensemble de ses pôles. Les énoncés ci-dessus montrent que α est déterminé sans ambiguïté par ses résidus, et par sa valeur en un point rationnel de X non contenu dans P. En particulier, la *valeur* de α peut se calculer à partir de ces données. Voici une formule permettant de faire un tel calcul si $\infty \notin \mathrm{P}$:

$$(4.4) \quad \alpha(x) = \alpha(\infty) + \sum_{y \in \mathrm{P}} \mathrm{Cor}_k^{k(y)} (x - y).r_y(\alpha),$$

où :

$\alpha(x)$ est la valeur de α en un point rationnel $x \in \mathrm{X}(k)$, $x \notin \mathrm{P}$, $x \neq \infty$;

$\alpha(\infty)$ est la valeur de α au point ∞ ;

$(x - y)$ est l'élément de $\mathrm{H}^1(k(y),\mu_n)$ défini par $x - y$;

$(x - y).r_y(\alpha)$ est le cup-produit de $(x - y)$ par le résidu $r_y(\alpha)$, calculé dans $\mathrm{H}^i(k(y),\mathrm{C})$;

$\mathrm{Cor}_k^{k(y)}$ est la corestriction : $\mathrm{H}^i(k(y),\mathrm{C}) \to \mathrm{H}^i(k,\mathrm{C})$.

Cela se déduit de (3.3), appliqué à la fonction $f(\mathrm{T}) = x - \mathrm{T}$, dont le diviseur D est $(x) - (\infty)$.

Généralisation à plusieurs variables

Soit $K = k(T_1,...,T_m)$ le corps des fonctions de l'espace projectif $\mathbf{P}_m$ de dimension m. Tout diviseur irréductible W de $\mathbf{P}_m$ définit une valuation discrète v_W de K. L'énoncé suivant se déduit de (4.1) par récurrence sur m :

(4.5) *Pour que* $\alpha \in H^i(K,C)$ *soit constant* (i.e. appartienne à $H^i(k,C)$), *il faut et il suffit que* α *n'ait de pôle en aucun* v_W (et l'on peut même se borner aux W distincts de l'hyperplan à l'infini, i.e. se placer sur *l'espace affine* de dimension m, et non sur l'espace projectif).

II. APPLICATION : SPÉCIALISATION DU GROUPE DE BRAUER

§5. Notations

Ce sont celles du §4, avec $i = 2$ et $C = \mu_n$, d'où $C(-1) = \mathbf{Z}/n\mathbf{Z}$. On a $H^2(K,C) = \mathrm{Br}_n K$, noyau de la multiplication par n dans le groupe de Brauer de K. La suite exacte (4.3) s'écrit alors :

$$0 \to \mathrm{Br}_n k \to \mathrm{Br}_n K \to \bigoplus_{x \in \underline{X}} H^1(k(x),\mathbf{Z}/n\mathbf{Z}) \to H^1(k,\mathbf{Z}/n\mathbf{Z}) \to 0.$$

Elle est due à D.K. Faddeev (*Trud. Math. Inst. Steklov* 38 (1951), 321-344).

Soit $\alpha \in \mathrm{Br}_n K$, et soit $P(\alpha) \subset \underline{X}$ l'ensemble de ses pôles. Si $x \in X(k)$ est un point rationnel de $X = \mathbf{P}_1$, et si $x \notin P(\alpha)$, la valeur de α en x est un élément $\alpha(x)$ de $\mathrm{Br}_n k$. On s'intéresse à la variation de $\alpha(x)$ avec x, et en particulier à l'ensemble $V(\alpha)$ des x tels que $\alpha(x) = 0$ (« *lieu des zéros de* α »). On aimerait comprendre la structure de $V(\alpha)$. (Par exemple, si k est infini, est-il vrai que $V(\alpha)$ est soit vide, soit de cardinal égal à celui de k ?).

Le cas où $n = 2$ et où α est un symbole (f,g), avec $f,g \in K^*$, est particulièrement intéressant, à cause de son interprétation en termes du *fibré en coniques* de base X défini par l'équation homogène

$$U^2 - f(T)V^2 - g(T)W^2 = 0.$$

L'étude de $V(\alpha)$ peut être abordée de plusieurs points de vue. Le cours en a envisagé trois :

annulation de α par changement de base rationnel (cf. §6) ;

conditions de Manin et approximation faible (cf. §7) ;

bornes du crible (cf. §8).

§6. Annulation par changement de base

On suppose, pour simplifier, que k est de caractéristique 0.

Soit $\alpha \in \mathrm{Br}_n\mathrm{K}$, avec $\mathrm{K} = k(\mathrm{T})$ comme ci-dessus. Soit $f(\mathrm{T}')$ une fonction rationnelle en une variable T' ; supposons f non constante. Si l'on pose $\mathrm{T} = f(\mathrm{T}')$, on obtient un plongement de K dans $\mathrm{K}' = k(\mathrm{T}')$. D'où, par changement de base, un élément $f^*\alpha$ de $\mathrm{Br}_n\mathrm{K}'$. On dit que α est *tué par* K'/K (ou par f) si $f^*\alpha = 0$ dans $\mathrm{Br}_n\mathrm{K}'$. S'il en est ainsi, on a $\alpha(t) = 0$ pour tout $t \in \mathrm{X}(k)$ qui n'est pas un pôle de α, et qui est de la forme $f(t')$, avec $t' \in \mathbf{P}_1(k)$. En particulier, $\mathrm{V}(\alpha)$ est *non vide* (et même de cardinal égal à celui de k). On peut se demander s'il y a une réciproque. D'où la question suivante :

(6.1) *Supposons* $\mathrm{V}(\alpha)$ *non vide. Existe-t-il une fonction rationnelle non constante f qui tue* α *?*

Voici une variante « à point-base » de (6.1) :

(6.2) *Soit* $t_o \in \mathrm{V}(\alpha)$. *Existe-t-il f comme dans* (6.1), *telle que* t_o *soit de la forme* $f(t'_o)$, *avec* $t'_o \in \mathbf{P}_1(k)$ *?*

On sait (Janchevskii, *Dokl. Akad. Nauk URSS,* 29, 1985, 1061-1064) que (6.2) a une réponse positive lorsque k est hensélien (ou lorsque $k = \mathbf{R}$).

Lorsqu'on ne fait pas d'hypothèse sur k, on n'a de résultats que pour $n = 2$. Pour les énoncer, introduisons la notation suivante :

(6.3) $$d(\alpha) = \deg \mathrm{P}(\alpha) = \sum_{x \in \mathrm{P}(\alpha)} [k(x):k].$$

(L'entier $d(\alpha)$ est le *nombre de pôles* de α, multiplicités comprises.)

Théorème 6.4. (J.-F. Mestre, non publié) (i) *La question* (6.2) *a une réponse positive lorsque* $n = 2$ *et* $d(\alpha) \leqslant 4$.

(ii) *La question* (6.1) *a une réponse positive lorsque* $n = 2$, $d(\alpha) = 5$, *et que tout élément de* Br_2k *est un symbole* (i.e. toute forme quadratique sur k de rang 6 et de discriminant -1 représente 0).

Remarques

1) Dans (ii), la condition portant sur k est satisfaite lorsque k est un corps de nombres algébriques.

2) La démonstration du th. 6.4 donne des informations supplémentaires sur les corps $\mathrm{K}' = k(\mathrm{T}')$ qui tuent α : par exemple, on peut choisir K' tel que $[\mathrm{K}':\mathrm{K}] = 8$ dans le cas (i), et $[\mathrm{K}':\mathrm{K}] = 16$ dans le cas (ii).

Du th. 6.4, Mestre a déduit le résultat suivant :

Théorème 6.5. *Le groupe* $\mathbf{SL}_2(\mathbf{F}_7)$ *a la propriété* « Gal_T », *i.e. est groupe de Galois d'une extension galoisienne régulière de* $\mathbf{Q}(\mathrm{T})$.

En particulier, il existe une infinité d'extensions galoisiennes de $\mathbf{Q}$, deux à deux disjointes, dont le groupe de Galois est $\mathbf{SL}_2(\mathbf{F}_7)$.

Mestre a obtenu des résultats analogues pour les groupes $6.A_6$ et $6.A_7$.

§7. Conditions de Manin, approximation faible et hypothèse de Schinzel

On suppose maintenant que k est un *corps de nombres* algébriques, de degré fini sur $\mathbf{Q}$. Soit Σ l'ensemble de ses places (archimédiennes et ultramétriques) ; si $v \in \Sigma$, on note k_v le complété de k pour v. Soit $\mathbf{A}$ *l'anneau des adèles* de k, autrement dit le produit restreint des k_v $(v \in \Sigma)$.

Soit $X(\mathbf{A}) = \prod_v X(k_v)$ l'espace des points adéliques de $X = \mathbf{P}_1$. C'est un espace compact. A un élément α de $\mathrm{Br}_n K$ on associe le sous-espace $V_{\mathbf{A}}(\alpha)$ défini de la façon suivante :

un point adélique $x = (x_v)$ appartient à $V_{\mathbf{A}}(\alpha)$ si, pour tout $v \in \Sigma$, on a $x_v \notin P(\alpha)$ et $\alpha(x_v) = 0$ dans $\mathrm{Br}_n k_v$.

(Autrement dit, $V_{\mathbf{A}}(\alpha)$ est l'ensemble des *solutions adéliques* de l'équation $\alpha(x) = 0$.)

Toute solution dans k de $\alpha(x) = 0$ est évidemment une solution adélique. On a donc une inclusion :

$V(\alpha) \subset V_{\mathbf{A}}(\alpha)$,

et l'on peut se demander quelle est *l'adhérence* de $V(\alpha)$ dans $V_{\mathbf{A}}(\alpha)$. Pour répondre (ou tenter de répondre) à cette question, il y a lieu d'introduire (à la suite de Colliot-Thélène et Sansuc) les « *conditions de Manin* » :

Disons qu'un élément β de $\mathrm{Br}_n K$ est *subordonné* à α si, pour tout $x \in \underline{X}$, $r_x(\beta)$ est un multiple entier de $r_x(\alpha)$; on a en particulier $P(\beta) \subset P(\alpha)$. Soit $\mathrm{Sub}(\alpha)$ l'ensemble de ces éléments ; c'est un sous-groupe de $\mathrm{Br}_n K$ contenant $\mathrm{Br}_n k$, et le quotient $\mathrm{Sub}(\alpha)/\mathrm{Br}_n k$ est fini. Si $\beta \in \mathrm{Sub}(\alpha)$, et si $x = (x_v)$ est un point de $V_{\mathbf{A}}(\alpha)$, on a $\beta(x_v) = 0$ pour presque tout v. Cela permet de définir un élément $m(\beta,x)$ de $\mathbf{Q}/\mathbf{Z}$ par la formule :

(7.1) $m(\beta,x) = \sum_v \mathrm{inv}_v\, \beta(x_v)$,

où inv_v désigne l'homomorphisme canonique de $\mathrm{Br}\, k_v$ dans $\mathbf{Q}/\mathbf{Z}$. La fonction $x \mapsto m(\beta,x)$ est localement constante sur $V_{\mathbf{A}}(\alpha)$ et s'annule sur $V(\alpha)$; de plus, elle ne dépend que de la classe de β mod $\mathrm{Br}_n k$. Notons $V_{\mathbf{A}}^{\mathrm{M}}(\alpha)$ le sous-espace de $V_{\mathbf{A}}(\alpha)$ défini par les « conditions de Manin » :

(7.2) $m(\beta,x) = 0$ *pour tout* $\beta \in \mathrm{Sub}(\alpha)$.

C'est un sous-espace *ouvert et fermé* de $V_{\mathbf{A}}(\alpha)$ qui contient $V(\alpha)$. Il paraît raisonnable de faire la *conjecture* suivante :

(7.3 ?) $V(\alpha)$ *est dense dans* $V_{\mathbf{A}}^{\mathrm{M}}(\alpha)$.

En particulier :

(7.4 ?) *Si* $V_A^M(\alpha) \neq \emptyset$, *on a* $V(\alpha) \neq \emptyset$: les conditions de Manin sont « les seules » à s'opposer à l'existence d'une solution rationnelle de l'équation $\alpha(x) = 0$.

(7.5 ?) *Si* $\mathrm{Sub}(\alpha) = \mathrm{Br}_n k$ (i.e. s'il n'y a pas de conditions de Manin), $V(\alpha)$ *est dense dans* $V_A(\alpha)$; il y a *approximation faible* ; le principe de Hasse est valable.

La plupart des résultats concernant (7.3 ?), (7.4 ?) et (7.5 ?) sont relatifs au cas $n = 2$. Dans le cas général, on a toutefois le théorème suivant, qui complète des résultats antérieurs de Colliot-Thélène et Sansuc (1982) et Swinnerton-Dyer (1991) :

Théorème 7.6. *L'hypothèse* (H) *de Schinzel entraîne* (7.3 ?).

[Rappelons l'énoncé de l'hypothèse (H) : soient $P_1(T),\ldots,P_m(T)$ des polynômes à coefficients dans $\mathbf{Z}$, irréductibles sur $\mathbf{Q}$, de termes dominants > 0, et tels que, pour tout nombre premier p, il existe $n_p \in \mathbf{Z}$ tel que $P_i(n_p) \not\equiv 0 \pmod p$ pour $i = 1,\ldots,m$. Alors il existe une infinité d'entiers $n > 0$ tels que $P_i(n)$ soit un nombre premier pour $i = 1,\ldots,m$.]

Remarque

Le th. 7.6 peut être étendu aux *systèmes d'équations* $\alpha_i(x) = 0$, où les α_i sont des éléments de $\mathrm{Br}_n K$ en nombre fini. On doit alors remplacer $\mathrm{Sub}(\alpha)$ par l'ensemble des $\beta \in \mathrm{Br}_n K$ tels que, pour tout $x \in \underline{X}$, $r_x(\beta)$ appartienne au sous-groupe de $H^1(k(x),\mathbf{Z}/n\mathbf{Z})$ engendré par les $r_x(\alpha_i)$.

§8. Bornes du crible

On conserve les notations ci-dessus, et l'on suppose en outre (pour simplifier) que $k = \mathbf{Q}$. Si $x \in X(k) = \mathbf{P}_1(\mathbf{Q})$, on note $H(x)$ la *hauteur* de x : si $x = p/q$ où p et q sont des entiers premiers entre eux, on a $H(x) = \sup(|p|, |q|)$. Si $H \to \infty$, le nombre des x tels que $H(x) \leqslant H$ est $cH^2 + O(H.\log H)$, avec $c = 12/\pi^2$.

Soit $N_\alpha(H)$ le nombre des $x \in V(\alpha)$ tels que $H(x) \leqslant H$. On aimerait connaître la croissance de $N_\alpha(H)$ quand $H \to \infty$. Un argument de crible (cf. *C.R. Acad. Sci. Paris,* 311 (1990), 397-402) permet en tout cas d'en donner une *majoration.* Pour énoncer le résultat, convenons de noter $e_x(\alpha)$ l'ordre du résidu $r_x(\alpha)$ de α en x (pour $x \in \underline{X}$) ; on a $e_x(\alpha) = 1$ si x n'est pas un pôle de α. Posons

$$(8.1) \quad \delta(\alpha) = \sum_{x \in \underline{X}} (1 - 1/e_x(\alpha)).$$

Théorème 8.2. *On a* $N_\alpha(H) << H^2/(\log H)^{\delta(\alpha)}$ *pour* $H \to \infty$.

Noter que, si α n'est pas constant, on a $\delta(\alpha) > 0$, et le théorème ci-dessus montre que « peu » de points rationnels appartiennent à $V(\alpha)$.

On peut se demander si la majoration ainsi obtenue est optimale, sous l'hypothèse $V(\alpha) \neq \emptyset$. Autrement dit :

(8.3) *Est-il vrai que* $N_\alpha(H) >> H^2/(\log H)^{\delta(\alpha)}$ *pour* H *assez grand, si* $V(\alpha) \neq \emptyset$?

Remarque

Il y a des énoncés analogues pour les corps de nombres, et pour les systèmes d'équations $\alpha_i(x) = 0$; on doit alors remplacer $e_x(\alpha)$ par l'ordre du groupe engendré par les $r_x(\alpha_i)$.

PUBLICATIONS

J.-P. SERRE, *Motifs*, Astérisque 198-199-200 (1991), 333-349.

— , *Lettre à M. Tsfasman*, Astérisque 198-199-200 (1991), 351-353.

— , *Topics in Galois Theory* (notes written by Henri Darmon), Jones and Bartlett Publ., Boston, 1992, 117 p.

— , *Lie Algebras and Lie Groups* (1964 Lectures given at Harvard University), 2e édition, Lect. Notes in Math. 1500, Springer-Verlag, 1992, 168 p.

MISSIONS

Exposés

— *Historical introduction to motives,* Seattle, juillet 1991.

— *The motivic Galois group,* Seattle, juillet 1991.

— *ℓ-adic representations associated to abelian varieties,* Seattle, août 1991.

— *Asymptotic properties of eigenvalues of graphs and Hecke operators,* Oxford, septembre 1991.

— *Le crible et les coniques*, Besançon, octobre 1991.

— *Problems in Galois cohomology*, Ascona, novembre 1991.

— *La forme trace en rang 6 ou 7*, Ascona, novembre 1991.

— *Revêtements de courbes algébriques*, séminaire Bourbaki, novembre 1991.

— *Une application de l'hypothèse* (H) *de Schinzel*, Bordeaux, février 1992.

— *Cohomologie galoisienne : éléments génériques, d'après Grothendieck* (2 exposés), séminaire de la chaire de Théorie des Groupes, Collège de France, mars 1992.

— *Nombres premiers, groupes de Galois, etc,* Genève, avril 1992.

— *Rademacher lectures* (3 exposés), Philadelphie, mai 1992.

— *Galois cohomology of* $k(t)$, Philadelphie, mai 1992 ; Sundance, mai 1992.

— *Negligible cohomology classes,* Sundance, mai 1992.

Table des Matières

—

Serre 7 oct. 199

Problèmes de coh. gal. liés aux corps de fonctions, surtout $\mathbb{Q}(T)$. Le plus souvent mod 2, quelques fois mod 3.

Plan du cours :

$\mathbb{Q}(T)$: corps des fct rat. sur $\mathbb{P}_1$.

On regarde les singularités des classes de cohomologie considérées, et on y attache des résidus.

Ceci a été fait pour la première fois par Fadeev ~ 1951 : il l'a fait pour le groupe de Brauer.

Coh. gal résidus corps résiduel

Formes quadr. groupe de Witt

K-théorie

Bruhat-Tits (coh. gal pour groupes semi-simples)

Plus précisément :

On peut obtenir les résidus par la suite spectrale des extensions de groupes.

Soit G un groupe (profini), et soit N un sous-groupe invariant (fermé). Alors $\Gamma = G/N$ est aussi un groupe profini.

Soit C un G-module discret (G agit continûment)

$$H^p(\Gamma, H^q(N, C)) \Longrightarrow H^{\cdot}(G, C)$$

Action de Γ sur $H^q(N,C)$. On fait l'hypothèse

(a) $H^q(N,C) = 0$, $q \geq 2$

(bouquet de cercles).

$$H^p(\Gamma, H^0(N, C))$$

$$H^p(\Gamma, H^1(N, C))$$

Hypothèse supplémentaire sur C:

(b) N opère trivialement sur C. Alors

$$H^p(\Gamma, H^0(N,C)) = H^p(\Gamma, C)$$

$$H^p(\Gamma, H^1(N,C)) = H^p(\Gamma, \mathrm{Hom}(N,C))$$

La suite spectrale dégénère en une suite

$$H^p(\Gamma, C) \to H^p(G, C) \xrightarrow{r} H^{p-1}(\Gamma, \mathrm{Hom}(N, C))$$
$$\to H^{p+1}(\Gamma, C) \to \cdots$$

Nous ferons l'hypothèse supplémentaire :

(c) L'extension de Γ par N est scindée,

i.e. G est un produit semi-direct

$$G \simeq N \cdot \Gamma$$

On obtient la suite exacte :

$$0 \to H^p(\Gamma, C) \to H^p(G, C) \xrightarrow{r} H^{p-1}(\Gamma, \mathrm{Hom}(N, C)) \to 0$$

On veut expliciter r. Pas facile, mais indispensable !

On donnera un procédé de calcul en termes de cochaînes.

On applique ceci à la cohomologie galoisienne d'un corps local.

K corps muni d'une valuation discrète, complet.

A_K entiers, π uniformisante.

$k = A/\pi$ corps résiduel.

Nous supposons ici (mais pas dans le cours) que k est *parfait*.

Soit K_s une clôture séparable de K,

$G_K = \mathrm{Gal}(K_s/K)$.

Val. s'étend de façon unique à K_s. Soit

$\bar{k}$ le corps résiduel de K_s, et

$\Gamma = G_k = \mathrm{Gal}(\bar{k}/k)$.

La théorie élémentaire ~~des~~ des corps locaux

nous dit que

$$1 \longrightarrow \underset{\substack{\shortparallel \\ \text{inertie}}}{I} \longrightarrow G_K \longrightarrow \Gamma \to 1$$

~~[illegible]~~

(1) Si car $k = 0$, alors I est isomorphe

à $\varprojlim \mu_n$, μ_n = racines $n$ièmes de 1 dans $\bar{k}$.

L'isomorphisme

$I \xrightarrow{\sim} \varprojlim \mu_n$ est canonique.

$(s\pi_{K'} = \pi_{K'} \cdot \zeta_s)$

(2) ~~[illegible]~~ Si car $k = p > 0$, on a

$$1 \to I_1 \longrightarrow I \to \varprojlim_{(n,p)=1} \mu_n \to 1$$

I_1 = groupe d'inertie sauvage

pro p-groupe. (plus gd pro-p-groupe contenu dans I)

$cd\, I = 1$, autrement dit on a

$$H^q(I, C) = 0 \quad \text{si } q \geq 2,$$

et si C est un I-module de torsion.

La suite exacte $1 \to I \to G_k \to \Gamma$ est scindée.

(si k est fini, $\Gamma = \hat{\mathbb{Z}}$ donc c'est évident !)

Si C est un Γ-module, de torsion

on a une suite exacte :

$$0 \to \underset{\substack{\| \\ H^p(k, C)}}{H^p(\Gamma, C)} \to \underset{\substack{\| \\ H^p(K, C)}}{H^p(G_k, C)} \to H^{p-1}(\Gamma, \mathrm{Hom}(I, C)) \to$$

On trouve cette suite exacte dans Witt (du moins pour le H^2).

<u>Hypothèse</u> : $n C = 0$, pour un n premier à la caractéristique résiduelle.

Alors $\mathrm{Hom}(I, C) = \mathrm{Hom}(\mu_n, C) = C(-1)$

$$\| \qquad\qquad$$
$$C \otimes_{\mathbb{Z}/n\mathbb{Z}} \mu_n^{\otimes(-1)}$$

" dual de μ_n.

La suite exacte prend la forme suivante :

$$0 \to H^p(k, C) \to H^p(K, C) \xrightarrow{r} H^{p-1}(k, C(-1)) \to 0$$

r : résidu.

$r(\alpha) = 0 \iff \alpha$ "provient du corps résiduel"

(α est holomorphe)

En termes de cohomologie étale :

Spec A consiste en 2 points Spec k, Spec K

C est vu comme un faisceau sur Spec A.

Foncteur dérivé nous donne ceci.

(on ne sait pas si l'on obtient r ou $-r$).

La flèche de résidu :

Cas $C = \mathbb{Z}/2\mathbb{Z}$, $p = 2$

Alors la suite exacte ci-dessus devient :

$$0 \to {}_2\mathrm{Br}\, k \to \mathrm{Br}_2 K \to H^1(k, \mathbb{Z}/2\mathbb{Z}) \to 0$$

$$\| $$

$$k^*/k^{*2}$$

On peut facilement donner des formules explicites pour r dans ce cas.

Par le thm de Merkurjev, tout élé de $Br_2 K$ est somme de symboles.

$(x,y) \qquad x, y \in K^*$

$r : (x,y) \mapsto 1$ si x, y unités $(v(x)=v(y)=0)$

$(\pi, x) \mapsto$ classe de $\tilde{x}$ dans k^*/k^{*2} $\qquad x$ unité

où $\tilde{x}$ est l'image ~~[illegible]~~ de x dans k

$r((\pi,\pi)) = r((\pi,-1))$

On peut donc calculer tous les résidus.

~~Corps de fonctions.~~

L'hypothèse "K complet" a servi. Mais :

La flèche résidu.

$$\begin{tikzcd}
H^p(K,C) \arrow[r] \arrow[dr] & H^{p-1}(k, C(-1)) \\
& H^p(\hat{K}, C) \arrow[u]
\end{tikzcd}$$

est définie même si K n'est pas complet.

k corps parfait.

Soit X une courbe algébrique projective et lisse sur k.

Les points fermés de X correspondent aux valuations discrètes de K triviales sur k.

$v \mapsto$ corps résiduel $k(v) =$ corps de fct. rat du point corr.

$\Gamma = Gal(\bar{k}/k)$

C = Γ-module annulé par n, $(n, car(k)) = 1$ si $car(k)$ est premier

On s'intéresse à la cohomologie galoisienne de $K = k(X)$ = corps des fonctions de X.

Si $\alpha \in H^p(K, C)$, et si v est un point fermé de X identifié à une valuation, alors $r_v(\alpha) \in H^{p-1}(k(v), C(-1))$.

On dira que α a un pôle en v si $r_v(\alpha) \neq 0$.

α n'a qu'un nombre fini de pôles.

(Supposons que C est de type fini. à clarifier plus tard).

Formule des résidus:

$$\sum_v Cor_k^{k(v)} r_v(\alpha) = 0$$

Si k'/k est ext. finie, on a une application de corestriction

$$\mathrm{Cor}_k^{k'} : H^p(k', \underset{\Gamma_k}{\text{module sw}}) \to H^p(k, \text{m module})$$

Pour aller plus loin, on est obligés de faire des hypothèses plus restrictives. Pour le résumé, nous supposerons :

<u>Hypothèse</u> $X \simeq \mathbb{P}_1$ $\begin{cases} g=0 \\ \text{a un point rationnel} \end{cases}$

$$H^p(k, C) \longrightarrow H^p(K, C) .$$

s'il existe un point rationnel, cette flèche est injective.

<u>Théorème</u> (Faddeev, Arason pour $C \cong \mathbb{Z}/2\mathbb{Z}, \dots$)

$$\begin{array}{l} 0 \to H^q(k, C) \to H^q(K, C) \to \bigoplus_v H^{q-1}(k(v), C(-1)) \\ \qquad\qquad\qquad\qquad\qquad\qquad \downarrow \oplus \mathrm{Cor} \\ \qquad\qquad\qquad\qquad\qquad\qquad H^{q-1}(k, C(-1)) \\ \qquad\qquad\qquad\qquad\qquad\qquad \downarrow \\ \qquad\qquad\qquad\qquad\qquad\qquad 0 \end{array}$$

D'un point de vue concret, ceci signifie :

Si $\alpha \in H^q(K, C)$, et si tous les résidus de α sont 0, alors α est constant :

$\alpha \in H^q(k, C)$

On peut évaluer les classes de cohomologie en les points.

Si $\alpha \in H^q(K, C)$ n'a pas de pôle en v, on peut définir :

$$\alpha(v) \in H^q(k(v), C).$$

Ces valeurs sont constantes si $\alpha \in H^q(k, C)$.

Dans l'exemple du groupe de Brauer : on a une alg. d'Azumaya sur X.

On s'intéressera au quotient : élé de rés. 0 modulo $H^q(k, C)$.

Est-ce que ce quotient est isomorphe à $Ext^q(J, C)$ (C fini)

$q = 1$ action triviale de C

$H^1(K, C)$ classifie les C-alg. gal. sur K (ext. ~~gal~~ de K)

Théorie de Rosenlicht donne : $H^1(J, C)$.

11

Cas particulier :

H^2, $C = \mathbb{Z}/2\mathbb{Z}$, k parfait car $k \neq 2$

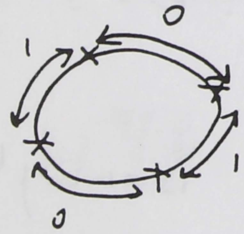
$K = k(T)$ = corps de fonctions de $\mathbb{P}_1$.

$$0 \to Br_2\, k \to Br_2\, K \xrightarrow{r} \bigoplus_v k(v)^*/k(v)^{*2} \xrightarrow{\prod N_k^{k(v)}} k^*/k^{*2} \to 1$$

Exemple : $k = \mathbb{R}$

v complexe : résidu $= 0$

v réel : à valeurs dans $\mathbb{Z}/2\mathbb{Z}$.



$\mathbb{P}_1(\mathbb{R})$

nombre pair de pôles

$Br_2\, \mathbb{R} = \mathbb{Z}/2\mathbb{Z}$

$\alpha \in Br_2\, K$, on peut prendre sa valeur sur l'intervalle $\leftrightarrow$. Par continuité, cette valeur est constante. La valeur change lorsqu'on passe un pôle.

Motivations.

1 Problèmes de Mestre (sur $\mathbb{Q}(T)$). 12

Montrer que certaines classes de cohomologie (d'obstruction) sont nulles.

Th (Mestre) : Toute extension centrale du groupe alterné A_n est groupe de Galois d'une extension régulière de $\mathbb{Q}(T)$.

Corollaire : Un tel groupe est groupe de Galois sur $\mathbb{Q}$.

$n \geq 5$ Schur a montré qu'il existe une ext. centrale universelle. Pour $n \neq 6, 7$, c'est $\tilde{A} = 2.A_n$

$$1 \to C_2 \to \tilde{A}_n \to A_n \to 1$$

Pour $n = 6, 7$

$$1 \to C_6 \to 6.A_n \to A_n \to 1$$

Première étape :

$$\begin{tikzcd} E \arrow[d, dash, "A_n"] \\ \mathbb{Q}(T) \end{tikzcd}$$

que l'on aimerait plonger dans ext. gal.

$$\begin{tikzcd} \tilde{E} \arrow[d, dash, "C"] \arrow[dd, dash, bend right] \\ E \arrow[d, dash] \\ \mathbb{Q}(T) \end{tikzcd} \qquad C = C_2,\ C_6$$

1: Construire une telle extension revient à

$$\begin{tikzcd} & A_n^{univ} = C \cdot A_n \arrow[d] \\ G_K \arrow[ur] \arrow[r, "suj"] & A_n \end{tikzcd}$$

le problème équivaut à la nullité d'une certaine classe de cohomologie dans

$H^2(K, C)$.

A démontrer : Si α est cette classe, que . $r_v(\alpha) = 0$ pour tout v

. puis l'évaluer en au moins un point v, et montrer que $\alpha(v) = 0$.

Il y a d'autres problèmes où la situation est moins simple :

2) Mestre $SL_2(\mathbb{F}_7)$

Groupe de Galois d'une extension régulière de $\mathbb{Q}(T)$.

Exemples connus à groupe de Galois $PSL_2(\mathbb{F}_7)$ (d'ordre 168)

Problème : ~~à~~ classe de cohomologie $\alpha \in H^2(K, C_2)$.

Mais $\alpha \neq 0$!

On voudrait changer de variable.

Question (conjecture):

$\mathbb{P}_1(k)$, car $k \neq 2$, k parfait

$$\alpha \in H^2(k(\mathbb{P}_1), C_2) = Br_2(k(\mathbb{P}_1)).$$

On suppose que $\alpha(v)=0$ pour une place de degré 1 ($k(v)=k$) de $k(\mathbb{P}_1)$.

$\alpha(v)=0$.

Alors, il existe (?) un morphisme

$\mathbb{P}_1 \xrightarrow{f} \mathbb{P}_1$ non constant, tel que:

(a) $f^*(\alpha)=0$

(b) il existe un point rationnel w de $\mathbb{P}_1$ tel que $f(w)=v$

On peut demander un peu plus:

que f soit disjoint de toute extension finie donnée.

Si l'on ne demandait pas $\mathcal{B}_1$, ce serait trivial:

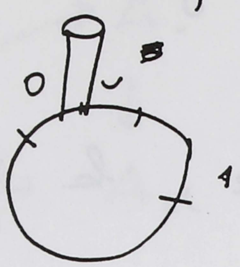
$\alpha \in H^2(K, C_2)$ est tué par une extension

15

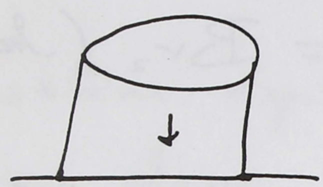
Résultats partiels:

C'est vrai pour un corps local.

$\mathbb{R}$:



on peut demander que l'image soit petite, tombe dans l'intervalle $\underset{0}{\sqcup}$.



Th (Meste) : Conjecture est vraie pour α si

$$\sum \deg(\text{pôles de } \alpha) \leq 4$$

Dans le problème sur $SL_2(\mathbb{F}_7)$, la condition sur les pôles est satisfaite.

$$\begin{array}{ccc} E' & & E \\ PSL_2(\mathbb{F}_7) \Big| & & \Big| \; PGL_2(\mathbb{F}_7) \\ K' = k(T') & \text{—} & K = k(T) \end{array}$$

(extensions disjointes)

$\uparrow$ l'obstruction est nulle.

Ce type de problème est apparu dans la théorie des surfaces rationnelles fibrées en coniques.

2 Surfaces rationnelle fibrées en coniques

$\bar{k}$-rationnelles

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

fibre générique : conique
(courbe de genre 0)

fibre exceptionnelle : 

$K = k(\mathbb{P}_1)$ $\qquad S \to \alpha(S) \in H^2(K, C_2)$
$\qquad\qquad\qquad\qquad\qquad\qquad \| $
$\qquad\qquad\qquad\qquad\qquad\qquad Br_2 K$

Quitte à modifier la surface, on peut supposer que pôles $\longleftrightarrow$ fibres exceptionnelles.

Deux droites ne sont pas rat.
résidu correspond à l'ext. quadr.
"sur laquelle les 2 droites se séparent".

On s'intéresse aux points rationnels de $\mathbb{P}_1$ en lesquels $\alpha = 0$ (i.e. projections des points rationnels de S, non situés sur fibres exceptionnels)

Conjecture :

Si S a un point rationnel non sur une mauvaise fibre, S est k-unirationnel.

Autrement dit, il existe une application rationnelle surjective $\mathbb{P}_2 \xrightarrow{f} S$

(et on peut exiger que $P \in$ image de $\mathbb{P}_2(k)$)

La Conjecture précédente entraîne celle-ci.

$\alpha \in Br_2 k$ correspond à S

$\alpha(P) = 0$ pour un certain P

$$\begin{tikzcd} S_1 \arrow[r] \arrow[d] & S \arrow[d] \\ \mathbb{P}_1 \arrow[r, "Q"] & P \in \mathbb{P}_1 \end{tikzcd}$$

S_1 a invariant 0.

Donc S_1 est birationnellement $\mathbb{P}_1 \times \mathbb{P}_1 \simeq \mathbb{P}_2$

Donc S_1 est k-rationnelle

S est unirationnelle.

En fait, les deux conjectures sont équivalentes.

(mettre une droite de travers ds $\mathbb{P}_2$)

$\alpha \in Br_2$ $\quad \alpha = (x, y)_2$ décomposables

$\rightarrow$ fibré en coniques.

Exercice :

Soit k un corps pour lequel la conjecture d'annulation dans $\alpha \in Br_2(k(T))$ est valable.

Alors on montre que tout 2-groupe est groupe de Galois d'une extension régulière de $k(T)$.

Autre conséquences

$\alpha \in Br_2\, k(T)$, k infini, car$(k) \neq 2$.

Supposons $\alpha(v) = 0$ pour une place v de $d^{\circ}1$.

$v \in \mathbb{P}_1(k)$

<u>Conjecture</u> : • Il existe une infinité de tels v

• Il existe un autre tel v.

même sur $\mathbb{Q}$, ceci n'est pas connu.

(3) Problème de Manin : <u>Estimer le nombre des v avec $\alpha(v)=0$</u>.

$\mathbb{P}_1$, $v \in \mathbb{P}_1(\mathbb{Q})$ $(k = \mathbb{Q})$

$\alpha \in Br_2\, \mathbb{Q}(T)$.

On s'intéresse à l'ensemble des v tels que $\alpha(v) = 0$. Manin voudrait une borne supérieure pour $\#\{ v \mid \alpha(v)=0 \}, H(v) < N\}$.

$v = \frac{p}{q}$ p, q premiers entre eux > 0

$$H(v) = \operatorname{Sup}(p, q)$$

Théorème

Nombre des v, $\alpha(v)=0$, $H(v)\le N$ est

$$\ll O\left(N^2/\log N\right)^{d/2})$$

où d est le nombre de pôles de α.

Problème:

Est-ce que c'est le bon ordre de grandeur?

Supposons que $\alpha(v)=0$ pour un v.

Est-ce que $\gg$?

Calculs de Coray et de Meste.

Variantes: • Prendre $\mathbb{P}_n$ au lieu de $\mathbb{P}_1$.

• Prendre Aff^n.

Exemple: Aff^1 T

$\alpha=(-1,T)$ $T\to t\in\mathbb{Z}$

$(-1,t)=0$ $\iff$ t est somme de 2 carrés

Estimer le nombre de t sommes de 2 carrés, $t\le N$. Conjecture donc: $\ll \frac{N}{\log N}$

Landau: $\sim c\cdot\frac{N}{\ldots}$

Manin:

$$aX^2+bY^2+cZ^2=0$$

a, b, c entiers premiers entre eux.

Estimer le nombre des $|(a,b,c)| \leq N$ tels que la conique ait un point rationnel.

Résultat partiel: $\ll N^3/(\log N)^{3/2}$

$\alpha = (-ab, -ac)$.

$N^3/(\log N)^3 \ll$

Serre (21) 14/10/91

Définir notion de résidu:

(1) Cohomologie des extensions de groupes.

G groupe profini:

N s/g invariant (fermé) de G

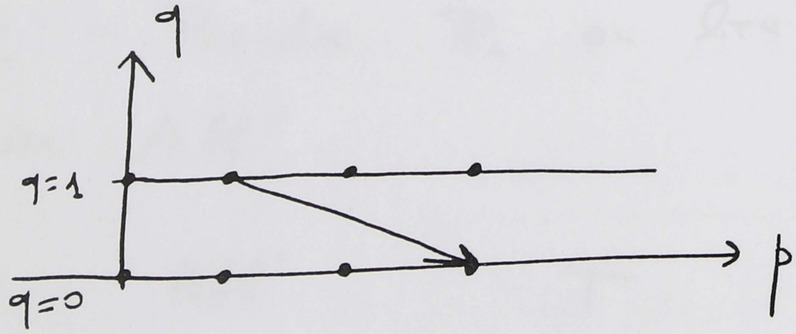
$\Gamma = G/N$.

C est un | Γ-module discret
| G-module discret où l'action de N est triviale.

Suite spectrale

$$H^p(\Gamma, H^q(N,C)) \Rightarrow H^*(G,C).$$

Hypothèse (1) $H^q(N,C)=0$ pour $q \geq 2$.



seule diff. non nul est d_2

$$p,1 \longrightarrow p+2,0$$

$$\cdots \to H^n(\Gamma, C) \longrightarrow H^n(G,C) \xrightarrow{r} H^{n-1}(\Gamma, \mathrm{Hom}(N, C$$

$$\xrightarrow{d_2} H^{n+1}(\Gamma, C) \longrightarrow \cdots$$

Identifier les flèches :

On ne parlera pas de d_2, car ce sera 0 dans les cas qui nous intéressent.

Par contre, r sera l'homomorphisme résidu — nous avons besoin de l'expliciter.

Construction de Hochschild :

Filtration des cochaînes sur G, à valeurs ds C (en fait, de "cochaînes normalisées")

$f(g_1, \dots, g_n)$ à valeurs ds C

normalisée si : $f = 0$ chaque fois que l'un des g_i est l'élément neutre.

Le $k^{\text{ième}}$ cran de la filtration est :

$f(g_1, \dots, g_n)$ ne dépend que des images de $g_{n-k+1}, \dots, g_n$ dans Γ.

(i.e. $f(g_1, \dots, g_{n-k}, g_{n-k+1}\nu_1, \dots, g_n \nu_k)$

$$= f(g_1, \dots, g_n)$$

pour $\nu_i \in N$.

Il résulte de cette construction (sous l'hypothèse 1) que tout n-cocycle f sur G ~~est cohomologue~~ à val. ds C

est cohomologue à un cocycle f tel que f normalisé, et $f(g_1, g_2, \dots, g_n)$ ne

(*)| dépend que des classes de $g_2, \dots, g_n$ mod N

Description de r.

Si α est la classe de f dans $H^n(G, C)$, ~~contient~~ $r(\alpha)$ contient le $(n-1)$-cocycle $r(f)$ défini par :

$$r(f)(\gamma_1, \dots, \gamma_{n-1})(\nu) = f(\nu, g_1, \dots, g_{n-1})$$

$\gamma_i \in \Gamma \qquad \nu \in N$

où les g_i sont des éléments des γ_i dans G.

Cas particuliers :

$n = 1$ $\quad H^1(G, C) \longrightarrow H^0(\Gamma, \mathrm{Hom}(N, C))$

homomorphisme croisé $G \to C$ | restr. à N $\to$ homomorphi[smes] $N \to C$ invariant par Γ

"Flèche de restriction"

$n = 2$. $\alpha \in H^2(G, C)$. On représente α par une extension E_α :

$$
\begin{tikzcd}
 & 1 \arrow[d] \\
1 \arrow[d] & C \arrow[d] \\
C \arrow[d, leftrightarrow] & E_\alpha \arrow[d] \\
E_{\alpha,N} & G \arrow[d] \\
N \arrow[u, "\varphi"] \arrow[r, phantom, "\subset"] & 1
\end{tikzcd}
$$

La restriction de α à N est 0

On a un élément de N à E_α.

Les éléments possibles forment un espace principal homogènes sous $\mathrm{Hom}(N, C)$.

Il y a une action de $\Gamma = G/N$ sur cet espace principal homogène.

On a un Γ-groupe $\mathrm{Hom}(N, C)$

P un Γ-principal homogène sous $\mathrm{Hom}(N,$

$$\downarrow$$

$$\mathrm{inv} \in H^1(\Gamma, \mathrm{Hom}(N, C)).$$

<u>Théorème</u> : Cet invariant est $-r(\alpha)$.

On choisit un élément $N \subset E_\alpha$.

Soit Σ un représentant de $G/N = \Gamma$

[illegible]

Σ_α relèvement de Σ dans E_α

$N\cdot\Sigma_\alpha$ est un relèvement de G ds E_α.

(ou $\Sigma_\alpha\cdot N$)

Multiplicativité de r p.r. au cup-produit

$C_1\times C_2\to C$ $\quad$ Γ-modules

$H^{n}(\overset{N}{~~}, C_1) = 0$, $n\geq 2$

$\alpha_1\in H^{n_1}(G, C_1)$, $\alpha_2\in H^{n_2}(\Gamma, C_2)$,

d'où par inflaton

$p: G\to\Gamma$ $\qquad p^*(\alpha)$

$\alpha=\alpha_1\cdot\alpha_2\in H^n(G, C)$, $\quad n=n_1+n_2$

Alors on a $\quad r(\alpha)=r(\alpha_1).\alpha_2$ dans

$H^{n_1+n_2-1}(\Gamma, \mathrm{Hom}(N, C))$.

$\mathrm{Hom}(N, C_1)\times C_2\longrightarrow\mathrm{Hom}(N, C$

Formule pour définir le cup-produit:

φ, ψ $\quad$ n_1, n_2-cocycles

$(\varphi.\psi)(g_1,\dots,g_{n_1}, g_{n_1+1},\dots,g_{n_1+n_2})$

$=\varphi(g_1,\dots,g_{n_1})\,{}^{g_1\cdots g_{n_1}}\psi(g_{n_1+1},\dots,g_{n_1+n_2})$

Hypothèse ② L'extension

$$1 \to N \to G \to \Gamma \to 1$$

est scindée :

autrement dit, $G \simeq$ produit semi-direct $N \cdot \Gamma$.

D'où $H^n(\Gamma, C) \to H^n(G, C)$ est injective (car même facteur direct).

D'où

$$0 \to H^n(\Gamma, C) \to H^n(G, C) \xrightarrow{r} H^{n-1}(\Gamma, \mathrm{Hom}(N, C)) \to 0$$

Ces suites exactes sont scindées, mais pas canoniquement.

<u>Deuxième étape</u> : Application aux corps locaux.

K corps complet pour une valuation discrète v, A l'anneau des entiers (π une uniformisante — $v(\pi) = 1$)

$k = A/\pi A$ corps résiduel

$G_K = \mathrm{Gal}(K_s/K)$, K_s clôture séparable

G_k

Structure de G_K

$$1 \to I \to G_K \to G_k \to 1$$

I = groupe d'inertie.

$$1 \to I_1 \to I \to I^{mod} \to 1$$

où I_1 est un pro-p-groupe

I^{mod} est isom (pas canoniquement) à

$$\prod_{\ell \neq p(k)} \mathbb{Z}_\ell$$

$p(k)$: "exposant caract. de k" ($= 1$ si car $= 0$)

Isom. canonique $I^{mod} = \varprojlim_{(n, p(k)) = 1} \mu_n$.

Soit L/K une extension finie galoisienne.

A_L, k_L — entiers, corps résiduel.

$$G \to \mathrm{Gal}(k_L/k)$$

k_L extension normale de k (pas néc. séparable (ext. gal. d'une ext. radicielle)

$G \to \mathrm{Gal}(k_L/k)$ surjectif,

noyau I_G : groupe d'inertie.

m_K : idéal maximal de A_K

m_L ——— de A_L

Action de I_G sur m_L/m_L^2, espace vectoriel de dim 1 sur k_L

$I_1 \to I_G \longrightarrow k_L^*$, image μ_n (racines de 1)

noyau

On montre que I_1 est un <u>p-groupe</u>.

<u>Normalisation</u> de l'isomorphisme $I^{mod} \simeq \varprojlim \mu_n$.

k_s : clôture séparable de k.

Si $k \subset k' \subset k_s$ fini sur k

$\longmapsto K'/K$ non ramifiée, d'ext. rés. k'/k.

D'où $K_{nr} = \bigcup K'$ (pas néc. complet)

on prend $\hat{K}_{nr}$.

$\mathrm{Gal}(\hat{K}_{nr}/K) \simeq \mathrm{Gal}(k_s/k) = G_k$.

$$\begin{array}{l} K_s \\ | \\ K_{nr} \\ |\ G_k \\ K \end{array} \qquad I = \mathrm{Gal}(K_s/K_{nr}) = \mathrm{Gal}(\hat{K}_s/\hat{K}_{nr}).$$

Si $(n, p(k)) = 1$, on définit une extension $K_{nr,n} = K_{nr}(\sqrt[n]{\pi})$

indépendante du choix de π

$Gal(K_{nr,n}/K_{nr}) \simeq \mu_n(k_s)$ Posons $\pi_n = \sqrt[n]{\pi}$

$s \in Gal$ $\quad s(\pi_n)/\pi \longrightarrow$ ds corps résiduel

$$\mu_n(k_s) = \mu_n(K_s)$$

$$\begin{array}{ccc} K_s & & \bar{k} \\ | & & | \\ K_{mod} & & k_s \\ | & & L \\ K_{nr} & & k_s \\ | \; G_k & & | \\ K & & k \end{array}$$

$$I/I_1 = Gal(K_{mod}/K_{nr}) \simeq \varprojlim \mu_n$$

$$= \prod_{\ell \neq p(k)} \mathbb{Z}_\ell(-1)$$

I_1 pro-p-groupe.

Théorème :

L'extension $1 \to I \to G_k \to G_{\bar{k}} \to 1$ est scindée

1ère étape : On peut élever mod I_1.

L'extension

$$1 \longrightarrow I^{mod} \longrightarrow G_k/I_1 \to G_{\bar{k}} \to 1$$

est scindée

"Non-démonstration" (convaincante).

$? \in H^2(G_{\bar{k}}, \varprojlim \mu_n)$. Ds $H^2(G_{\bar{k}}, \mu_n) \ni \gamma_n$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\parallel$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad Br_n(\bar{k})$

Prouver par propr. de fonctorialité que obst. $= 0$

non-démonstration $\to$ démonstration.

Démonstration (difficile)

$$K_{nr} \qquad\qquad K_{nr}(\pi^{1/n})$$

Pour tout n, premier à $p(\bar{k})$, on choisit $\pi_n \in K^{mod}$, avec $\pi_n^n = \pi$ de façon cohérente. $\pi_{nm}^m = \pi_n \qquad n, m$

$K(\pi_n)$ est linéairement disjoint de K_{nr}/K, $\quad K(\pi_n) K_{nr} = K_{nr}(\pi^{1/n})$

$\mu_n \to Gal(K_{nr}(\pi^{1/n})/K) \longrightarrow G_{\bar{k}} \to 1$

<u>Scindage</u> : le s/g $\mathrm{Gal}(K_{nr}(\pi^{1/n})/K(\pi_n))$ donne un relèvement de G_k.

Par passage à la limite sur n, on a le relèvement.

Idée :

$$\begin{tikzcd} & C \arrow[d, dash] \\ & B \arrow[d, dash] \\ D \arrow[r, dash] & A \end{tikzcd} \qquad C = D \otimes B.$$

Ext. scindée : le s/g correspondant étant formé des st G_K/I_1 qui fixent tous les π_n.

<u>Proposition</u> : Toute extension de G_k par un pro-p-groupe est scindée.

<u>Théorème</u> : Si k est de car. $p > 0$, on a $cd_p(G_k) \leq 1$.

Suffit de voir (pour k et toutes ses ext.) que $H^i(G_k, \mathbb{Z}/p\mathbb{Z}) = 0$.
En fait, il suffit de le voir que c'est vrai pour $i = 2$ (dévissage).

$$0 \to \mathbb{Z}/p\mathbb{Z} \to k_s \xrightarrow{\wp} k_s \to 0$$

$$\wp(x) = x^p - x.$$

$H^i(G_k, k_s) = 0$ pour tout $i \geq 1$

d'où l'affirmation.

Par "Cohomologie Galoisienne" (~ I-74) le thm entraîne la proposition.

Il ne faut pas prendre ce thm au sérieux — les ext. radicielles donnent des choses non triviales. Par ex. $Br_p(k)$ peut être $\neq 0$

$$1 \to N \to G \to \Gamma \to 1$$

$$1 \to I \to G_K \to G_k \to 1.$$

Théorème:

(a) $cd_\ell I = 1$ si $\ell \neq p$

(b) $cd_p I = 1$ si $\operatorname{car} K = p$

ou si $\operatorname{car} K = 0$ et k parfait

≥ 2 si $\operatorname{car} K = 0$ et k imparfait

Corollaire :

Si k est parfait, $cd_\ell\, I = 1$ pour tout ℓ premier.

Démonstration :

a) Le ℓ-groupe de Sylow de I est isomorphe à $\mathbb{Z}_\ell$, d'où $cd_\ell = 1$.

b) Si $\operatorname{car} K = p$, $I = \operatorname{Gal}(K_s/\underline{\underline{K_{nr}}})$ car p

on a $cd_p\, I \leq 1$,

d'où $= 1$ car $I_1 \neq \{1\}$.

b') Si $\operatorname{car} K = 0$, k parfait.

Quitte à remplacer K par $\widehat{K_{nr}}$,

on peut supposer k alg. clos.

Théorème (Lang ?) :

Si K est complet pour une valuation discrète à corps résiduel algébriquement clos, alors K est C_1

(i.e. toute équation homogène à coeff. ds K de degré < nombre de variables a une solution non triviale)

$\Longrightarrow cd(G_K) \leq 1$.

b'' On peut supposer k séparablement clos, et que K contient μ_p.

Soit π une uniformisante de K. Soit $u \in A_K^*$ une unité telle que $\tilde{u} \in k^*$ ne soit pas une puissance p-ème.

Soit z une racine primitive p-ème de 1.

Soit $(\pi, u) \in Br_p(K)$.

Alors, on démontre que $(\pi, u) \neq 0$.

$Br_p(K) \neq 0 \Rightarrow cd_p(G_K) \geq 2$

Cas considéré par la suite:

C est un Γ-module (où $\Gamma = G_k$) annulé par n, avec $(n, p(k)) = 1$.

(voir Kato)

On définit $C(-1) = Hom(\mu_n, C)$.

$\mu_n = \mu_n(k_s)$

<u>Théorème:</u> $0 \to H^m(G_k, C) \to H^m(G_K, C) \to$

$\to H^{m-1}(G_k, C(-1)) \to 0$.

Scindage de l'extension

$H^i(I, C) = 0$, $i \geq 2$ $\quad cd_\ell I \leq 1$.

$$C(-1) = \mathrm{Hom}(I, C) = \mathrm{Hom}(I/I_1, C) = \mathrm{Hom}(\mu_n, C).$$

<u>Remarque:</u> r peut être défini même si

K n'est pas complet.

K muni de v, $k(v)$ = corps résiduel

C un G_K-module, annulé par n

"non ramifié en v" (i.e. action triviale de l'inertie en v).

On a alors un homomorphisme

$$\begin{tikzcd} r : H^m(G_K, C) \arrow[rr, "r_v"] \arrow[dr] & & H^{m-1}(G_{k(v)}, C(-1)) \\ & H^m(G_{\hat{K}}, C) \arrow[ur, "r_{\hat{K}}"'] & \end{tikzcd}$$

En termes de topologie étale:

A anneau de val,

$T = \mathrm{Spec}\, A$ "trait"

point fermé $\mathrm{Spec}(k) = 1_k$

ouvert $\mathrm{Spec}(K) = 1_K$.

$j : 1_K \longrightarrow T$

On regarde C comme faisceau étale sur A.

Supposons A complet.

$$R^q j_* C = \begin{cases} C & q = 0 \\ C(-1) & q = 1 \quad \text{concentré au pt fermé } 1_k \\ 0 & q \geq 2 \end{cases}$$

Suite spectrale de Leray pour j :

$$H^p(T, R^q_{j_*} C) = \begin{cases} H^p(T, C) & q = 0 \\ H^p(1_k, C(-1)) & q = 1 \\ 0 & \text{sinon.} \end{cases}$$

Comme A est complet, $H^p(T, C) = H^p(1_k, C$

$$H^n(G_k, C) \to H^n(G_K, C) \xrightarrow{r} H^{n-1}(G_k, C(-1$$

Relier l'homomorphisme de résidu à une

décomposition du groupe de Brauer.

Cas particulier :

$m = 2$, $C = \mu_n$, $(n, p(k)) = 1$.

Supposons k parfait pour simplifier.

$$\mu_n(-1) = \mathrm{Hom}(\mu_n, \mu_n) = \mathbb{Z}/n\mathbb{Z}$$

$$r : H^2(G_k, \mu_n) \to H^1(G_k, \mathbb{Z}/n\mathbb{Z})$$

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

$$r : Br_n(K) \longrightarrow \mathrm{Hom}(G_k, \mathbb{Z}/n\mathbb{Z})$$

Calcul de $Br(K)$ par Witt.

Le groupe de Brauer est décomposé par K_{nr}. Autrement dit, il est égal à $H^2(G_k, K_{nr}^*)$.

On a une suite exacte

$$1 \longrightarrow \underset{\substack{\downarrow \\ \bar{k}^*}}{U_{nr}} \longrightarrow K_{nr}^* \xrightarrow{v} \mathbb{Z} \to 0$$

scindée (par le choix de π).

Donc suite exacte

$$0 \to H^2(U_{nr}) \longrightarrow Br(K) \to H^2(G_k, \mathbb{Z})$$

$$H^2(U_{nr}) \cong H^2(\bar{k}^*) = Br(k), \qquad H^2(G_k, \mathbb{Z}) = \mathrm{Hom}(G_k, \mathbb{Q}/\mathbb{Z})$$

Suite exacte de W.H. :

$(*)$ $0 \to Br(k) \to Br(K) \to Hom(G_k, \mathbb{Q}/\mathbb{Z}) \to 0$

$(*_n)$ $0 \to Br_n(k) \to Br_n(K) \xrightarrow{r_W} Hom(G_k, \mathbb{Z}/n\mathbb{Z}) \to 0$

<u>Proposition</u> : $r_W = -r$.

<u>Cas particulier</u> $n=2$ (et $r = r_W$).

$$r : Br_2(K) \longrightarrow \underbrace{Hom(G_k, \mathbb{Z}/2\mathbb{Z})}_{\parallel \; k^*/k^{*2}}$$

<u>Formule</u> pour r :

Il suffit de donner r pour des symboles (par Merkurjev) du type suivant :

(u, v) u, v unités

(u, π) u unité

(car $(\pi, \pi) = (\pi, -1)$).

$r(u, v) = 0$

$r(u, \pi)$ = classe de $\bar{u}$ dans k^*/k^{*2}

où $\bar{u}$ est l'image de u dans k.

<u>Résidu</u> pour la cohomologie d'un corps local

K corps local, k corps résiduel

G_k-module C, $nC = 0$, n premier à $p(k)$.

Suite exacte

$$0 \to H^m(G_k, C) \to H^m(G_K, C) \xrightarrow{r} H^{m-1}(G_k, C(-1)) \to$$

$$C(-1) = \mathrm{Hom}(\mu_n, C) = C \otimes (\mu_n)^\vee$$

$$0 \to H^m(k, C) \xrightarrow{i} H^m(K, C) \xrightarrow{r} H^{m-1}(k, C(-1)) \to 0$$

$$1 \to I \to G_K \to G_k \to 1$$

Suite exacte <u>scindée</u> (par le choix d'une uniformisante)

$$H^1(K, \mu_n) \simeq K^*/K^{*n}$$
$$\qquad\qquad\qquad\quad \Psi$$
$$(x) \longleftarrow x$$

π définit un élément $(\pi) \in H^1(K, \mu_n)$

Soit $\alpha \in H^{m-1}(k, C(-1))$. On a $i(\alpha) \in H^{m-1}(K, C(-1$

On a une flèche naturelle

$$\mu_n \otimes C(-1) \longrightarrow C$$

D'où $(\pi).\, i(\alpha) \in H^m(K, C)$.

L'application $\alpha \mapsto (\pi)\, i(\alpha)$ "relève r" :

$$r((\pi).\, i(\alpha)) = \alpha \;.$$

r pour $m=1$:
$$H^1(K,C) \to H^0(k, C(-1))$$

Prenons $C = \mu_n$.
$$H^1(K,\mu_n) \xrightarrow{r} \mathbb{Z}/n\mathbb{Z}$$

$\mu_n(-1) = \mathbb{Z}/n\mathbb{Z}$ (act. de Galois triviale)

$$\begin{array}{c} \wr\wr \\ K^*/K^{*n} \nearrow \end{array}$$

La flèche $K^*/K^{*n} \xrightarrow{r} \mathbb{Z}/n\mathbb{Z}$
est donnée par la valuation :
$$x \longmapsto v(x) \pmod n.$$

On a $r(\alpha_1 \, i^*(\alpha_2)) = r(\alpha_1)\cdot\alpha_2$
(formule de projection).

D'où $r((\pi)\cdot i(\alpha)) = 1\cdot\alpha = \alpha$.

Ceci donne une autre façon de voir r :
$$H^m(K,C) = H^m(k,C) \oplus (\pi)\cdot H^{m-1}(k, C(-1)).$$

<u>Application aux symboles galoisiens</u> dans
$$Br_n(K) = H^2(K,\mu_n).$$

Hypothèse : $\mu_n \subset K^*$, et on choisit un générateur de μ_n.

Si $x, y \in K^*$, on leur associe

$$(x,y)_n \in Br_n(K) = H^2(K, \cancel{\mathbb{Z}/n\mathbb{Z}}\ \mu_n)$$

$$\overset{\shortparallel}{(x)(y)}$$

$(x), (y) \in H^1(K, \mu_n)$. Donc

$$(x).(y) \in H^2(K, \mu_n^{\otimes 2}) \simeq H^2(K, \mu_n)$$

On a $\quad (x).(y) = -(y)(x)$.

$$Br_n(K) = Br_n(k) \oplus (\pi) H^1(k, \mathbb{Z}/n\mathbb{Z}).$$

$$\begin{aligned} &\quad\ \ \shortparallel\!\wr \\ &H^1(k, \mu_n) \\ &\quad\ \ \shortparallel\!\wr \\ &k^*/k^{*n}. \end{aligned}$$

Si u_1, u_2 sont des unités de K

$(u_1, u_2) \in Br_n(K)$, appartient à $Br_n(k)$.

$(u_1, u_2) = (\tilde{u}_1, \tilde{u}_2)$ où $\tilde{u}_i$ = image de u_i dans k^*

u unité de K

$(\pi, u) \in Br_n(K)$

$(\pi, u) = (\pi)(\bar{u}) \qquad \bar{u} \in H^1(k, \mathbb{Z}/2\mathbb{Z})$.

Autrement dit, $\quad r((\pi, u)) = \bar{u}$.

Ceci permet de calculer r pour tous les symboles.

$r((x,y)) = ?$ $\quad x, y \in K^*$

Il suffit de calculer ce résidu lorsque

$x = \pi$, $y = u$ $\qquad r = (\tilde{u})$

$x = u_1$, $y = u_2$ $\qquad r = 0$

$x = u$, $y = \pi$ $\qquad r = -(\tilde{u})$

$x = \pi$ $\quad y = \pi$ $\qquad r = (-1)$

$$(\pi, \pi) = (\pi, -1) + \underbrace{(\pi, -\pi)}_{=0}$$

(Cas particulier $n = 2$, $\mu_2 \simeq \mathbb{Z}/2\mathbb{Z}$)

Comparaison de la suite exacte avec celle de Witt.

Supposons k parfait.

Comparaison avec la <u>décomposition de Witt</u> du groupe de Brauer.

$$(\text{Witt}) \qquad 0 \to Br(k) \to Br(K) \xrightarrow{r_W} \operatorname{Hom}(G_k, \mathbb{Q}/\mathbb{Z}) \to 0.$$

K_{nr} extension non ramifiée maximale de K.

$$\begin{array}{l} K_{nr} \\ \mid G_k \\ K \end{array} \qquad Br(K) = H^2(G_k, K_{nr}^*).$$

$$1 \to U_{nr} \to K_{nr}^* \xrightarrow{v} \mathbb{Z} \to 0$$

Donc

$$0 \to H^2(G_k, U_{nr}) \to Br(K) \to H^2(G_k, \mathbb{Z}) \to 0$$

$$\cong \downarrow$$

$$Br(k) = H^2(G_k, \bar{k}^*)$$

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

$$\begin{array}{c} H^1(G_k, \mathbb{Q}/\mathbb{Z}) \\ \equiv \downarrow \delta \\ H^2(G_k, \mathbb{Z}) \end{array}$$

On obtient ainsi la suite exacte de Witt

~~Proposition : $r_w = -r$.~~

~~Soit $\chi \in \mathrm{Hom}(G_k, \mathbb{Q}/\mathbb{Z})$~~

n, premier à la car.

$$0 \to Br_n(k) \to Br_n(K) \xrightarrow{r_w} \mathrm{Hom}(G_k, \mathbb{Z}/n\mathbb{Z}) \to$$

Proposition : $r_w = -r$ pour tout n premier à $p(k)$

Soit $\chi \in \mathrm{Hom}(G_k, \mathbb{Z}/n\mathbb{Z})$.

$$\begin{array}{c} \cap \\ \mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z}). \end{array}$$

$$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$$

$$\delta_\chi \in H^2(G_K, \mathbb{Z}).$$

π uniformisante de K. On peut voir π comme

$$\pi \in H^0(K, \mathbb{G}_m).$$

$\pi \cdot \delta_\chi \in H^2(K, \mathbb{G}_m) = Br(K)$

$\pi \cdot \delta_\chi \in Br_n(K)$.

On a : $r_w(\pi \cdot \delta_\chi) = \chi$.

$\pi \cdot \delta_\chi \in H^2(K, \mu_n)$

$\parallel$ $\qquad \chi \in H^1(K, \mathbb{Z}/n\mathbb{Z})$

$\chi \cdot (\pi)$ $\qquad (\pi) \in H^1(K, \mu_n)$

$\parallel$ $\qquad \chi \cdot (\pi) \in H^2(K, \mu_n) = Br_n(k)$.

$-(\pi) \cdot \chi$

$r((\pi) \cdot \chi) = \chi$

D'où le signe $-$ dans la formule.

<u>Changement de corps</u> local

$K_1 \subset K_2$ deux corps, v_2, v_1 val. discrètes.

$v_2 | K_1^* = e \cdot v_1$ $\qquad e \in \mathbb{N}$, $e \geq 1$ indice de ramification.

$k_1 \subset k_2$ corps résiduels.

$G_{K_2} \longrightarrow G_{K_1}$ défini à conjugaison près.

$G_{k_2} \longrightarrow G_{k_1}$

(On ne suppose <u>pas</u> K_2 fini sur K_1).

C un G_{k_1}-module.

$$\begin{tikzcd} H^m(K_1, C) \arrow[r, "r_1"] \arrow[d, "\mathrm{Res}"] & H^{m-1}(k_1, C(-1)) \arrow[d, "e \cdot \mathrm{Res}"] \\ H^m(K_2, C) \arrow[r, "r_2"] & H^{m-1}(k_2, C(-1)) \end{tikzcd}$$

diagramme commutatif.

<u>Proposition :</u> Ce diagramme est commutatif.

$$\begin{tikzcd} 1 \arrow[r] & N_1 \arrow[r] & G_1 \arrow[r] & \Gamma_1 \arrow[r] & 1 \\ 1 \arrow[r] & N_2 \arrow[r] \arrow[u] & G_2 \arrow[r] \arrow[u] & \Gamma_2 \arrow[r] \arrow[u] & 1 \end{tikzcd}$$

$$\begin{tikzcd} r : H^m(G_1, C) \arrow[r] \arrow[d] \arrow[dr, phantom, "\circlearrowright"] & H^{m-1}(\Gamma_1, \mathrm{Hom}(N_1, C)) \arrow[d] \\ {} \arrow[r] & {} \end{tikzcd}$$

On a fait l'identification

$$\mathrm{Hom}(I_1, C) \simeq C(-1)$$

$$\mathrm{Hom}(I_1^{mod}, C) = \mathrm{Hom}(I_{1,n}^{mod}, C)$$

$$I_{1,n}^{mod} \cong \mu_n$$

$$\begin{array}{ccc} I_{2,n}^{mod} & \longrightarrow & I_{1,n}^{mod} \\ \wr\wr & & \wr\wr \\ \mu_n & \xrightarrow{e} & \mu_n \end{array}$$

car on a regardé

$s(\pi_1^{1/n})/\pi_1^{1/n}$

et ceci donne l'isom.

Or, $\pi_1 = \pi_2^{e} . u$ u unité

ce qui donne le facteur e dans le diagramme ci-dessus.

Identification de I_n^{mod} avec μ_n.

Soit V_K le groupe des valeurs de la valuation discrète v. (En fait, $V \cong \mathbb{Z}$)

$$I_n^{mod} \cong \mathrm{Hom}(V_K, \mu_n).$$

$w \in V$

$\alpha \in K^*$, $v(\alpha) = w$.

On regarde $s(\alpha^{1/n})/\alpha^{1/n} \mod \pi \in \mu_n$.

$$I_n^{mod} \to \mathrm{Hom}(V_K, \mu_n)$$

est défini même si la valuation n'est pas discrète (mais pas isom. en général).

Ceci permet de voir la fonctorialité en K :

$$K_1 \longrightarrow K_2$$

$$\begin{array}{ccc} V_{K_1} & \longrightarrow & V_{K_2} \\ & e & \\ \mathbb{Z} & \longrightarrow & \mathbb{Z} \end{array}$$

.

K corps muni d'une valuation discrète v.

$$r : H^n(K, C) \to H^{n-1}(k, C(-1))$$

$$k = k(v)$$

<u>Critère de nullité</u> du résidu.

K corps avec valuation discrète v
corps résiduel $k(v)$.

Soit G un groupe fini, et C un G-module annulé par n, $(n, p(k(v))) = 1$.

On se donne $\varphi : G_K \to G$ un homomorphisme.

Soit $I_K(v)$ le groupe d'inertie de G_K relativement à v (défini à conjugaison près).

<u>Hypothèse</u> :

$\varphi(I_K(v))$ opère trivialement sur C

("C est non ramifié en v")

Soit
$$e_\varphi = |\varphi(I_K(v))|.$$

(Dans l'exemple de Mestre : $K = \mathbb{Q}(T)$,
$G = PSL_2(\mathbb{F}_7)$, $C = \mathbb{Z}/2\mathbb{Z}$, v place
à l'infini, $e_\varphi = 3$ (ou 9 ?)).

Soit $\alpha \in H^n(G, C)$

$$\varphi^*\alpha \in H^n(K, C)$$

<u>Théorème:</u> $e_\varphi \cdot r(\varphi^*\alpha) = 0$

<u>Corollaire</u>: Si $(e_\varphi, n) = 1$, $r(\varphi^*\alpha) = 0$.

(Mestre : $\alpha \in H^2(C, \mathbb{Z}/2\mathbb{Z})$, $\tilde{G} = SL_2(\mathbb{F}_7) \to G$
classe de cette extension $= \alpha$.
Le corollaire dit qu'il n'y a pas de résidu
à l'infini)

On peut supposer K complet

(1) Cas particulier "φ non ramifié"
φ trivial sur I_K.

$$\begin{tikzcd} G_K \arrow[r, "\varphi"] \arrow[dr] & G \\ & G_k \arrow[u] \end{tikzcd}$$

$\varphi^*\alpha \in H^n(G_k, C) \hookrightarrow H^n(G_K, C)$

$\Rightarrow r(\varphi^*\alpha) = 0$.

On a alors $r(\varphi^*\alpha)=0$

② Cas général

<u>Lemme :</u> Il existe $K' \subset K_s$, $[K':K]=e$ de corps résiduel k' avec k' ~~résiduel~~ radiciel sur k.

$\varphi(I_{K'}) = \{1\}$.

On admet le lemme.

On applique au couple K, K' la ~~propriété~~ proposition :

$e_\varphi = |\varphi(I_K)|$.

$$r_{K'}(\varphi^*\alpha) = e\, r_K(\varphi^*\alpha)$$

où e est l'indice de ramification de K'/K.

$[K':K] = e(K'/K)[k':k]$

$$e_\varphi = e.p^s \qquad p^s = [k':k]$$

Par ① appliqué à K', on a

$$r_{K'}(\varphi^*\alpha)=0.$$

D'où $e.r(\varphi^*\alpha)=0$

et <u>a fortiori :</u> $e_\varphi . r(\varphi^*\alpha)=0$.

(3) Démonstration du lemme : (50)

$$\varphi : G_K \to G$$

$$I_K \longrightarrow \varphi(I_K)$$

$I'_K = \ker \varphi : I_K \to \varphi(I_K)$.

I'_K est un s/g ouvert de I_K d'indice e_φ.

Ce s/g est normal dans G_K.

On a vu que $G_K = I_K \cdot \Gamma$, où Γ est un relèvement de G_k.

On définit $I'_K \cdot \Gamma$ s/g ouvert de G_K d'indice e_φ.

$$G_{K'} = I'_K \cdot \Gamma .$$

$$I_{K'} = I'_K$$

Radiciel sur k :

$$1 \to I_K \to G_K \to G_k \to 1$$

$G_{K'} \nearrow$ surjectif

Ceci entraîne que k'/k est radiciel (mais pas néc. $k = k'$!!).

Parenthèse :

Comparaison du résidu cohomologique avec celui de la K-théorie de Milnor et de la théorie des formes quadratiques.

(Relation avec la théorie de Bruhat-Tits — mais ceci n'est pas encore explicité).

K-théorie de Milnor

F corps commutatif. Milnor définit :

$$K_*^M F = \bigoplus_{m \geq 0} K_m^M F \qquad K_0 F = \mathbb{Z}$$

$$K_1 F = F^{\bullet}$$

engendré par $K_1 F$

relation ~~$(x, 1-x) = 0$~~

$$(x)(1-x) = 0 \qquad x \in F^{\bullet},\ x \neq 1$$

dans $K_2 F$

On prend l'algèbre engendrée sur $\mathbb{Z}$ par $F^{\bullet}$ et on prend ces relations.

Homomorphisme de résidu :

$F = K$ corps local

$$K_m K \xrightarrow{\partial} K_{m-1} k$$

(Milnor, Invent. Math. — 1970).

caractérisé par

$$(\pi, u_1, \dots, u_{n-1}) \longmapsto (\tilde{u}_1, \dots, \tilde{u}_{n-1})$$

$$K_n(K) \qquad\qquad K_{n-1}(k)$$

π uniformisante

$u_1, \dots, u_{n-1}$ unités

$\tilde{u}_1, \dots, \tilde{u}_{n-1} \in k^*$ leurs images.

On travaille avec $K_n(K)/n.K_n(K)$

et on construit un homomorphisme

$$K_n(K)/nK_n(K) \xrightarrow{\theta} H^n(K, \mu_n^{\otimes n})$$

n premier à car(k).

L'existence résulte d'un théorème de Tate

I. M. 1976

$n = 2$, Milnor 1970.

caractérisé par $\begin{cases} \text{multiplicativité} \\ x \in K^* \quad (x) \mapsto (x) \in H^1(K, \mu_n) \end{cases}$

$x \neq 0, 1$ $\qquad (x)(1-x) = 0$ dans $H^2(K, \mu_n^{\otimes 2})$

$1-x$ norme dans $K[T]/(T^n - x)$.

θ commute au résidu.

K local.

$$\begin{array}{ccc} K_m(K)/n\,K_m(K) & \xrightarrow{\theta_K} & H^m(K, \mu_n^{\otimes m}) \\ \downarrow{\scriptstyle r^M} & & \downarrow{\scriptstyle r} \\ K_{m-1}(k)/n\,K_{m-1}(k) & \xrightarrow{\theta_k} & H^{m-1}(k, \mu_n^{\otimes m-1}) \end{array}$$

$$\mu_n^{\otimes m}(-1) = \mu_n^{\otimes (m-1)}.$$

On vérifie que le diagramme est commutatif : il suffit de regarder

$$(\pi, u_1, \dots, u_{m-1}) \longmapsto (\tilde{u}_1, \dots, \tilde{u}_{m-1}).$$

Théorie de Quillen ??

Pas de flèche (il faut prendre les classes de Chern).

Théorie des formes quadratiques

K local complet, car $k \neq 2$.

Anneau de Witt : W_K.

Idéal fondamental : I_K.

$$0 \to I_K \to W_K \longrightarrow \mathbb{Z}/2\mathbb{Z} \to 0$$

k corps local, π uniformisante.

f corps quadratique sur K

f anisotrope (ne représente pas 0)

$$\Longrightarrow \quad f = \underbrace{g(x_1, \dots, x_a)}_{\substack{\text{à coeff. ds } A_K \\ \text{réd. mod } \pi \text{ non dég} \\ \text{et anisotrope}}} + \pi \underbrace{h(x_{a+1}, \dots, x_n)}_{\text{idem.}}$$

$$f = \langle u_1, \dots, u_a \rangle \oplus \langle \pi u_{a+1}, \dots, \pi u_n \rangle$$

u_i unités

aniso. après réduction sur k

Plongement naturel

$$W_k \hookrightarrow W_K$$

on relève les coeff. (indép. du relèvement)

$$W_K = W_k \oplus \langle \pi \rangle W_k .$$

$$I_K^m = I_k^m \oplus (\langle \pi \rangle - 1) I_k^{m-1} .$$

$$W_K = W_k \oplus (\langle \pi - 1) W_k$$

$$1 = \langle 1 \rangle .$$

$$I^n_K / I^{n+1}_K = I^n_k / I^{n+1}_k \oplus I^{n-1}_k / I^n_k$$

$$\begin{tikzcd}
0 \arrow[r] & I^n_k / I^{n+1}_k \arrow[r] \arrow[d, "e^k_n"] & I^n_K / I^{n+1}_K \arrow[r] \arrow[d] & I^{n-1}_k / I^n_k \arrow[r] \arrow[d, "e"] & 0 \\
0 \arrow[r] & H^n(k, \mathbb{Z}/2\mathbb{Z}) \arrow[r] & H^n(K, \mathbb{Z}/2\mathbb{Z}) \arrow[r, "r"] & H^{n-1}(k, \ldots) \arrow[d] & \\
& & & 0 &
\end{tikzcd}$$

(indép. du choix de π).

Si les flèches existent, le diagramme est commutatif (dans les 2 théories, $\pi, u_1, \ldots, u_{n-1} \to u_1, \ldots, u_{n-1}$)

Flèches existent pour $n \leq 4$ (Jacob-Rost. I.M. 1989).

<u>Corestriction et résidus</u> :

$K' \supset K$ ext. finie,

C un G_K-module, on veut définir

$$\mathrm{Cor} : H^n(G_{K'}, C) \longrightarrow H^n(G_K, C)$$

$$\overline{K} \setminus K' \setminus K$$

$G_{K'} \subset G_K$, indice $[K':K]_s$

$\left(\mathrm{Cor}_{G_K}^{G_{K'}}\right)$: $\mathrm{Cor} : H^n(G_{K'}, C) \longrightarrow H^n(G_K C)$ est défini :

$$\mathrm{Cor}_{K'/K} : H^n(K', C) \longrightarrow H^n(K, C)$$

<u>Définition</u> : $\mathrm{Cor}_{K'/K} = [K':K]_i \, \mathrm{Cor}_{G_K}^{G_{K'}}$

Pourquoi est-ce raisonnable ?

$$H^0 \to \text{trace}.$$

$C = \mu_n$ $\quad H^1(K, \mu_n) = K^*/K^{*n}$

$$H^1(K', \mu_n) = K'^*/K'^{*n}$$

$$\mathrm{Cor}_{K'/K} : K'^*/K'^{*n} \longrightarrow K^*/K^{*n}$$

est induite par la <u>norme</u> $N_{K'/K}$.

<u>Cas local complet</u> :

C. G_k-module

K'/K séparable (mais k'/k non néc. séparable).

Proposition :

Le diagramme suivant est commutatif :

$$\begin{array}{ccc} H^n(K',C) & \xrightarrow{\mathrm{Cor}} & H^n(K,C) \\ \downarrow r_{K'} & & \downarrow r_K \\ H^{n-1}(k,C(-1)) & \xrightarrow{\mathrm{Cor}_{k'/k}} & H^{n-1}(k,C(-1)) \end{array}$$

(En fait, K'/K séparable n'est pas nécessaire)

Il vaut mieux voir ça dans toute la suite exacte :

$$\begin{array}{ccccccc} 0 \to & H^n(k,C) & \to & H^n(K,C) & \to & H^{n-1}(k,C(-1)) & \to \\ & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & & \downarrow e.\mathrm{Res} & \\ 0 \to & H^n(k',C) & \to & H^n(K',C) & \to & H^{n-1}(k',C(-1)) & \to \\ & \downarrow e.\mathrm{Cor} & & \downarrow \mathrm{Cor} & & \downarrow \mathrm{Cor} & \\ 0 \to & H^n(k,C) & \to & H^n(K,C) & \to & H^{n-1}(k,C(-1)) & \to \end{array}$$

$$e.[k':k] = [K':K]$$

Donc le composé est chaque fois $\times n$.

Démonstration la prochaine fois.

$$H^p(G/H, H^q(H,C)) \Rightarrow H^*(G,C)$$

$G' \subset G$ indice fini. $\quad H' \subset H \quad G'/H' \subset G/H$

$H^*(G',C) \xrightarrow{\mathrm{Cor}} H^*(G,C) \qquad (G = G_K,\ H = \text{inerti})$

28 oct 91
Cours 4

pas de cours les 4 et 11 Nov.

Restait à démontrer lemme de compatibilité corestriction / residu :

K'/K corps locaux, ext séparable.
k'/k corps residuels
C : G_k - module annulé par n $\quad (n, p(k)) = 1$.

lemme
on a diagramme **commutatif**

$$\begin{tikzcd} H^n(K, C) \arrow[r, "r_K"] & H^{n-1}(k, C(-1)) \\ H^n(K', C) \arrow[u, "\mathrm{Cor}"] \arrow[r, "r_{K'}"] & H^{n-1}(k', C(-1)) \arrow[u, "\mathrm{Cor}"'] \end{tikzcd}$$

(on rappelle : $\mathrm{Cor}_k^{k'} : H^n(k') \longrightarrow H^n(k)$
$$\begin{tikzcd} H^n(k') \arrow[r] \arrow[d, phantom, "\wr\wr"] & H^n(k) \arrow[d, phantom, "\wr\wr"] \\ H^n(G_{k'}) \arrow[r, "i"] & H^n(G_k) \end{tikzcd}$$
) $\quad i = [k' : k]_{ins}$

pf : Il suffit de traiter 2 cas
1 K'/K non-ramifiée ($e = 1$ et $[k' : k]_i = 1$)
2 k'/k est radiciel.

$$\begin{tikzcd} 0 \arrow[r] & H^n(k, C) \arrow[r] & H^n(K, C) \arrow[r, "r_K"] & H^{n-1}(k, C(-1)) \\ 0 \arrow[r] & H^n(k', C) \arrow[r] \arrow[u, "e.\mathrm{Cor}"] & H^n(K', C) \arrow[r] \arrow[u, "\mathrm{Cor}"] & H^{n-1}(k', C(-1)) \end{tikzcd}$$

où pr $\alpha \in H^n(k', C)$, $r_{k'}(\alpha) = 0$
$\mathrm{Cor}\,\alpha$: $r_k(\mathrm{Cor}\,\alpha) = 0$.

Cas 1 - π unif de K, est une unif de K'.
$\alpha \in H^n(K', C)$. Peut s'écrire
$\alpha = \alpha_0 + \underbrace{(\pi) \cdot \beta}_{\text{cup prod}}$ où $\alpha_0 \in H^n(k', C)$
$\beta \in H^{n-1}(k', C(-1))$
$\underbrace{(\pi) \in H^1(K', \mu_n)}_{\text{Kummer}}$

$r_{K'}(\alpha) = \beta$
formule connue : $\mathrm{Cor}\,\alpha = \mathrm{Cor}\,\alpha_0 + (\pi) . \mathrm{Cor}(\beta)$
d'où $r_K(\mathrm{Cor}(\alpha)) = \mathrm{Cor}(\beta)$.

Cas 2 : π' unif de K'.

$$N\pi' = \pi^i . u$$

où π est une unif de K — serait unif de K si ext residuelle separable

u unité

$i = [k_s : k]$;

radiciel $\Rightarrow H^*(k, C(-1)) \simeq H^*(k', C(-1))$.

on écrit $\alpha = \alpha_0 + (\pi') \cdot \beta$ où $\beta \in H^{n-1}(k, C(-1))$ (identifié par restriction à un élmt de k', de k)

$$\mathrm{Cor}\, \alpha = \mathrm{Cor}\, \alpha_0 + (N\pi') \cdot \beta$$

$$r\left((N\pi') \cdot \beta \right) = i\beta = \mathrm{Cor}_k^{k'} \beta .$$

$\square$

Désormais on laissera tomber les ext radicielles, on pourra récuperer cas insep à la fin à partir du cas separable.

III Corps de fonction d'une variable

(~~[illegible]~~)

k parfait

X courbe projective lisse, abs. connexe sur k
(i.e k alg. fermé ds K)

$K = k(X)$: corps des fonctions ~~de~~ X

$\bar{k}$: clot alg de k dans K_s, clot sep de K.

$$\begin{tikzcd} K_s \arrow[d, dash, "N"] \\ \bar{k}\otimes_k K = \bar{k}\cdot K \arrow[d, dash, "G_k"] \\ K \end{tikzcd} \quad G_K$$

(c'est un corps, pas necess de prendre corps de frac)

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

$N = \mathrm{Gal}(K_s/\bar{k}K)$

$\bar{k}K$: corps des fcts de X sur $\bar{k}$.

Prop : Si X a un pt rationnel sur k (i.e $X(k) \neq \emptyset$), la suite exacte $1 \to N \to G_K \to G_k \to 1$ est scindée

Soit $P \in X(k)$, d'où v, val discrète sur K, à corps res k.

Soit $w : K_s^* \to \mathbb{Q}$ une ext de v à K_s

Soit $G_w \subset G_K$ le gpe de <u>décomp</u> de w
(l'ens des $s \in G_K$, $sw = w$).

$G_w \simeq$ ~~Gal~~ G_{K_v} ~~[illegible]~~ où K_v = complété de K pour v.
(on a clairement $G_{K_v} \twoheadrightarrow G_w$
iso : pas évident. lemme d'approx. ou ~~K~~rasner).

par la théorie locale : on a relevmt de G_k ds G_{K_v}

$$\begin{tikzcd} G_w \arrow[r, phantom, "\simeq"] \arrow[dr] & G_{K_v} \arrow[d] \\ & G_k \arrow[u, dotted, bend right] \end{tikzcd}$$

On voit donc que la donnée d'un pt détermine (pas canon) un relevmt.

Soit $\bar{k}$ clot ~~sep~~ alg de k dans K_s, clot sep de K.

Prop : $cd_\ell\, N = 1$

pf : ≥ 1 clair
≤ 1 : Thm (Tsen) $\bar{k}K$ est un (C_1)-corps. $\square$.

C : G_k-module annulé par n. , $(n, p(k)) = 1$.

N.B : Si X a un pt rat / k, la flèche
$H^m(G_k, C) \longrightarrow H^m(G_K, C)$ est injective
(et m une injection directe (i.e "split injection" : $\exists$ relev

Prop Soit δ le pgcd des degrés des pts fermés de X (sens des schemas)
Si $(\delta, n) = 1$, les flèches
$H^m(k, C) \longrightarrow H^m(K, C)$ sont injectives.
pf Quitte à couper C en morceaux, on peut supposer
$n = \ell^\alpha$, ℓ premier.
Par hypothese, il y a un $P \in X$, deg P premier à ℓ
$k(P) = k'$, $[k' : k] = d$, $(d, \ell) = 1$.
Sur k' : $H^m(k', C) \to H^m(k'K, C)$ est inject, par N.B

$$\begin{tikzcd} & H^m(k', C) \arrow[r] & H^m(k'K, C) \\ H^m(k, C) \arrow[ur, "\text{inject car } (d,\ell)=1"] \arrow[rr] & & H^m(K, C) \arrow[u] \end{tikzcd}$$

$\square$

Ça nous suffira, mais ça laisse entière des tas de pbs :
(contre) e.g car $\neq 2$
X courbe de genre 0 sans pt rat
$\updownarrow$
$\alpha \in Br_2(k)$, α décomposable
$\overset{\shortparallel}{H^2}(k, \mathbb{Z}/2\mathbb{Z})$.

$C = \mathbb{Z}/2\mathbb{Z}$, $\mathrm{Ker}\left(H^n(k, \mathbb{Z}/2\mathbb{Z}) \to H^n(K, \mathbb{Z}/2\mathbb{Z})\right) = ?$

$\mathrm{Ker} = 0$ si $n = 1$

$\mathrm{Ker} = \{0, \alpha\}$ si $n = 2$

$\mathrm{Ker} = \{0, \alpha\} \cdot H^1(k, \mathbb{Z}/2\mathbb{Z})$ si $n = 3$ (Arason).

Conj (?) $\mathrm{Ker} = \{0, \alpha\} \cdot H^{n-2}(k, \mathbb{Z}/2\mathbb{Z})$???

On va maintenant s'occuper des résidus –

v val discrète de K triviale s/k

$\Leftrightarrow$ pt fermé de courbe X

$\Leftrightarrow$ anneaux locaux de X (sauf celui du pt générique)

$k(v)$ = corps résiduel corresp. $\updownarrow$ orbites de G_k opérant sur $X(\bar{k})$

Pour chaque v, on a (rappel $C(-1) = C \otimes (\mu_n)^\vee = \mathrm{Hom}(\mu_n, C)$).

$$r_v : H^n(K, C) \longrightarrow H^{n-1}(k(v), C(-1))$$

résidu :

On démontrera (aujourd'hui) :

Pour $\alpha \in H^n(K, C)$ donné :

Thm 1 (a) Presque tous les $r_v(\alpha)$ sont 0

(b) $\sum_v \mathrm{Cor}_k^{k(v)} r_v(\alpha) = 0$ dans $H^{n-1}(k, C(-1))$.

Thm 2 : Si $X = \mathbb{P}_1$, on a une suite exacte

$$0 \longrightarrow H^n(k, C) \to H^n(K, C) \xrightarrow{(r_v)} \bigoplus H^{n-1}(k(v), C(-1)) \xrightarrow{\Sigma\,\mathrm{Cor}} H^{n-1}(k, C(-1)) \to 0$$

Voir errata : page + 10 18 NOV.

Si $X(k) \neq \emptyset$ et $J = \mathrm{Jac}(X)$, on a suite exacte

$$\cancel{0} \to H^{m-1}(k, J_n \otimes C(-1)) \to H^n(K, C)/H^n(k, C) \to \bigoplus_v H^{m-1}(k(v), C(-1)) \to H^{m-1}(k, C(-1)) \to \cancel{0}$$

$H^{n-2}(\ldots)$

H^n

... Ker de ...

où J_n est le G_k-module $\mathrm{Ker}\, n : J(\bar{k}) \to J(\bar{k})$

$J_n \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$ où g = genre de X

par canon.

Cette suite nous dit où sont les résidus, et (à gauche) comment se comportent les pts holomorphes.

On a

$$1 \to N \to G_K \to G_k \to 1$$

$N = G_{\bar{k}K}$, $\mathrm{cd}\, N = 1$.

par suite spectrale, on sait

$$\cdots \to H^n(k, C) \to H^n(K, C) \xrightarrow{r} H^{n-1}(G_k, \mathrm{Hom}(N, C)) \to \cdots$$

pb : étudier $\underline{\mathrm{Hom}(N, C)}$. C'est un G_k-module.

C est de la poudre aux yeux : peut sat.

$\mathrm{Hom}(N, C) \simeq \mathrm{Hom}(N, \mu_n) \otimes C(-1)$.

Provient de ce que N^{ab} est isom à un prod de gpes $\mathbb{Z}_\ell$ (pas de torsion)

(idem pr $(N^{ab})'$: partie première à $p(k)$ alors $\ell \neq p(k)$).

c'est alors un $\mathbb{Z}_\ell$-module projectif.

$$\mathrm{Hom}(N, \mu_n) = H^1(G_{\bar{k}K}, \mu_n) \qquad N = G_{\bar{k}K}$$

$$= (\bar{k}K)^* / (\bar{k}K)^{*n} \qquad \bar{k} \text{ contient } \mu_n$$

On a une suite exacte :

$$\boxed{0 \to J_n \to \mathrm{Hom}(N, \mu_n) \to D/nD \xrightarrow{\deg} \mathbb{Z}/n\mathbb{Z} \to 0}$$

où D est le gpe des diviseurs de $X/\bar{k}$ (= module libre s/ $X(\bar{k})$)

$$(\bar{k}K)^* / (\bar{k}K)^{*n}$$

$$f \in (\bar{k}K)^* \longmapsto (f) = \sum_{w \in X(\bar{k})} w(f) \cdot w$$

montrons surjectivité :

on prend $\Delta \in D/nD$ choisi t.q. $\deg \Delta = 0$

définit un pt $[\Delta] \in J(\bar{k})$

or $[\Delta] = n[\Delta']$, $\deg[\Delta'] = 0$.

on est ramené au cas $[\Delta] = 0$

d'où $\Delta = (f)$.

(peut aussi se voir avec lemme du serpent :

$$\begin{array}{ccccccc} 0 \to & (\bar{k}K)^*/(\bar{k})^* & \to & D^0 & \to & J & \to 0 \\ & \downarrow n & & \downarrow n & & \downarrow n & \end{array}$$

(D^0 = div de degré 0)

donc serpent : $0 \to J_n \to \mathrm{Hom}(N, \mu_n) \to D^0/nD^0 \to 0$

suite encadrée : $\boxed{0 \to J_n \to \mathrm{Hom}(N, \mu_n) \to D/nD \xrightarrow{\deg} \mathbb{Z}/n\mathbb{Z} \to 0}$

(s'il y a un pt rat, c'est scindé)

D/nD comme G_k-module : $= \bigoplus_w \mathbb{Z}/n\mathbb{Z}$

$= \bigoplus_{v \text{ places de } k} \bigoplus_{w/v} (\mathbb{Z}/n\mathbb{Z})$

$= \bigoplus_v \mathrm{Ind}_{G_k}^{G_{k(v)}} \mathbb{Z}/n\mathbb{Z}$. : modules induits.

~~on sepa~~

Tord par $C(-1)$:

$$0 \to J_n \otimes C(-1) \to \mathrm{Hom}(N, C) \to \bigoplus_v \mathrm{Ind}_{G_k}^{G_{k(v)}} C(-1) \to C(-1) \to 0$$

"rappel" $H^{m-1}(G_k, \mathrm{Ind}_{G_k}^{G_{k(v)}} C(-1)) \underset{\text{Shapiro}}{=} H^{m-1}(G_{k(v)}, C(-1))$

$\downarrow \mathrm{Cor}$

$H^{m-1}(G_k, C(-1))$

par suite spectrale avec N,

on avait $r : H^m(K, C) \to H^{m-1}(G_k, \mathrm{Hom}(N, C))$

$$\begin{tikzcd} H^m(K, C) \arrow[r, "r"] \arrow[dr, "(\partial_v)"'] & H^{m-1}(G_k, \mathrm{Hom}(N, C)) \arrow[d] \\ & \bigoplus_v H^{m-1}(G_{k(v)}, C(-1)) \end{tikzcd}$$

(∂_v) s'en convaincre

lemme : ce triangle est commutatif.

$$\text{cf}: \begin{tikzcd} 1 \arrow[r] & N \arrow[r] & G_K \arrow[r] & G_k \arrow[r] & 1 \\ 1 \arrow[r] & I_v \arrow[r] \arrow[u] & G_{K_v} \arrow[r] \arrow[u] & G_{k(v)} \arrow[r] \arrow[u] & 1 \end{tikzcd}$$ diag comm pour les v.

permet de se convaincre (avec pbs d'écriture) que la composée du triangle est bien donnée par r_v (i.e triangle commute). $\square$.

composer avec
$$\begin{tikzcd} \bigoplus_v H^{n-1}(G_{k(v)}, C(-1)) \arrow[d, "\mathrm{Cor}"] \\ H^{n-1}(G_k, C(-1)) \end{tikzcd}$$

composee est 0.

Soit $P = \ker : D/nD \longrightarrow \mathbb{Z}/n\mathbb{Z}$.

Donc Thm 2.

On (Gabber) peut tout traduire en cohomologie étale pr les courbes.

Exemple 1

$X = \mathbb{P}_1$

pour $\alpha \in H^n(K, C)$,

* on a formule des résidus ("comme g_{ro}") : $\sum \mathrm{Cor}(r_v(\alpha)) =$
* Si ts les $r_v(\alpha)$ sont 0, alors α est "constant". i.e $\alpha \in H^n(k, C)$.

valeur de α en v si $r_v(\alpha) = 0$.

(marche ds cas local). défini en passant au cas local appartient à $H^n(k(v), C)$.

Cor : si ts les résidus de α (sf peut-être en 1 pt rationnel) sont 0, et si $\alpha(v) = 0$ pour un pt rat alors $\alpha = 0$.

(Analogue du Thm d'Abel sur les diviseurs)

Thm : Soit $\alpha \in H^n(K, C)$

Soit S l'ens. des pôles de α (places v où $r_v(\alpha) \neq 0$).

Soit $f \in K^*$, valant 1 en tt pt de S.

soit $D = \sum n_v v$, le diviseur de f.

Alors $\alpha(D) = 0$, où $\alpha(D) = \sum_{n_v \neq 0} n_v \alpha(v)$

Pf : voir f comme un morphisme $X \xrightarrow{f} \mathbb{P}_1$

On suppose f séparable :

$\alpha \in H^n(K, C)$

$\longrightarrow f_*(\alpha) = \mathrm{Cor}(\alpha)$ pr l'ext de corps $K / k(f)$

d'où $f_*(\alpha) = \beta \in H^n(K_{\mathbb{P}_1}, C)$.

les résidus de β sont 0.

(ne pourrait avoir des résidus qu'aux images des pôles.

or ils vont tous sur 1. (et $r_{v_0}(f_* \alpha) = \sum_{v / v_0} \mathrm{Cor}\, r_v(\alpha)$)

par fule de résidus sur $\mathbb{P}_1$,

la somme est 0.

$\Longrightarrow \beta$ est cst, et $\beta(0) = \beta(\infty)$

$$\sum_{n_v \geq 1} n_v \alpha(v) \qquad \sum_{n_v \leq -1} -n_v \alpha(v)$$

d'où (?) $\alpha(v) = 0$.

□.

Cor 1 Soit $X = E$ une courbe elliptique munie d'une origine 0.

Soit $\alpha \in H^n(K, C)$, sans pôles, et $\alpha(0) = 0$

(si on avait une courbe de genre 0, α serait cste, ici g = 1).

Alors la flèche $P \in E(k) \longmapsto \alpha(P) \in H^n(k, C)$,

est un homomorphism.

Cor 2 : Si $C = \mathbb{Z}/2\mathbb{Z}$ on a $\alpha(2P) = 0 \quad \forall P \in E(k)$.

pf : Il faut démontrer : P_1, P_2, $Q = P_1 + P_2$

$\overset{?}{\Rightarrow} \alpha(Q) = \alpha(P_1) + \alpha(P_2)$

on a un diviseur $(f) = (0) + (Q) - (P_1) - (P_2)$

$f = 1$ sur S puisque $S = \emptyset$.

d'où : $\underset{\overset{\shortparallel}{0}}{\alpha(0)} + \boxed{\alpha(Q) - \alpha(P_1) - \alpha(P_2) = 0}$

□.

vu expérimentalement par Fait (surprise !)

pr $C = \mathbb{Z}/2\mathbb{Z}$, $m = 2$; regarde Br_2.

4 pts ramifiés.

<u>Résultat analogue</u> pr une courbe X arbitraire avec un pt rat, S quelconque, mais il faut faire intervenir J_S : Jac. généralisée sur la courbe.

<u>Exemple</u> de détermination de $Br_2 K$.

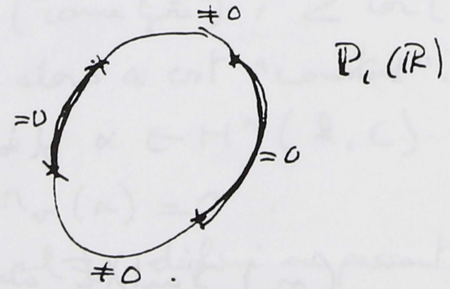
(v. 1er cours :

① $k = \mathbb{R}$, $X = \mathbb{P}_1$

le nbre de pts à résidu est pair,

$Br_2 \mathbb{R}(T)$

déterminé dès qu'on a valeur (0 ou $\neq 0$) en 1 pt, alors intervalles alternent



)

② $K = \mathbb{C}(X, Y)$. Pourrait se faire par récurrence ; quand on connaît $Br_2(K(T))$.

Résultat : $K = \mathbb{C}(\mathbb{P}_2)$.

$\alpha \in Br_2 K$

V = ens des val discrètes de K associées aux <u>courbes</u> irréd de $\mathbb{P}_2$.

$v \in V \longleftrightarrow \Gamma_v$: courbe irred, corps fcts : $\mathbb{C}(\Gamma_v)$

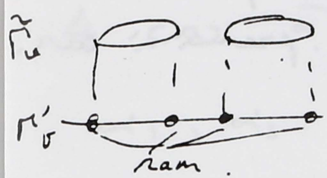
$r_v(\alpha) \in H^1(\mathbb{C}(\Gamma_v), \mathbb{Z}/2\mathbb{Z})$ — Γ'_v : normalisée de Γ_v

donc un elmt $\neq 0$ correspond à un revet quad de Γ'_v (elmt de Br_2)

$$0 \to Br_2 K \longrightarrow \bigoplus_v H^1(\mathbb{C}(\Gamma_v), \mathbb{Z}/2\mathbb{Z})$$

on se donne plusieurs courbes. à quelles conditions y-a-t-il un elmt de $Br_2 K$ qui y correspond ? (i.e determiner Im Br_2)

revêt quad $\tilde\Gamma_v \to \Gamma'_v$



ram $(\tilde\Gamma_v \to \Gamma'_v)$: le diviseur de ramification sur Γ'_v.

Pour tt $v \in$ ens fini, soit $\tilde\Gamma_v \to \Gamma'_v$ un revêt quad

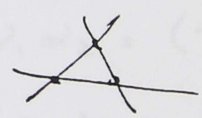
$\sum_v$ images des ram $(\tilde\Gamma_v \to \Gamma'_v)$ = <u>ram totale</u>.

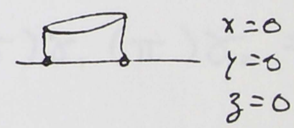
$$\boxed{Br_2 K \simeq \text{ens des } \{\tilde\Gamma_v\} \text{ t.q ram totale} \equiv 0 \pmod 2}$$

sur une droite : pas possible : valeur aux pts de S.

" 2 droites " "

3 droites : ça marche

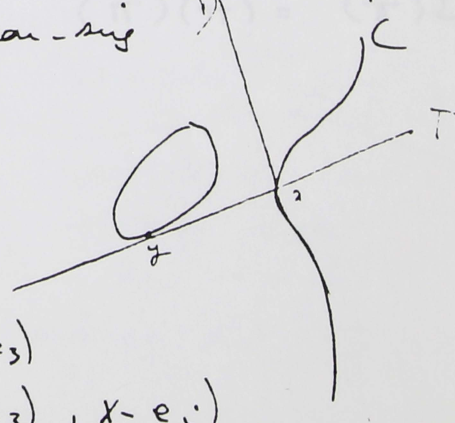




écrire α comme un symbole $\alpha(\frac{x}{y}, \frac{z}{y})$.

courbe ell : cubique non-sing

3 revêt quad



C, T, D

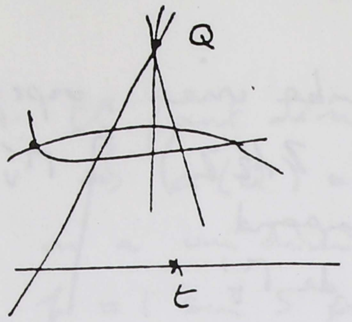
symbole $\alpha = \left(\frac{C}{T^3}, \frac{D}{T}\right)$

où, si $y^2 = (x-e_1)(x-e_2)(x-e_3)$

$\alpha = \left(y^2 - (x-e_1)(x-e_2)(x-e_3),\ x - e_i\right)$.

tt elmt de Br_2 est un (x, y) pour $x, y \in K^*$: symbole pur. (car formes quad à 5 vbls représentent 0.)

pf ?



On choisit Q en posit. gale.

K : corps de fcts d'une droite

proj. sur $k = \mathbb{C}(T)$

α : ds $H^1(K_c, \mathbb{Z}/2\mathbb{Z})$

$\mathrm{Cor}\ r(\alpha) \in H^1(\mathbb{C}(t), \mathbb{Z}/2\mathbb{Z})$

"et la somme de ts ces machins-la est zero".

v : Artin Mumford : Proc L. Math. Soc, 1972

décrivent $\mathrm{Br}\,K/\mathrm{Br}(\text{surfaces})$. pr surface simplement connexe partie de Br. premier à car.

Serre

Résidu d'un produit   cas local

Formule : $r(\alpha_1\alpha_2) = r(\alpha_1)\alpha_2 \pm \alpha_1 r(\alpha_2) + r(\alpha_1)r(\alpha_2)\cdot\varepsilon$

où $\pm = (-1)^{\deg(\alpha_1)}$, ε = classe de -1 dans $H^1(K,\mu_n)$

Dém : π un. f. de K

Soit $\gamma \in H^m(k, C(-1)) \subset H^m(K, C(-1))$

$(\pi)\cdot\gamma \in H^{m+1}(K, C)$

$r((\pi)\cdot\gamma) = \gamma$.

4 cas à vérifier :

α_1, α_2 tous les deux non ramifiés ($\in H^*(k)$).

α_1 non ramifié, $\alpha_2 = (\pi)\cdot\gamma_2$ γ_2 non ramifié

$\alpha_1 = (\pi)\cdot\gamma_1$ α_2 non ramifié

$\alpha_1 = (\pi)\cdot\gamma_1$ $\alpha_2 = (\pi)\cdot\gamma_2$

. $r(\alpha_1) = r(\alpha_2) = 0$: tout est 0 dans la formule.

. $r(\alpha_1) = \gamma_1$, $r(\alpha_2) = \gamma_2$ $\alpha_1\alpha_2 = (\pi)\gamma_1(\pi)\gamma_2 =$

$= \pm(\pi)(\pi)\gamma_1\gamma_2 = \pm(\pi)\varepsilon\gamma_1\gamma_2$

On a : $(\pi)(-\pi) = 0$, donc $(\pi)(\pi) = (\pi)\varepsilon$

$r(\alpha_1\alpha_2) = \varepsilon\gamma_1\gamma_2$.

Cas particulier :

$C_1 = C_2 = C = \mathbb{Z}/2\mathbb{Z}$

$m_1 = m_2 = 1$ $\alpha_1 \in H^1(K) = K^*/K^{*2}$

α_2

$\alpha_1 = (a_1) \quad a_1 \in K^*$ $\quad \alpha_2 = (a_2) \in K^*$

$a_2 \in K^*$

$\alpha_1 \alpha_2 \in Br_2(K)$

$(a_1, a_2) = (a_1)(a_2) \in Br_2(K)$

$r((a_1)(a_2)) \in H^1(k)$

$r((a_1)(a_2)) = (x)$, où

$(x) = v(a_1)(a_2) + v(a_2)(a_1) + v(a_1)v(a_2)\varepsilon \quad (\varepsilon = -1)$

$x = (-1)^{v(a_1)v(a_2)} a_2^{v(a_1)} / a_1^{v(a_2)}$

Calcul du résidu du H^3

$C_1 = C_2 = \mathbb{Z}/2\mathbb{Z}, \quad r: H^3(K) \to H^2(k) \subset H^2(K)$

$r((a_1)(a_2)(a_3)) = \underset{\substack{\text{sommation} \\ \text{par perm. circ.}}}{S} v(a_1)(a_2)(a_3) + [S v(a_1)v(a_2)(a_3)]\varepsilon$

$+ v(a_1)v(a_2)v(a_3)\varepsilon.\varepsilon$

$(-1)(-1)$

Fin du supplément !

Correction du dernier cours :

"Thm 2" est faux.

Retour à la situation du thm ? :

courbe X/k, k parfait, X lisse, proj. abs. irr

$K = k(X)$ corps de fonctions de X

C un G_k-module annulé par n,
n premier à $p(k) = p(K)$.

$\bar{k}$: clôture algébrique de k.

$$G_K\left(\begin{array}{l} K_s \\ \mid\ N \\ \bar{k}K \\ \mid\ G_k \\ K \end{array}\right.$$

$\mathrm{cd}\, N \leq 1$

$$1 \to N \to G_K \to G_k \to 1$$

$$\cdots \to H^m(G_k, C) \to H^m(G_K, C) \xrightarrow{r} H^{m-1}(G_k, \mathrm{Hom}(N, C)) \to \cdots$$

$$\mathrm{Hom}(N, C) = \underbrace{\mathrm{Hom}(N, \mu_n)}_{= \, (\bar{k}K)^*/(\bar{k}K)^{*n}} \otimes C(-1)$$

$$0 \to J_n \to \mathrm{Hom}(N, \mu_n) \to D/nD \underset{\longleftarrow}{\to} \mathbb{Z}/n\mathbb{Z} \to 0$$

dû à P (*)

D = diviseurs de $X/\bar{k}$

(compatible avec l'action de G_k

On a trouvé la formule des résidus
(comp. 2 flèches = 0)

(Hyp) X a un point rationnel $/k$., $P^{(*)}$

$D = D_0^{\cdot} \oplus \mathbb{Z}P.$

$$0 \to J_n \to \mathrm{Hom}(N, \mu_n) \to D_0/nD_0 \to 0$$

$$G_k \rightleftarrows G_k .$$

On a donc des suites exactes courtes

$$0 \to H^n(G_k, C) \to H^n(G_K, C) \to H^{n-1}(G_k, \mathrm{Hom}(N, C)) \to$$

$$H^n(G_K, C)/H^n(G_k, C) \cong H^{n-1}(G_k, \mathrm{Hom}(N, C))$$

$$\parallel$$

$$H^{n-1}(G_k, \mathrm{Hom}(N, \mu_n) \otimes C(-1))$$

On tensorise la suite $0 \to J_n \cdots$ par $C(-1)$

et on trouve :

$$0 \to J_n \otimes C(-1) \to \mathrm{Hom}(N, \mu_n) \otimes C(-1) \to D_0/nD_0 \otimes C(-1)$$

$$\cdots \to H^{n-1}(k, J_n \otimes C(-1)) \to H^n(K, C)/H^n(k, C) \to$$

$$H^{n-1}(k, D_0/nD_0 \otimes C(-1)) \to \cdots$$

$$H^{n-1}(k, D_0/nD_0 \otimes C(-1)) \cong$$

Il manque la page 74 dans le document original.

$P \in X(k) \qquad (P)-(0)$

$$X(k) \longrightarrow D^0(X,k)/n\,D^0(X,k)$$

$$P \longmapsto (P)-(0).$$

$$X(k) \xrightarrow{\delta} H^1(k, X_n)$$

Théorie de la descente fournit :

$$0 \to X_n \to X \xrightarrow{n} X \to 0$$

$$0 \longrightarrow X(k)/n\,X(k) \xrightarrow{\delta'} H^1(k, X_n)$$

calcul : $\delta = -\delta'$.

Trouver courbe elliptique t.q. $X(k)/n\,X(k) \neq 0$

— très facile.

Donc $\delta' \neq 0 \implies \delta \neq 0$ en général.

k <u>imparfait</u>

X courbe proj. lisse abs. irréd. sur k

La formule des résidus est vraie pour X

$K = k(X)$.

$\alpha \in H^n(K, C)$

$$\sum_v \mathrm{Cor}_k^{k(v)} r_v(\alpha) = 0 \qquad \text{dans } H^{n-1}(k, C(-1))$$

On remplace k par $k^{p^{-\infty}}$. On applique la formule des résidus à α sur $k^{p^{-\infty}} = k'$

k', $k'(v)$.

Applications à $\mathbb{P}_1$, $\mathbb{P}_n$

Si $X = \mathbb{P}_1$.

$$H^n(K, C)/H^n(k, C)$$

$$\Vert S\, r$$

$$\bigoplus_v^{\circ} H^{n-1}(k(v), C(-1))$$

$$\Vert S$$

$$\bigoplus_{v \neq \infty} H^{n-1}(k(v), C(-1)).$$

Tout classe de cohomologie dont les résidus sont nuls (∞ excepté) est "constante", i.e. $\in H^m(k, C)$.

<u>Corollaire</u>: Si les résidus de α sont 0 et si α s'annule en un point rat. de $\mathbb{P}_1$, alors $\alpha = 0$.

α

v pas un pôle

Dans K_v, $\underset{K_v}{\alpha} \in H^m(k/v), C)$

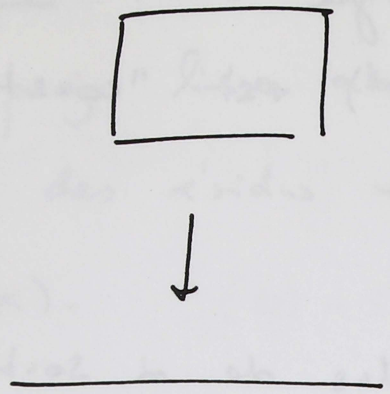
$$\underset{K_v}{\alpha} = \alpha(v) \quad \text{"valeur de } \alpha \text{ en } v\text{"}.$$

$Y = \mathrm{Aff}^N / k$

$K = k(Y) = k(t_1, \dots, t_N)$.

<u>Th</u>: Tout classe de cohomologie dans $H^m(K, C)$ (C G_k-module annulé par n) dont les résidus (p.r. aux diviseurs irréd. de Y) sont 0, est constante (i.e. $\in H^m(k, C)$)

<u>Démonstration</u>: par récurrence sur N.



Aff^N

fibré dte affine

Aff^{N-1}

$$K = K_N$$

$$|$$

$$K_{N-1} = k(t_1, \dots, t_{N-1})$$

1ère étape : $\alpha \in H^n(K_{N-1}, C)$

A voir : les résidus de α p.r. aux points fermés de la droite affine $\mathrm{Spec}\, K_{N-1}[t_N]$ sont 0.

$\rightarrow$ div. irred. de Aff^N non "verticaux"

2ème étape : voir que les résidus de

$\alpha \in H^n(K_{N-1}, C)$

par rapport aux div. irréd. de Aff^{N-1} sont 0.

div. irréd. de Aff^N

corps résiduels pas les mêmes

div. irr. de A^{N-1}

$$K_N(v) = K_{n-1}(v)(t_N)$$

$$K_{N-1}(v)$$

$$r_v(\alpha) \in H^{m-1}(K_{N-1}(v), C(-1)) = 0 \ ?$$

$\downarrow$ se tue ds $H^{m-1}(K_N(v), C(-1))$

injectif $\longrightarrow$ $r_\alpha(\alpha) = 0$.

Soit $\alpha \in H^m(k(t_1, .., t_N), C)$

on peut regarder sur $\mathbb{P}_{N-1}$

(mais inutile - suffit de regarder

l'espace affine).

Applications (à la vérification des formules)

Ex: $m = 2$, $C = \mathbb{Z}/2\mathbb{Z}$, $H^2(K, C) = Br_2(k)$.

Ex 1 (trivial)

$(x)(y) = (x+y)(-xy)$ si $x, y, x+y \neq 0$.

facile à montrer directement.

Ici on fait une dém. plus compliquée :

$\alpha = (x)(y) + (x+y)(-xy)$ $\quad \alpha \in H^2(k(x,y), ()$

k $\begin{cases} \text{pas de résidus} \\ \text{valeur 0 en un pt} \end{cases}$ $x = y = 1$ $\quad (1) = 0$

$(2)(-1) = 0.$

$\begin{cases} x = 0 \\ y = 0 \end{cases}$ $\quad (x)(y) \to (y)$ vu comme fonction sur $x=0$.

$(x)(x+y) \to (y)$
$(x+y)(-y) \to 0$
$\overline{\quad 0 \quad}$

$x + y = 0$

$(x)(y) \to 0$

$(x+y)(-xy) \to -xy$ sur $x+y=0$

$\overset{\shortparallel}{x^2}$

$(x^2) = 0$!

Ex 2 : x, y, z $\quad \sigma_1 = x+y+z \quad \sigma_2 = xy + yz + zx$

$\sigma_3 = xyz$

$(x)(y) + (y)(z) + (z)(x)$

$= (-\sigma_2)(\sigma_1\sigma_2 - \sigma_3) + (\sigma_2)(-\sigma_3)$

Ex 3 :

$= (\sigma_1)(-\sigma_3) + (\sigma_1\sigma_2 - 9\sigma_3)(-\sigma_1\sigma_3)$

Ex 2 ~~Sont~~ vraies si $x, y, z \neq 0$, $\sigma_2 \neq 0$, $x+y \neq 0$, $x+z \neq 0$, $y+z \neq 0$

Vérification de ex 2

$x = y = z = 1$ $\qquad \sigma_1 = \sigma_2 = 3$ $\qquad \sigma_3 = 1$

$$0 = (-3)(2) + (3)(-1) = (3)(2) + \cancel{(-1)(2)} +$$

$$+ (3)(-1) = (3)(-2) = (3)(1-3) = 0.$$

<u>vérifions</u>

On a : $\sigma_1 \sigma_2 - \sigma_3 = (x+y)(y+z)(z+x)$.

$x = 0$ $\qquad (yz) \overset{?}{=} \sigma_2$ par $x=0$ i.e. (yz) ✓

$y = 0$

$z = 0$

$\sigma_2 = 0$ $\qquad 0 \overset{?}{=} (-\sigma_3) + (-\sigma_3) = 0$ ✓

$x + y = 0$ $\qquad 0 = (-\sigma_2)$ sur $x+y=0$

$x + z = 0$ $\qquad = (-xy)$ "

$y + z = 0$ $\qquad = (+x^2) = 0$.

Ex 3 : difficile à vérifier par cette méthode

$\sigma_1 \sigma_2 - 9\sigma_3$ irréd.

montrer que $-\sigma_1 \sigma_3$ est un carré.

L'identité de l'ex 3 est beaucoup plus facile à démontrer par la théorie des formes quadratiques.

$$q = \langle x \rangle \oplus \langle y \rangle \oplus \langle z \rangle$$

$$= \langle x, y, z \rangle$$

$$w_2(q) = (x)(y) + (y)(z) + (z)(x).$$

A trouver : e_1, e_2, e_3 orthogonaux 2 à 2 qui donne la formule cherchée par w_2.

$e_1 = (1,1,1)$ $\qquad q(e_1) = x+y+z = \sigma_1$

$e_2 = (y-z,\ z-x,\ x-y)$ $\qquad q(e_2) = S\, x(y-z)^2$

$$= \sigma_1\sigma_2 - 9\sigma_3$$

e_3 $\qquad q(e_3) = \gamma$

$$x(y-z) + y(z-x) + z(x-y) = 0$$

$$S\, x(y-z)^2 = S\, x(y^2 - 2yz + z^2) = \sum xy^2 - 6xyz$$

$$= \sigma_1\sigma_2 - 9\sigma_3$$

$$\langle x, y, z \rangle \simeq \langle \sigma_1, \sigma_1\sigma_2 - 9\sigma_3, \gamma \rangle$$

$xyz = \sigma_3$ $\qquad \gamma = \sigma_1\sigma_3(\sigma_1\sigma_2 - 9\sigma_3)$

$$w_2 = (\sigma_1)(\sigma_1\sigma_3) + (\sigma_1\sigma_2 - 9\sigma_3)(\sigma_1\sigma_3(\sigma_1\sigma_2 - 9\sigma_3))$$

$(x)(x) = (x)(-1)$ $\qquad = (\sigma_1)(-\sigma_3) + (\sigma_1\sigma_2 - 9\sigma_3)(-\sigma_1$

83

X courbe proj. lisse sur k

$\alpha \in H^m(K, C)$ hyp. habituelles

S : ensemble fini de places contenant les pôles de α

$$D = \sum_{v \notin S} n_v v$$

$$\alpha(D) = \sum_v n_v \operatorname{Cor}_k^{k(v)} \alpha(v)$$

$$\begin{array}{c} \alpha(v) \in H^m(k(v), C) \\ \downarrow \operatorname{Cor} \\ H^m(k, C) \end{array}$$

$D = (f)$ $\qquad f \in K^*$

$f(v) \neq 0, \infty$ si $v \in S$

$f(v) \in k(v)^*$.

Formule : $\alpha(D) = \sum_{v \in S} \operatorname{Cor}_k^{k(v)} \left(((f(v))_{r_v} / \alpha) \right)$

$f(v) \in k(v)^*$

$(f(v)) \in H^1(k(v), \mu_m)$

$r_v(\alpha) \in H^{m-1}(k(v), C(-1))$

cup produit $\in H^m(k(v), C)$

Corollaire : Si $f(v)=1$ pour tout $v \in S$,

alors $\alpha(D)=0$. (formule à la Abel).

Corollaire Si $S=\emptyset$, $\alpha(D)=0$ (— ·)

$P \in X(k)$, $\alpha(P_0)=0$ alors $\alpha(P)$ ne dépend que de l'image de P dans la jacobienne généralisée J_S rel. à S.

$$1 \longrightarrow L_S \longrightarrow J_S \to J \to 1$$

$$L_S = \left(\prod R_{k(v)/k} \mathbb{G}_m\right) / \mathbb{G}_m$$

Préliminaire : Autre formule

$\alpha_1 \in H^{m_1}(K, C_1)$ $\alpha_2 \in H^{m_2}(K, C_2)$

$C_1 \times C_2 \to C$

S_1, S_2 ens. finis de places, $S_1 \cap S_2 = \emptyset$

$$\sum_{v\in S_1} \mathrm{Cor}_k^{k(v)}\left(r_v(\alpha_1)\cdot \alpha_2(v)\right) + (-1)^{m_1} \sum_{v \in S_2} \mathrm{Cor}_k^{k(v)} \left(\alpha_1(v)\cdot r_v(\alpha\right.$$

$$= 0$$

dans $H^{m_1+m_2-1}(k, C(-1))$.

<u>Démonstration</u>

On applique la formule des résidus à $\alpha_1 \alpha_2$

On applique la formule à $C_1 = \mu_n$, $C_2 = C$

$\mu_n \times C \longrightarrow C(1)$

$m_1 = 1$, $\alpha_1 = (f) \in H^1(K, \mu_n)$

$m_2 = n$, $\alpha_2 = \alpha \in H^n(K, C)$

$S_1 =$ zéros et pôles de f, $S_2 = S$

$$\underbrace{\sum \mathrm{Cor}_k^{k(v)} (\alpha_2(v)) \cdot \underbrace{v(f)}_{n^v}}_{\alpha(D} + \sum (f(v))$$

donne la formule.

25 NOV 91
cours 6

*Remarque sur la dernière fois :
On avait formule "vraie génériquement".
$(X+Y, -XY) = (X,Y)$ ds $Br_2\, k(X,Y)$

par spécialisation, c'est vrai $\forall x, y \in k$
t q $x, y, x+y \neq 0$
(i.e. formule a un sens)

expliciter cette spécialisation :
A local régulier, corps rés. k, de car $\neq 2$ (faux pr anneau qualconque)
K = corps de frac de A
$a_i, b_i, c_i, d_i \in A^*$;
$\tilde{a}_i, \tilde{b}_i, \tilde{c}_i, \tilde{d}_i \in k^*$ leurs résidus.
on a $\sum(a_i)(b_i)$, $\sum(c_i)(d_i) \in Br_2(K)$
$\sum(\tilde{a}_i)(\tilde{b}_i)$, $\sum(\tilde{c}_i)(\tilde{d}_i) \in Br_2(k)$

lemme de spécialisation. $\sum(a_i)(b_i) = \sum(c_i)(d_i)$
$\Rightarrow \sum(\tilde{a}_i)(\tilde{b}_i) = \sum(\tilde{c}_i)(\tilde{d}_i)$

Dem

$$\begin{array}{ccc} \sum(a_i)(b_i) = \sum(c_i)(d_i) & & \\ \alpha_A, \gamma_A & \longmapsto & \alpha_K, \gamma_K \\ & Br(A) & \longrightarrow Br(K) \\ \downarrow & \downarrow & \\ \alpha_k, \gamma_k & Br(k) & \end{array}$$

Th (Groth. : "10 exposés s/ la th des schemas")
$Br(A) \to Br(K)$ est injectif
pr A local regulier.

ou : autre methode : récurrence sur la dim de A
dim $A = 1$: ann. de val discrete (
on a $Br(A) \hookrightarrow Br(K)$
dim $A+1$: prend var. une ss. var
$t \in m - m^2$, passer à A/tA ...

et on induit situation sur la ss-var.

* <u>retour aux formules</u>

$K = k(X)$

$$\alpha(D) = \sum_{v \in S} \mathrm{Cor}_k^{k(v)} \Big(\underbrace{\underset{\in H^1}{(f(v))} \cdot \underset{\in H^{n-1}}{r_v(\alpha)}}_{\in H^n} \Big)$$

où $\alpha \in H^n(K, C)$

S ens fini de places contenant les pôles de

$f \in K^*$, $f(v) \neq 0, \infty$ si $v \in S$

$D = (f) = \sum v(f)\, v$ div. princ

$$\alpha(D) = \sum_{v(f) \neq 0} v(f)\, \mathrm{Cor}_k^{k(v)} \alpha(v)$$

$r_v(\alpha) \in H^{n-1}(k(v), C(-1))$

$f(v) \in k(v)^*$

si $x \in k(v)^*$ soit $(x) \in H^1(k(v), \mu_n)$

formule a un sens ds $H^n(k, C)$.

on note $\alpha(D) = \mathrm{Cor}_S\big((f(S)) \cdot r_S(\alpha)\big)$

et $k(S) = \prod_{v \in S} k(v)$ son Spec est produ de corps

On suppose maintenant que <u>$X = \mathbb{P}_1$</u>

$K = k(T)$.

poles de α.

$\mathbb{P}_1$

S : ens fini contenant pôles de α, $\infty \notin$

$x, y \in \mathbb{P}_1(k) - (S \cap \mathbb{P}_1(k))$

$$\alpha(x) - \alpha(y) = \sum_{v \in S} \mathrm{Cor}_k^{k(v)} \left(\left(\frac{x - t_v}{y - t_v} \right) \cdot r_v(\right.$$

places de $\mathbb{P}_1$:

rationales : élts de k

non rat. : pr $T \in K$. $T \mapsto t_v \in k(v)^*$.

diviseur : $D = \{x\} - \{y\}$

$D = (f)$ où $f = \dfrac{T-x}{T-y}$

m̂ hyp, On suppose $\alpha(\infty) = 0$

$$\alpha(x) = \sum_{v \in S} \mathrm{Cor}_k^{k(v)} \big((x - t_v) \cdot r_v(\alpha) \big)$$

(appliquer la formule $\alpha(D) = \dots$

à $f = x - T$ (ou à $\lambda(T-x)$)

Cas particulier $m = 2$, $C = \mathbb{Z}/2\mathbb{Z}$.

$C(-1) = C$.

alors $H^2(k) = \mathrm{Br}_2(k)$

$H^2(K) = \mathrm{Br}_2(K)$.

$r_v(\alpha) \in H^1(k(v)) = k(v)^* / k(v)^{*2}$

$\alpha \in \mathrm{Br}_2(K)$ est déterminé (à l'addition près d'un élt de $\mathrm{Br}_2(k)$) par ses <u>résidus</u>

Détermination explicite de α à partir de ses résidus

e.g pôles tous rationnels sur k, $\neq \infty$.

$\alpha(\infty) = 0$

$\lambda_1, \dots, \lambda_n \in k$ distincts

$r_1, \dots, r_n \in k^*$ (mod carrés).

$\alpha(x) = \sum (x - \lambda_i) \cdot (r_i)$ $\quad x \in k,\ x \neq \infty, \lambda_1, \dots, \lambda_n$

$\alpha = \sum (T - \lambda_i)(r_i)$: somme de symboles explicites.

pôles pas ts rat^t, e.g : 1 pôle quadratique.

k'/k. $(x)(y) \in B_2(k')$. $x, y \in k'^*$

Comment écrire $\mathrm{Cor}_k^{k'}(x)(y)$ comme comb lin de symboles $x_i, y_i \in k^*$?

ça peut se faire, v. article Bass-Tate K-théorie de Milnor

e.g α, pôles $\{\sqrt{2}, -\sqrt{2}, 3\}$ en 3, résidu $= -1$ (pr faire marcher formule des résidus).

$k = \mathbb{Q}$, $\alpha(\infty) = 0$

résidus ds $\mathbb{Q}(\sqrt{2})$

e.g ("au hasard") $r = 1+\sqrt{2}$ = "$1+t$"

conjugué $r' = 1-\sqrt{2}$

norme $rr' = -1$

$1+\sqrt{2}$: eqn

on écrit $(t^2-2, 1+t) = \gamma$

pole de γ en $t^2 = 2$: bon résidu

en $t = -1$: résidu -1.

pose $z = \frac{1}{t}$, $\gamma = (1-2z^2, z(1+z))$

$\alpha + \gamma$: poles en 3 : résidu -1

-1 : res. -1

$\alpha + \gamma = \gamma(\infty) + (-1, t-3) + (-1, t+1)$

$\Rightarrow \alpha = (t^2-2, 1+t) + (-1, (t-3)(t+1)) + \mathrm{cste}$

pr déterminer la cste : calculer en 1 pt connu : ∞

calcul de $\gamma(\infty)$:

calcul d'un symbole en un pole apparent, $z = 0$

$\gamma = (1-2z^2, z) + \underbrace{(1-2z^2, 1+z)}_{\to 0}$

comment calculer $(z, 1+\varphi(z))$ en termes de φ sachant $d^\circ \geq 1$ i.e divisible par z.

$1-2z^2 \sim (1-2z^2)(1+2z+z^2)$ mod carré.

$= 1+2z-z^2-4z^3-2z^4$

or $(x, 1-x)=0$ (c'est une forule !)

d'où $(1+2z-z^2\cdots, -2z+z^2+4z^3+2z^4)=0$

$$\ddot{=}\ z(-2+z+4z^2+2z^3)$$

d'où, exp cherchée $=(1+2z-z^2\cdots, -2+z+\cdots)$

$=1$ pr $z=0$.

!

ça donne cote $=0$.

Questions

pr $\mathbb{Q}(T)$: Y-a-t-il un entier N t.q tt elmt de $Br_2(\mathbb{Q}(T))$ soit somme de N symboles si oui, quel est le meilleur ? (x_i, y_i)

$N=1$: non. tt elmt n'est pas un symbole

$N=2$???

e.g : L'élément $\alpha=(a,b)+(c,T)$ où $a,b,c\in k^*$. c non-carré.

Si l'alg de quaternions (a,b) est décomp par $k(\sqrt{c})$ alors $\exists d\in k^*$ t.q $(a,b)=(c,d)$

et donc $\alpha=(c,dT)$.

Thm : Si $k(\sqrt{c})$ ne décompose pas (a,b), alors α n'est pas un symbole (est la somme de 2 symb

forme norme de l'alg de quat (a,b) $\langle 1,-a,-b,ab\rangle$

Critère d'Albert : Pour que $(a,b)+(c,d)$ $(a,b,c,d\in k^*)$ soit un symbole, il faut et il suffit que la forme quad $f_6=\langle -a,-b,ab,c,d,-cd\rangle$ représente 0 (soit isotrope).

appliquons le critère d'Albert :

$$\langle -a, -b, ab, c, T, -cT\rangle$$
$$= \langle -a, -b, ab, c\rangle \oplus T\langle 1, -c\rangle .$$

or : lemme : g_1, g_2 anisotrope sur k $\Rightarrow g_1 + Tg_2$ est anisotrope sur $k(T)$.

or : $k(\sqrt{c})$ ne décompose pas (a,b),
on ne peut pas plonger $k(\sqrt{c})$ ds l'alg de quat,
et $\langle -a, -b, ab, c\rangle$ est anisotrope,
et $\langle 1, -c\rangle$ anisotrope car c non-carré.

pf du critère d'Albert

Si f_6 repr $0 \overset{?}{\Rightarrow} (a,b) + (c,d)$ est un symbole

$\Updownarrow$

$H_{a,b} \otimes H_{c,d} \simeq H \otimes M_2$

alg centrale simple.

si pas symbole, $H_{a,b} \otimes H_{c,d}$ est un corps gauche.

$\Rightarrow \exists\, e \in k^*$
représenté à la fois par $\langle -a, -b, ab\rangle$
et par $\langle -c, -d, cd\rangle$

(en gal : $g_1 \oplus g_2$ repr 0, rang $g_i \geq 1$
$\Leftrightarrow \exists\, e \in k^*$ représenté à la fois par g_1 et par $-g_2$

$\Leftarrow$:

$\Rightarrow g_1(x_1) + g_2(x_2) = 0$ si $g_1(x_1) = 0$, repr. tt.
$\Rightarrow$ on prend un élmt t.q $g_2(x_2) \neq 0$, et x_1 t.q $g_1(x_1) = \cdots$

$\Rightarrow k(\sqrt{e})$ décompose (a,b)
$\Leftrightarrow (a,b) = (e,f)$
et $k(\sqrt{e})$ déc $(c,d) \Leftrightarrow (c,d) = (e,g)$.
$\Rightarrow (a,b) + (c,d) = (e, fg)$.

$(\Leftarrow)$ $(a,b)+(c,d)=(e,f)$

soit $k' = k\sqrt{e}$

$(a,b) = (c,d)$ sur k'

$\Rightarrow (-a,-b,ab) \simeq (-c,-d,cd)$ sur k'

sur k', $f_6 = \varphi_3 \oplus -\varphi_3$ où φ_3 forme de rg

$\simeq$ forme hyperbolique de rang 6.

et on a supposé f_6 anisotrope

$\Rightarrow f_6 \simeq_k \psi_3 \otimes \langle 1, -e\rangle . \simeq \langle d_1, -ed_1, d_2, -ed_2, d_3, -ed_3\rangle$

$\mathrm{discr}(f_6) = -e \in k^*/k^{*2}$.

or discr $f_6 = -1$ mod carrés (par $f_6 = \langle -a,-b,ab,c,d,-cd\rangle$)

$\Rightarrow e = 1$: e est un carré. $\Rightarrow k' = k$.

$\Rightarrow ab = cd$

$\vdots$

$\Rightarrow f_6$ repr 0. $\square$.

<u>autre explication du <u>critère</u> d'Albert "à la Tits"</u>

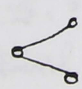
$\alpha = (a,b)+(c,d)$ $\alpha \in \mathrm{Br}_2(k)$

$\downarrow$

f_6 : forme à 6 vbles

(f_6 est déterminé par α au prod près par un élt de k^*)

A_3 :  $\leftrightarrow SL_4$

D_3 :  $\leftrightarrow SO_6$

$\downarrow$

μ_2 $(H^1(\mu_2) = k^*/k^{*2})$

$\downarrow$

$PGL_2 = SL_2/(\pm 1)$

$SL_2/\{\pm1\} \times SL_2/\{\pm1\} \xrightarrow{\otimes} SL_4/\{\pm1\} \xrightarrow[\text{par comparaison des dim.}]{\Lambda^2} SO_6$ (de la forme quad déployée $\langle 1,-1,1,-1,1,-1\rangle$ disc $=-1$)

(a,b) $\quad$ (c,d)

$\in H^1_a(k, SL_2/\{\pm1\})$

$\alpha \in PSL_4 = SL_4/\mu_4$

$\longmapsto \in H^1(\;) \subset \mathrm{Br}_4 \longrightarrow \in H^1(SO_6)$

$\simeq$ f quad à 6 v de disc -1

appl $Sl_4 \to SO_6$:

V de dim 4 , $e \in \Lambda^4 V$ fixé, $\neq 0$.

$\Lambda^2 V \times \Lambda^2 V \longrightarrow \Lambda^4 V \simeq k$

dim 6

$\star$ Propriété d'un corps k ("hamiltonien"?)

(H) si $a, b, c, d \in k^*$
alors $(a,b) + (c,d)$ est un symbole
i.e : la forme $\langle a, -b, ab, c, d, -cd \rangle$ est isotrope.

$\Longleftrightarrow$ (Merkurjev) tt elmt de $Br_2(k)$ est de la forme $(a)(b)$
$a, b \in k^*$.

e.g : corps locaux $\mathbb{Q}_p$ (corps res. fini)
corps globaux : corps de nbres
corps de fct d'un vble
sur corps fini.

(H) $\Leftrightarrow$ tte forme quad non-dégen de rang 5 et de discr. 1, représente 1.

pf ($\Rightarrow$) : q_5 repr 1 $\Leftrightarrow$ $q_5 \oplus \langle -1 \rangle$ repr 0
i.e $q_6 = \langle x_1, x_2, x_3, x_4, x_5, -1 \rangle$ repr 0?
(avec $x_1 x_2 \cdots x_5$ carré).

montrer $\exists\, \lambda, a, b, c, d$
t q $q_6 \simeq \lambda \langle -a, -b, \ldots \rangle$.

on a $q_6 \sim \langle \lambda x_1, \lambda x_2, \lambda x_3, \lambda x_4, \lambda x_5, -\lambda \rangle$

$\lambda x_1 = -a$, $\lambda x_2 = -b$, $\lambda x_3 = ab$ en posant $\lambda = x_1 x_2 x_3$
$-a = x_2 x_3$
$-b = x_1 x_3$

on ~~pose~~ $d x_4 = c$, $d x_5 = d$

est-ce que $-d = -cd$?

par calcul des discr :

$$x_1 x_2 x_3 = d^2 x_4 x_5 \quad \text{mod carrés.}$$

OK.

$(\Leftarrow)$ $\langle c, d\rangle \otimes \langle -a, \dots, -cd\rangle$, ok.

Calcul et assassinat des symboles

on veut "tuer" les élmts de $Br_2 K$ (obstruction)

où k infini où $K = k(T)$.

situation : $\alpha \in Br_2(K)$ (symbole ou somme de symboles),

e.g chercher des pts $x \in \mathbb{P}_1(k)$, x non-pôle,

où $\alpha(x) = 0$ ds $Br_2(k)$.

<u>Question</u> S'il existe un $x \in \mathbb{P}_1(k)$ où α s'annule, en existe-t-il d'autre ? ~~une~~ infinité ? Card k ?

pas connu m̂ sur $\mathbb{Q}$.

on va parler des conjectures associées à cette question.

Changement de base

e.g : α ayant 2 pôles rat$/k$

supposons ces poles sont $0, \infty$,

de résidu $r \in k^*/k^{*2}$ (le m̂ par foule résidus)

et que $\alpha(1) = 0$.

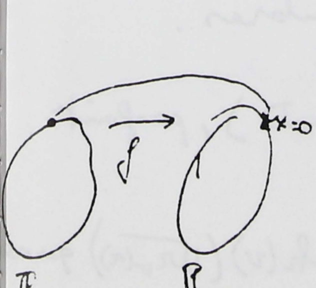
alors $\alpha = (r, T)$. (a les bons poles et 0),

Si on force T à être un carré, α devient 0.

$$f : \mathbb{P}_1 \longrightarrow \mathbb{P}_1 \qquad k(T) \hookrightarrow k(U)$$
$$U \longmapsto T = U^2$$

$f^*(\alpha) = 0$ ds $Br_2(k(U))$.

et $\operatorname{Im} f$ est un ens de pts rat s/lequel α est 0.



<u>Question</u> : soit $\alpha \in Br_2(k(T))$,

soit $x \in \mathbb{P}_1(k)$ avec $\alpha(x) = 0$,

Existe-t-il $f : \mathbb{P}_{1,U} \longrightarrow \mathbb{P}_{1,T}$ non-cst

t.q (1) $f^*(\alpha) = 0$ $\;Br_2(k(U))$: α tué ds corps de fcts du $\mathbb{P}_1$ à g

et (2) $x \in f(\mathbb{P}_1(k))$.

Supposons (2) satisfaite. Alors (1) équivaut à :

(1') : les résidus de $f^*(\alpha)$ sont tous nuls.

i.e v pôle de α, $k(v)$

$$r_v(\alpha) \in k(v)^*/k(v)^{*2}$$

soit w place de $\mathbb{P}_1$, v t.q $f(w)=v$.

soit $e_{w/v}$ l'indice de ram.

$$r_w(f^*\alpha) = e_{w/v}\cdot(r_v(\alpha))$$

r vu ds $k(w)^*/k(w)^{*2}$.

la condition $r_w(f^*\alpha)=0$

$k(v)(\sqrt{r_v(\alpha)})$ | $k(v)$

équivaut à : ou bien $e_{w/v}$ est pair.

ou bien $r_v(\alpha)$ devient un carré ds $k(w)$

i.e $k(w) \supset \sqrt{r_v(\alpha)}$.

<u>Résultats</u>

(1) <u>Janchevski</u> : la question ci-dessus a une réponse positive si $k=\mathbb{R}$ ou si k est hensel[ien] (e.g corps local)

(2) <u>Mestre</u> : réponse positive si $\sum_{v \in \text{pôles de } \alpha} \deg(v) \leq 4$

(3) <u>Mestre</u> : ~~réponse~~ existence de f t.q $f^*(\alpha)=0$ (~~mais~~ peut-être pas $x \in f(\mathbb{P}_1(k))$.

si $\sum_{v \text{ pôle de } \alpha} \deg(v) \leq 5$ et k satisfait à (H)

e.g k est un corps de nombres.

pf de (1) k hensélien (e.g complet pr une val discrète), parfait.

α symbole, S pôles, $\alpha(\infty)=0$.

pr $v \in S$ on a $k(v)$ ext finie de k, et $k(v)(\sqrt{r_v(\alpha)})$ qua[dratique]

soit k' ext gal finie de k contenant tous les corps $k(v)(\sqrt{r_v(\alpha)})$

soit $n = [k' : k]$.

$k' = k(y)$, P poly min de y.

$P(t) = t^n + \lambda_1 t^{n-1} + \dots + \lambda_n \quad \lambda_i \in k$

$f : \mathbb{P}_{1,U} \longrightarrow \mathbb{P}_{1,T}$

on prend $f_N = P(U) \cancel{/} \pi^N$ où π unif, N assez gd.

<u>lemme</u> : f_N a les propriétés (1) et (2) pr tt N assez grand

4
$$\begin{array}{c} w \\ \downarrow ? \\ v \in S \\ \uparrow \\ t_v \in k(v) \end{array} \qquad P(U) = \pi^N t_v \xrightarrow[N \to \infty]{} 0$$

lemme de Krasner : corps hensélien :
les équs voisines d'une est irr
définissent le m corps.

on aura $k(w) = k'$, sur laquel le
résidu est trivial : $r_v(a)$
est un carré.

$\square$.

2 décembre 91 cours 7

$1^{\text{ère}}$ heure : thms de Mestre pr tuer des elts de Br_2

k corps, car $\neq 2$, infini (essai de généraliser à k fini)

$\alpha \in Br_2\, K(T)$

S = ens des pôles de $\alpha \subset \mathbb{P}_{1/k}$

hypothèses :

① $\deg S \leq 4$ $\left(\deg S = \sum_{v \in S} \deg(v)\right)$

② $\infty \notin S$ et $\alpha(\infty) = 0$

Théorème (Mestre$_4$)

Il existe un morphisme $f : X \to \mathbb{P}_1$ dominant, où $X \cong \mathbb{P}_1$, avec

1 - $f^*(\alpha) = 0$

2 - Il existe $x \in X(k)$ (i.e pt. rat.) avec $f(x) = \infty$.

3 - $\deg f = 8$

(pas canon, bcp de choix.

Mestre$_5$: pr $\deg S \leq 5$, on peut obtenir 1 : $f^*(\alpha) = 0$.

2 méthodes : 1 explicite, 2 courbes elliptiques.

Methode explicite

on a fixé pt base : ∞.

agrandir $S :=$ poles $\cup \{Q_1, \ldots, Q_n\}$, $Q_i \in \mathbb{P}_1(k) - \infty - S$

t.q $\deg S = 4$ (on aura $\operatorname{Res} Q_i = 0$, ou non nul)

$S \longleftrightarrow P = T^4 + a_1 T^3 + a_2 T^2 + a_3 T + a_4$.

S = ens des zéros de P

résidus : pr chaque pt de S, un elt du corps residuel mod carrés

ou : on prend $k(S) := k[T]/(P)$ base : $1, T, T^2, T^3$

$\operatorname{Res}_S(\alpha) = r \in k(S)^* / k(S)^{*2}$

on peut représenter r par $R(T)$: poly de degré ≤ 3.

R est défini au remplacement près par $RW^2 \pmod P$

où W est inversible mod P.

lemme : les R correspondant à r sont dense pr la top de Zariski ds l'esp. des polys de deg. ≤ 3 (vus comme esp. affine de dim 4 sur k).

<u>Dem</u> $G := \prod_{S/k} \mathbb{G}_m$ or $X \mapsto X^2$ surjectif.
gpe mult de l'esp affine $\Rightarrow$ dense.

on peut donc éviter les relations générantes en remplaçant. □

Choisissons R : $\begin{cases} P(T) = T^4 + a_1 T^3 + \dots \\ R = r_0 T^3 + \dots \end{cases}$

$$P(T) + X^2 R(T) = T^4 + (a_1 + r_0 X^2) T^3 + \dots$$
$$= \underbrace{\left(T^2 + b_1(X^2)T + b_2(X^2)\right)^2}_{\text{"racine carrée formelle"}} + \underbrace{b_3(X^2)T + b_4(X^2)}_{\text{"reste"}}$$

si $b_3(X^2) \neq 0$, on pose $f(X) = -\dfrac{b_4(X^2)}{b_3(X^2)}$.

t pr corps finis — A démontrer : si R est assez général (i.e. on évite certaines rel,
on a : $\deg b_4 = 8$ (deg. en X) $\deg b_4(X^2) = 4$, $\deg b_3(X^2) = 3$.
$\deg b_3 = 6$ b_3, b_4 premiers entre eux

f tue α : $f^*(\alpha) = 0$.

on a 2 morceaux $\mathbb{P}_1 \xrightarrow{X^2} \mathbb{P}_1 \xrightarrow{f} \mathbb{P}_1$

on a bien f : deg 8 , $\infty \mapsto \infty$: pt rationnel.

pourquoi $f^*(\alpha) = 0$?

on a changé vbles : $T = -\dfrac{b_4(X^2)}{b_3(X^2)}$

$X \xrightarrow{f} \mathbb{P}_1$

clair : res $f^*(\alpha) = 0$

regarder pts au-dessus des zéros de P, $R(T)$.

on a écrit : $\square \times R = \square \Rightarrow R$ est un carré.

Méthode à courbes elliptiques.

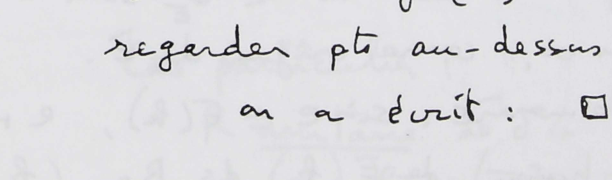
Points sur les C.E. (v. Euler)

methode classique $Y^2 = P(T)$ P de deg 4, unitaire

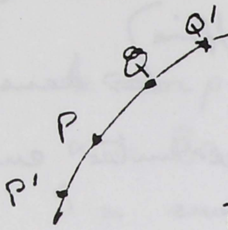
éclate à l'∞ en 2 branches, 2 pts rationnels

$Y = T^2 + \dots$

$Y = -T^2 + \dots$



pr trouver d'autres pts rats : symétriques.

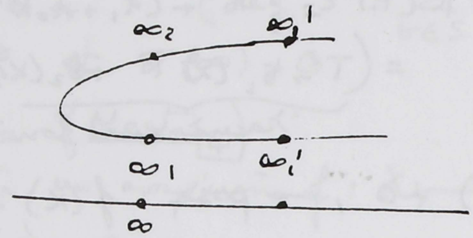


symétriques des pts ∞_i, on trouve 2 autres pts rats (au-dessus d'un m^ pt).

$$P(T) = T^4 + \dots = (T^2 + \dots)^2 + cT + d$$

$T = -\frac{d}{c}$: pt rat

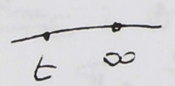
(on continue, si ce n'est pas un pt d'ordre fini on obtient ∞ de pts rats)



<u>Énoncé + général</u> :

courbe E, tq. $\infty \in \mathbb{P}_1(k)$ est image de 2 pts rationnels $\infty_1, \infty_2 \in E(k)$.

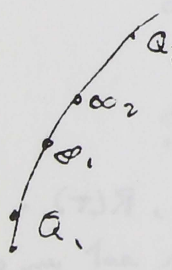
$f \mid \deg 2$.



$\mathbb{P}_1$ soit $t = -\frac{d}{c}$ (au-dessus duquel on a aussi des pts rats.).

<u>Thm</u> Soit $\alpha \in Br_2\, k(T)$. Supposons $\alpha(\infty) = 0$ et que les résidus de $f^*(\alpha)$ soient 0. Alors $\alpha(t) = 0$.

<u>Dém</u> Utilise props de corps de fcts.



$$\alpha_E = f^* \alpha$$

par hyp : les résidus de α_E sont 0, et $\alpha_E(\infty_1) = 0$

Choisissons ∞_1 comme origine de E.

on avait démontré : si $e \in E(k)$, $e \mapsto \alpha_E(e)$ est un <u>homom</u> de $E(k)$ ds $Br_2(k)$.

de plus ∞_2 est aussi au-dessus de 0. $\alpha_E(\infty_2) = 0$

donc $\alpha_E(-\infty_2) = 0$ mais, si ∞_1 est l'origine,

$-\infty_2 = Q_1$ (symétrique de ∞_2 % ∞_1)

d'où $\alpha_E(Q_1) = 0$
$= \alpha(t)$.

(en fait : C.E. sur $k(X,T)$?). □

Pour $\deg S = 5$

Hypothese sur k : (H) : formes quad de rang 6, det -1 représentent 0

($\iff$ si $a, b, c, d \in k^*$, alors $(a,b)+(c,d)$ est égal à (e,f), avec $e, f \in k^*$

(i.e Σ symboles est un symbole)

Thm (Mestre$_5$) On suppose que k satisfait à (H)
soit $\alpha \in Br_2\, k(T)$ t.q $\deg S = 5$ et $\alpha(\infty) = 0$.
Il existe alors $f : \mathbb{P}_1 \to \mathbb{P}_1$, non-constant,
t.q $f^*(\alpha) = 0$.

(pas sûr qu'on couvre ∞)

Dem : S = zeros d'un poly de deg 5.
résidus représentés par R de $d^\circ 4$ (ou ≤ 4, mais mod $\square$, $\Rightarrow$ on peut prendre deg 4).
il faut utiliser fmle des résidus.
Si $S = \{P_1, \ldots P_5\}$: 5 pts rat.
$\prod_{i=1}^{5} R(P_i)$ est un carré : fmle des résidus.
en gal : $k(S) := k[T]/(P)$.
fmle des résidus : $N_{k(S)/k}\, R \in k^{*2}$.

Cas particulier :
R unitaire de $d^\circ 4$: $R = T^4 + r_1 T^3 + \cdots$
$R = (T^2 + \underbrace{\tfrac{r_1}{2}}_{b_1} T + b_2)^2 + b_3 T + b_4$.

Lemme : Si $t \in k$ est t.q $b_3 t + b_4 = 0$,
alors $\alpha(t) = 0$.
(= cas particulier de l'argument p/ courbes ell, $Y^2 = R(T)$ à laquelle on applique lemme gal).

~~On regarde V = variété dans Aff^5 (a poly de d° ≤ 4 en T)~~.

Choisissons R_0 un poly représentant le résidu de α (pas forcément unitaire)

$R_w = R_0 w^2 \pmod{P}$ où W : poly de d° ≤ 4

soit $\mathcal{W}$: la var. des W t.q R_W soit unitaire de d° 4.

$w \in \mathcal{W}(k') \longmapsto t(w) \in k'$ appl. rationnelle

k' : ext de k où $t(w) = -\dfrac{b_4(w)}{b_3(w)}$

On a $\alpha(t(w)) = 0$.

$\mathcal{W}$ est une quadrique affine dans Aff^5 (défini par forme quad = 1)

on a donc défini $\mathcal{W} \overset{F}{\dashrightarrow} \mathbb{P}_1$: appl rat

$w \longmapsto t(w)$

avec $F^*(\alpha) = 0$

on applique ça au pt gen (d'où le k')

<u>Lemme</u> : (H) ⇒ : la quadrique $\mathcal{W}$ a un pt rat.

(d'où : $\mathcal{W}$ est ≃ variété k-rat.

ça termine le thm (mais ⚡ : on ne voit pas si ∃ pt d'image ∞)

<u>Dem du lemme</u>. $\mathcal{W}$, W un poly de d° 4, $R_0 W^2$.

$\lambda : k(S) \longrightarrow k$ $\quad k(S)$: base $1, T, T^2, T^3, T^4$

$G \longmapsto$ coeff de T^4 ds G.

$\mathcal{W} = \{ W \mid \lambda(R_0 W^2) = 1 \}$

$\lambda(R_0 W^2)$ est une forme quad non-dégén en 5 vbles.

<u>Lemme</u> : son discriminant est 1 (mod carrés)

alors : $q \oplus \langle -1 \rangle$ représente 0, forme à 6 vbles de discr. -1.

<u>Dem du lemme</u> $A := k(S)$, de rang 5 sur k.

$= k[T]/(P(T))$ algèbre étale.

calcul du discriminant. (Euler? corps locaux

$\lambda(G) = \mathrm{Tr}\left(\dfrac{G}{P'(T)}\right)$ (par calcul)

et $q(W) = \mathrm{Tr}\left(\dfrac{R_0}{P'(T)} W^2\right)$

en g^{al}, A algèbre étale, $a \in A^*$, $w \mapsto \mathrm{Tr}(a w^2)$

a pour disc r $= \left(N_{A/k}\, a\right) \cdot \mathrm{disc}(A)$.

calcul... $\mathrm{disc}\, q = \mathrm{disc}(P) \cdot \dfrac{1}{NP'(T)}$ $= 1$ mod carrés

par formule des résidus : $N R_0 = 1$

$NP'(T) = (-1)^{\frac{n(n-1)}{2}} \mathrm{disc}\, P$

$= \mathrm{disc}\, P$. $(n=5)$.

$\square$.

N.B : si $\alpha = (x)(y) = (x, y)$ est un seul symbole $x, y \in k(T)^*$.

interprétation par fibré en coniques $Y \to \mathbb{P}_1$

$Z^2 - x X^2 - y Y^2 = 0$

trouver $\mathbb{P}_1 \to \mathbb{P}_1$ surj qui tue α

$\Updownarrow$

Y est k-unirationnel.

$$\begin{array}{ccc} Y_1 & \to & Y \\ \downarrow & & \downarrow \\ \mathbb{P}_1 & \to & \mathbb{P}_1 \end{array}$$

Application à la construction d'extensions galoisiennes de $\mathbb{Q}(T)$.

<u>1er cas</u> (thm hypothétique : hypothèses rarement satisfaites)

Thm k de car 0, t.q le pb $(*)$: $\forall \alpha \in \mathrm{Br}_2\, k(T)$

$(*)$ $\left\{\begin{array}{l} \text{et } \forall\, t \text{ pt rat } \in \mathbb{P}_1(k) \text{ avec } \alpha(t) = 0, \\ \exists\, f : \mathbb{P}_1 \to \mathbb{P}_1 \text{ non-cst, qu}^t\ q f^*(a) = 0 \\ \quad \text{et } t \in f(\mathbb{P}_1(k)) . \end{array}\right.$

ait tjs une solution, <u>alors</u> :

si G est un 2-groupe, il existe une <u>ext gal-régulière</u> $L / k(T)$, de gpe de Galois G, avec un <u>"pt-base"</u> (i.e un pt rat de $\mathbb{P}_1$, i.e une place de d° 1 de $k(T)$, non ram et complètement décomposée dans L).

Pour $k = \mathbb{Q}$.

Question : pr n'importe quel gpe G, est-ce possible ?
pas de contre-exemple ; peu d'exemples
(rigidité donne rarement pt-base)
pas d'exemples à pt-base pr G sporadiques.
($\hat{m}$ pas t.q. pts au-dessus soient reels : ttes les ext connues ont pts complexes).

N.B : Si $L / k(T)$ vérifie ces cond, $\exists\, L'/k(T)$ vérifiant les $\hat{m}$ cond (pr le $\hat{m}$ gpe G) et t.q. le genre de tt corps K, $L' \supset K \supset k(T)$, $K \neq k(T)$ soit ≥ 1 (ou $\geq n$ donné).
i.e genre de courbe correspondant.

pour ce :
$$\begin{tikzcd} X_F \arrow[r, dashed] \arrow[d, dashed, "G"'] & Y \arrow[d, "G"] \\ \mathbb{P}_1 \arrow[r, "f"] & \mathbb{P}_1 \\ \infty \arrow[u, phantom, "\in" rotate=90] \arrow[r, mapsto] & \infty \arrow[u, phantom, "\in" rotate=90] \end{tikzcd}$$

certains courbes ont $g = 0$, on les évite en changeant de vble pr augmenter la ramification pr les corps intermédiaires

0 non-ram ds Y

prendre $f(x) = x^N$

Dem du th :

① : G ~~ab~~ élémentaire de type $(2, 2, \dots, 2)$
Soient $P_1, \dots, P_r$ des polys unitaires de degré pair ≥ 4, premiers entre eux.
$L = k(T)(\sqrt{P_1}, \dots, \sqrt{P_r})$.

② G non élémentaire. Récurrence sur $|G|$
$G^* := \mathrm{Fratt}(G) = \bigcap (\ker(G \to \{\pm 1\}))$ $\quad G^* \neq 1$.
alors G/G^* est élémentaire de type $(2, \dots, 2)$.
$\exists\, x \in G^*$, $x^2 = 1$, $x \neq 1$, $x \in Z(G)$: centre.
alors $1 \to \underset{\{1, x\}}{\overset{\parallel}{C_2}} \to G \to G' \to 1$

$G' = G/C_2$

$$\begin{tikzcd} Y' \arrow[d, dash, "G'"] & \text{décomp} \arrow[d] \\ \mathbb{P}_1 & \infty \end{tikzcd}$$

par hyp. de récurrence, on sait construire L' pr G'.

on veut étendre à L

on se heurte à $\alpha \in H^2(k(T))$.

$$\begin{tikzcd} L' \arrow[d, dash, "G'"] \\ k(T) \end{tikzcd} \quad G$$

soit $u \in H^2(G')$ l'élément correspondant à l'extension de G' par C_2 qui donne G.

$u \mapsto \alpha \in H^2(k(T)) = Br_2(k)$.

$\alpha(\infty) = 0$.

Par l'hypothèse faite sur k, $f^*(a) = 0$

$\infty \mapsto \infty$

$$\begin{tikzcd} Y'' \arrow[r, dashed] \arrow[d, dash, dashed] & Y' \arrow[d, dash, "G'"] \\ \mathbb{P}_1 \arrow[r, "f"] & \mathbb{P}_1 \\ \infty \arrow[r, mapsto] & \infty \end{tikzcd}$$

et les corps intermédiaires sont de genre ≥ 1. évite décomposition donc ext lin disjointe

$$\begin{tikzcd} L \arrow[d, dash, "C_2"] \\ L' \arrow[d, dash, "G'"] \\ k(T) \end{tikzcd} \quad G$$

On peut supposer $\alpha = 0$: obstruction liquidée.

donc $\mathrm{Gal}(K_s/K) \xrightarrow[\text{surject}]{} G'$ se relève

$$\begin{tikzcd} & G \arrow[d] \\ \mathrm{Gal}(K_s/K) \arrow[ur] \arrow[r] & G' \end{tikzcd}$$

$G_1 \subset G$, image de $\mathrm{Gal}(K_s/K)$.

Par les propriétés du Frattini, $G_1 = G$

c'est surject.

il faut encore arranger ∞ pr qu'il soit complètement décomp ds L (pas de ram ni d'inertie de L' à L).

or relèvement de $\mathrm{Gal}(K_s/K) \to G'$ est défini à mult. près par $\mathrm{Gal}(K_s/K) \to C_2$,

i.e un caractère quadratique ε de $K = k(T)$

$\varepsilon \leftrightarrow k(\sqrt{T})/k(T)$

ça marche bien
sur corps de nbres:
y a d'autres places
ds sur corps locaux.

si ramifié : $\begin{matrix} L \\ | \\ L' \end{matrix}$ $\begin{matrix} k(\sqrt{a}) \\ | \\ k \end{matrix}$: on prend $\varepsilon \leftrightarrow k(\sqrt{a})$.

□.

Le thm n'a pas d'applications :
pr les cas $k = \mathbb{R}$, $\mathbb{Q}_p$, on avait ut.

Prochaine fois : $SL_2(\mathbb{F}_7)$, $6A_6$, $6A_7$

9-12-91 – Construction par Mestre d'extensions régulières de $\mathbb{Q}(t)$ de groupe de Galois G avec (107)

$$G = \begin{cases} SL_2(\mathbb{F}_7) & \text{(Mestre, non publié)} \\ \tilde{G} \cdot A_7 & \\ \tilde{G} \cdot A_7 & \end{cases}$$

Cas $SL_2(\mathbb{F}_7)$ $\qquad SL_2(\mathbb{F}_7)/_{\pm 1} \simeq PSL_2(\mathbb{F}_7) \simeq SL_3(\mathbb{F}_2)$

groupe simple d'ordre 168.

On construit des extensions à groupe $PSL_2(\mathbb{F}_7)$, pb. de plongt quadratiq.

Construction de La Macchia : $P_a(X) = X^7 + \ldots$

$Q_a(X) = X^3(-1)$

par $P_a - TQ_a$ $\quad$ T indét.

3 pour ex. de degré 7 de $\mathbb{Q}(a, T)$ par $P_a - TQ_a = 0$ est $PSL_2(\mathbb{F}_7)$

$\overset{3}{\infty}$ ① ⓪ $\quad \mathbb{P}_{1,x}$

$\varphi \downarrow$ $\qquad T = P_a(x)/Q_a(x)$ revêt^t de degré 7, à fibre générique

∞, ∞ $\quad \mathbb{P}_{1,x}$

il y a 4 pts de ram. avec ram. d'ordre 2

1 pt de ramif avec ram. ordre 3

Soit $a \in \mathbb{Q}$, ext. non dégénérée, $K = \mathbb{Q}(T)$ $\quad \mathrm{Gal}(\bar{K}/K) \longrightarrow PSL_2(\mathbb{F}_7)$

peut-on relever ?

$$\begin{array}{ccc} & ? & SL_2(\mathbb{F}_7) \\ & \nearrow & \downarrow \\ \mathrm{Gal}(\bar{K}/K) & \longrightarrow & PSL_2(\mathbb{F}_7) \end{array}$$

$\alpha \in H^2(K, C_2)$ obstruction au relèvement invariant de Hasse-Witt de la forme $\mathrm{Tr}(X^2)$, mais pas besoin de calculer :

α a au plus 4 pôles (+ exact. degré (4 pôles) ≤ 4)

On utilise le Th. de Mestre pour tuer α. On doit chercher une valeur $a \in \mathbb{Q}$, $t \in \mathbb{Q}$ telles que α_a s'annule au point t. On en connaissait (tests sur machine : Mestre, Malle $a = 4?$, $t = 0?$)

il semble difficile de faire autrement qu'utiliser la machine.

Mais alors, on peut trouver, une copie $\mathbb{P}_{1,T'} \xrightarrow{f} \mathbb{P}_{1,T}$

avec $\deg(f) = 8$, $f^*(\alpha) = 0$, couvrant le point base. $t = f(t')$

vérifier que les extensions sont disjointes

il n'y a plus d'obstruction de L'/k'

$$\begin{array}{ccc} L' & & \\ | & \searrow & L \\ & & |\, G/\pm 1 \\ K' & \searrow & K \end{array}$$

On peut donner les équations.

Second cas. extension centrale de A_6 par C_6.

Th. d'ext. c'est $\alpha_2 \in H^2(K, C_2)$ $\quad \alpha_3 \in H^2(K, C_3)$

Pr. Construit une ext. de $K = \mathbb{Q}(T)$ à ram. d'ordre 2 et 5.
à groupe A_6.

$\mathbb{P}_{1,X}$
$\downarrow$
$\mathbb{P}_{1,T}$

$T = P(X)/Q(X)$ $\quad$ P polynôme de d° 6

Q ——— d° 5

tel que $P'Q - PQ' = R^4 S$ où R et S polynômes quadratiques

donnera 2 pt. avec ram. ordre 5 et 2 pt. avec ram ordre 2.

Hyp. dégénérescence. $(R, S) = 1$, & les T corresp aux ram sont distincts)

$P(X) = X^6 + a_1 X^4 + a_2 X^2 + a_3$

$Q(X) = X(X^4 + b_1 X^2 + b_2)$

$R(X) = X^2 + c$, $\quad S(X) = X^2 + d$

On se donne Q, R, et on essaie de déterminer les coef de P et de S.
(on peut les prendre unitaires car $6-5=1$!!)

- Condition $9b_1^2 + 100 b_2 = \square$.

On obtient un Revêtement avec Groupe de Galois S_6.

ramifié $\begin{array}{l}(1.2) \ \text{2 fois} \\ (1 - - 5) \ \text{2 fois}\end{array}$

1er chang^t de base pour tomber sur A_6

K' a encore genre 0, on cherche dis$(Q) = \square \iff b_2 = \square$.

la fibre de $T = \infty$ formée de ∞, 0 et racines de $X^4 + b_1 X^2 + b_2$.

$$\begin{array}{ccccc} & L & & & \\ & | & & & \\ \mathbb{P}_{1,T'} & K' & \infty_1 & & \infty_2 \\ & \downarrow & & \searrow \swarrow & \\ \mathbb{P}_{1,T} & K & & \infty & \end{array}$$

sur K', la ramification de L est d'ordre 5 en 4 pts (dédoubl^t)

On regarde $\alpha_2 \in H^2(K', C_2)$ et α_3. Comme $(5,2)$ et $(5,3) = 1$
ces éléments n'ont pas de pôle $\Rightarrow$ Constants.

pour les annuler ~~trouver~~ un pt où il s'annullent

Calcul de W_2 avoir $= \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}[x]/x^4+b_1x^2+b_2$). (109)

On s'arrange pour avoir $\alpha_2 = 0$

Pour α_3., en un pt $= 0$ (Groupe de Galois $\subset D_4$)

3ème Cas $G = G A_7$.

On part de $P(x) = x^7 + a_1 x^5 \dots$

$Q(x) = x^4 + b_1 x^2 + b_2$.

$T = \frac{P(x)}{Q(x)}$, $P'Q - Q'P = 3 R^4 S(x)$

On ressent comme précédemment — bien prendre le calcul, il faut être un Mestre en la matière!

$P_{1,x}$

$|$

$P_{1,T}$ — ram. ordre 5 2 fois $(1,2 \dots 5)$; ram. ordre 2 2 fois $(1,2)$; ram $\geq \infty$ 3 1 fois $(1,2,3)$ | faire le calcul du genre. $-2 = 7 \times (-2) + 2 \times 4 + 2 \cdot 1 + 1 \cdot 2$.

Groupe de Galois S_7. (regarder les cycles)

L

$| A_7$ — $K' \simeq \mathbb{Q}(T')$ avec un pt base.

S_7 K'

$| 2$ — Calcul pour α_2, α_3

K — α_2 est C^k (ramif. d'ordre impair), suffit de l'annuler

si invariant de Witt de P est 0. (Calcul sur Machine de Mestre: $P = x^7 + a_1 x^5 + a_2 x^3 + a_3 x$ $a_1 = 1/100$, $a_2 = \frac{24499}{3500}$, $a_3 = -\frac{6125}{25}$

Lemme: $\alpha_3 = 0$

On démontre que en 1 pt de ramifica° d'ordre 3, le # du Groupe de décomposition n'est pas divisible par 9 (en fait D/C_3 2-groupe)

et donc $u \in H^2(A_7, C_3)$ alors $u/_H = 0$ si $9 \nmid |H|$

car Sylow (A_7). 3×3 élément $\Lambda^2(\ )$ sur chacun des sous groupes d'ordre 3

la propriété du groupe de décomposition provient des polynômes impairs

$x \mapsto -x$: $\exists$ élém^t ordre 2 de S_7 qui centralise D.

... en pt de base qui éclate en pts
rationnel – (il aurait fallu $P \in$ racine de $\mathbb{Q}$)

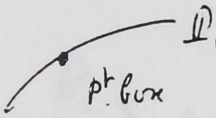
(110)

Si $\begin{array}{c} L \\ \big| \, G \\ \mathbb{Q}(T) \end{array}$ regulier avec P' base

Th. irréd. de Hilbert : $\forall S$ fini de places de $\mathbb{Q}$

$\exists$ $L_S/\mathbb{Q}$ de groupe de Galois où les places de S sont tot. decomposées (place ∞ tot. réelle.

algebre $\mathbb{Q} \to \cdots \to \mathbb{Q}$.



t S-voisin lemme de Krasner algebre attachée à t est decomposée en les places de S on peut ajouter dans irréd. de Hilbert que L_t est un corps

10h40

Annulation de α sur $\mathbb{Q}$

$\alpha \in Br_2(\mathbb{Q})$, ensemble des $t \in \mathbb{P}_1(\mathbb{Q})$, non pôles de α pour lesquels $\alpha(t) = 0$.

exemple $\alpha = (f)(g)$ $f, g \in \mathbb{Q}(T)^*$.

t : conique $X^2 - f(t)Y^2 - g(t)Z^2 = 0$ a un pt. rationnel.

$S_{f,g}$ définie par equa° ci-dessus. $f, (t), g(t) \neq 0, \infty$

$$\begin{array}{c} S \\ \downarrow \\ \mathbb{P}_1 - \{\text{Nbre fini de pts}\} \end{array}$$

surface fibrée en coniques.

image de $\mathbb{P}_1(\mathbb{Q})$ des pts rationnels de S.

Critères pour qu'il y ait de tels points.

- principe de Hasse ?
- approximation faible ?

Resultats et conjectures.

1. Obstruction de Manin. $\alpha \in Br_2(\mathbb{Q}(t))$

decomp. de α en $\alpha = \beta + \gamma$ $\beta, \gamma \in Br_2(\mathbb{Q}(t))$ de pôle disjoints

(decomposition disjointe)

on peut ajouter $\delta \in Br_2(\mathbb{Q})$ $(\beta + \delta) + (\gamma + \delta)$

modulo cette equivalence, il n'y a qu'un nombre fini de decomposition disjointe = partition des pôles + formule des résidus.

on dit que α indécomposable si seul $\alpha = \alpha + 0$ (11)

Question 1? Si α indécomposable le principe de Hasse et approximation faible vrais.

i.e. Hasse: $\forall p \in \mathcal{P}(\mathbb{Q})$ $\exists$ $t_p \in \mathbb{P}_1(\mathbb{Q}_p)$ qui "tue" α dans $Br_2(\mathbb{Q}_p) = \mathbb{Z}/2\mathbb{Z}$ Alors $\exists t \in \mathbb{P}_1(\mathbb{Q})$ avec $\alpha(t) = 0$.

Approxi faible: Si $\exists t$, $\alpha(t) = 0$. Si S ensemble fini de places et $t_p \in \mathbb{P}_1(\mathbb{Q}_p)$, $\alpha(t_p) = 0$ alors $\exists$ suite $t^{(n)}$ $t \in \mathbb{P}^1(\mathbb{Q})$ avec $\alpha(t^{(n)}) = 0$ $t^{(n)} \longrightarrow t_p$ pour S-topologie.

$\alpha = \beta + \gamma$ $\beta + \gamma$ à pôles disjoints, donne des contraintes sur les valeurs p-adiques

Adèle de $\mathbb{Q}$ $\mathbb{P}_1(\mathbb{A}_\mathbb{Q}) = \prod'_p \mathbb{P}_1(\mathbb{Q}_p)$

$\underline{t} = (t_p)$, $\alpha(t_p)$ de $Br_2(\mathbb{Q}_p)$

$H_A = \prod_p H_p$, $H_p = \{t_p \mid \alpha(t_p) = 0\}$, symbole continu ces ensembles sont ouverts et fermés de $\mathbb{P}_1(\mathbb{Q}_p) - \{\text{pôles}\}$.

Soit $H_\mathbb{Q} = \{t \mid \alpha(t)\} = 0$.

Hasse + App. faible = $H_\mathbb{Q}$ est dense de $H_\mathbb{A}$

$\alpha = \beta + \gamma \implies H_\mathbb{A}(\beta, \gamma) \subset H_\mathbb{A}$ $t = (t_p) \in H_\mathbb{A}(\beta, \gamma)$

$\iff t \in H_\mathbb{A}$ et $\sum'_p \mathrm{inv}_p(\beta(t_p)) = 0$.

(pas besoin de regarder γ, valable in v. (formule de Σ dans B_r)

Proposition:

① $H_\mathbb{A}(\beta, \gamma)$ est ouvert et fermé dans $H_\mathbb{A}$

② $H_\mathbb{Q} \subset H_\mathbb{A}(\beta, \gamma)$

Corollaire $\overline{H_\mathbb{Q}} \subset \bigcap_{\alpha = \beta + \gamma} H_\mathbb{A}(\beta, \gamma)$

La conjecture qui remplace Hasse dans le cas général: $H_\mathbb{Q}$ est dense dans l'intersection de $H_\mathbb{A}(\beta, \gamma)$.

Proposition Supposons β et γ à supports disjoints. Alors pour tout p sauf un nombre fini. et $\forall$ $p \in \mathbb{P}_1(\mathbb{Q}) -$ Pôles on a soit $\beta(t_p) = 0$ soit $\gamma(t_p) = 0$.

(112)

<u>idée</u> Lemme Soit $\alpha \in Br_0(?(t))$, pour tout p assez grand, on a

$\alpha(t_p) = 0$ pour tout t_p dont la réduction de $\mathbb{P}_1(\mathbb{F}_p)$ n'est pas la réduction d'un pôle.

(Résulte de formule explicite avec la co-restriction)

D'où la nécessité des pôles disjoints.

Soit S ensemble fini tel que la prop. s'applique si $p \notin S$.

Soit $p \notin S$; $t = (t_p) \in H_A \rightarrow \beta(t_p) = 0$

donc $H_A(\beta, \gamma) = \{ \underset{(t_p)}{t} \in H_A \mid \sum_{p \in S}' \mathrm{inv}_p(\beta(t_p)) = 0 \}$

D'où ouvert et fermé.

<u>Rem</u> La proposition est toujours fausse si le supports pas disjoints.

<u>Ex</u> $\alpha = (f)(g)$ $V_{f,g}$ surface associé, compactifié

$$\begin{array}{ccc} 0 & & V_{f,g} \\ \uparrow & & \downarrow \\ \alpha & & \mathbb{P}_1 \end{array}$$

β et $\gamma \longmapsto$ classe de Br_2 (corps des fct. de $V_{f,g}$) non ramifié.

donc $\in Br_2$ (variété $V_{f,g}$ sens de Groth.) modulo $Br_2(\mathbb{Q})$.

Iskovskii: on trouve tout le Br_2

<u>Exemples</u> de Sw. D. contre Hasse et App. faible.

+ Th. (modulo Conj. Buniakovski) si α a un seul pôle alors (H) + App. faible vrai

<u>Exemples</u> :

$\alpha = \beta + \gamma$ $\quad \beta = (-1)(T^2 - 3)$

$\gamma = (-1)(2 - T^2)$

$\alpha = (-1)(f(t))$ où $f = (t^2-3)(2-t^2)$

(H) est faux : sol. locales mais pas globale.

(*) $\left[\begin{array}{l} \text{pour } p \neq \infty \text{ et } \forall\ t_p \in \mathbb{P}_1(\mathbb{Q}_p) - \text{pôle} \quad \beta(t_p) \text{ ou } \gamma(t_p) = 0 \text{ et choisir } t_p \text{ où } \beta(t_p) = \gamma(t_p) = 0 \\ \text{à } \infty \quad |t| \geq \sqrt{3}, \quad |t| \leq \sqrt{2} \quad \text{soit } \beta(t_p) \neq 0 \text{ soit } \gamma(t_p) \neq 0. \end{array}\right.$

il y a des solutions locales, modulo (*)

et $H_A(\beta, \gamma) = \emptyset$. car si $t = (t_p) \in H_A(\beta, \gamma)$ alors $\beta(t_p) = 0$ car $\alpha = 0$ et l'un des 2 est nul. mais $\beta(t_\infty) \neq 0$. formule de somme n'est plus valable.

-t passez grand, on a
... de $\mathbb{P}_1(\mathbb{F}_p)$ n'est pas

(113)

co-restriction)

... n P & S.

$= 0$

... $\mathrm{inv}_p(\beta(t_p)) = 0\}$

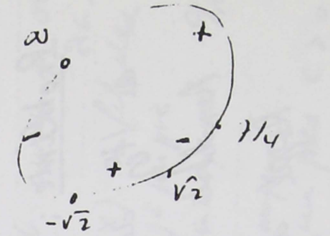
... supports par des points.
... spécifié

... des fct. de $V_{f,g}$) non vous fié.
Variété $V_{f,g}$ (sens de Groth.)
modulo $Br_2(\mathbb{Q})$.

faible.

... seul pôle alors (H) + App. faible vrai

Approximation faible $\beta = (-1)(4t-17)$ $\quad \gamma = (-1)(t^2-2)$ (PSU)



Sur $\mathbb{R}$ semble $]17/4, \infty[$, $]-\sqrt{2}, \sqrt{2}[$ n'ont pas de pt. rationnel sur le second, par le même argument.

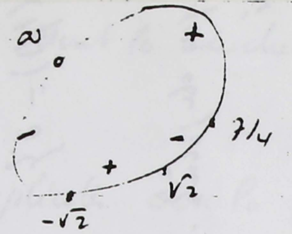
- Théorème à la Lagrange.
- La conjecture entière (pour $\mathbb{R}$ top) de $H_{\mathbb{Q}} \subset \mathbb{P}_1(\mathbb{Q})$ formé d'un nombre fini d'intervalles dont les extrémités sont des pôles $/\mathbb{R}$ de α. Liée à une conjecture de Mazur. Soit V une variété algébrique lisse sur $\mathbb{Q}$, suppo. $V(\mathbb{Q})$ Zariski-dense alors $\overline{V(\mathbb{Q})}$ pour $\mathbb{R}$-top. est ouvert et fermé de $V(\mathbb{R})$: c'est une réunion de composantes connexes. Entraîne des conséquences extraordinaires : "$\mathbb{Z}$ n'est pas définissable polynom. dans $\mathbb{Q}$" :

$$\begin{array}{ccc} V(\mathbb{Q}) & & \\ \downarrow \pi & \quad \pi(V(\mathbb{Q})) = \mathbb{Z} & \\ \mathbb{A}^1 & & \end{array}$$

"des équations $P(\underline{x}, t)$: a une solution en x dans $\mathbb{Q}$" $\iff t \in \mathbb{Z}$.

— pas d'analogue p-adique.

Approximation faible $\beta = (-1)(4T-7)$ $\gamma = (-1)(T^2-2)$



Sur $\mathbb{R}$ semble $]7/4, \infty[$, $]-\sqrt{2}, \sqrt{2}[$ on perd le pt. rationnel sur le second, par le même argument.

- Théorème à la Hasse.
- la conjecture entière (pour $\mathbb{R}$ top) est $H_{\mathbb{Q}} \subset \mathbb{P}_1(\mathbb{Q})$ formé d'un nombre fini d'intervalles dont les extrémités sont des pôles $/\mathbb{R}$ de α. Liée à une conjecture de Mazur. Soit V une variété algébrique lisse sur $\mathbb{Q}$, suppo. $V(\mathbb{Q})$ Zariski-dense alors $\overline{V(\mathbb{Q})}$ pour $\mathbb{R}$-top. est ouvert et fermé de $V(\mathbb{R})$: c'est une réunion de composantes connexes. Entraîne des conséquences extraordinaires : "$\mathbb{Z}$ n'est pas définissable polynom. dans $\mathbb{Q}$" :

$$\begin{array}{c} V/\mathbb{Q} \\ \downarrow \pi \\ \mathbb{A}^1 \end{array} \qquad \pi(V(\mathbb{Q})) = \mathbb{Z}$$

des équations $P(\underline{x}, t)$: a une solution en x dans $\mathbb{Q}^n \Leftrightarrow t \in \mathbb{Z}$.

— pas d'analogue p-adique.

Le 16-12-1991.

<u>Problème</u> : Démontrer que l'hypothèse H de Schinzel entraîne la conjecture "densité de $H_{\mathbb{Q}}$ dans $\bigcap_{\beta+\gamma=\alpha} H_{A}(\beta,\gamma)$". Cas particulier par Colliot-Th. + Sansuc.

Résultats récents sur Sur HPF. en nombre fini, non proportionnels.

Rappel de Hyp. de Schinzel $P_i \in \mathbb{Z}[X]$, irréd. sur $\mathbb{Q}$. tq Terme domin. >0

$\forall p$ premier $\exists n$ tel que $\prod P_i(n) \not\equiv 0 \ (p)$.

(H) : il existe une infinité de $n > 1$ tels que $P_i(n)$ soit premier $\forall i$.

<u>ex</u> $P_1 = X$, $P_2 = X+2$ Nbres premiers jumeaux

$P = X^2+1$?

difficult accessible vu les exemples !

version raffinée $n \le X$, $P_i(n)$ premier $\forall i$ Conjecture nbre $\simeq c \dfrac{X}{\log(X)^k}$

et vérifications numériques.

L'hypothèse de Schinzel permet de simplifier les calculs de symboles.

Soient $t=(t_1,\dots,t_n)\in\mathbb{Z}^n$; $f_j(t)$, $g_j(t)$ est défini $\neq 0$

$\alpha(t)\in Br_2(\mathbb{R})$ a un sens.,

$\mathbb{Z}_\alpha = \{t\in\mathbb{Z}^n, \alpha(t)=0\}$; X nombre réel $\to\infty$

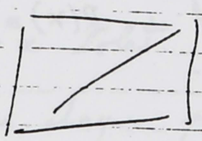
$Z_\alpha(X) = \{t\in Z_\alpha \mid |t|\le X\}$, on s'interesse à la taille

<u>Cas Particulier</u> $n=1.$; $\alpha=(-1,T_1)$, $t\in\mathbb{Z}$ $\alpha(t)=0$ $t\neq 0$ et $t=\square+\square$.

$Z_\alpha(X) = \#\{t \mid 1\le t\le X;\ t=\boxed{2}.\}$

Landau : $Z_\alpha(X)\sim c.\dfrac{X}{\sqrt{\log(X)}}$

<u>Th</u> 1 $Z_\alpha(X) \ll X^n/(\log(X))^{d/2}$ pour $X\to\infty$ où d = Nbre de diviseurs polaires irreduct de α vu sur l'espace affine Aff^n.



W = div Ω ass. $\to$ évaluation sans de probl. de pôle à W,

Donc le cas particulier $\infty, 0$ pôles de α seul 0 est dans Aff.

On peut travailler dans l'espace projectif.

<u>Th 2</u> $Z_\alpha^{proj}(X) \ll X^{n+1}/(\log(X))^{d^{proj}/2}$

nbre de pts rationnels de P_n de hauteur $\le X$ qui annulent α

Th 1 $\Rightarrow$ Th 2 standard passage Proj. en affine de dim $+1$

$d=0$. cas où α est C^t. pas intéressant.

<u>Corollaire</u> : si $\alpha\neq 0$, il y a une ∞ de $t\in\mathbb{Z}^n$ avec $\alpha(t)\neq 0$.

<u>Méthode de démonstration</u> Grand Crible,

$\Lambda = \mathbb{Z}^n \subset \prod_p \mathbb{Z}_p^n$; $\Omega_p \subset A_p$, $Z_\Lambda = \{\lambda\in\Lambda \mid$ il n'existe aucun p avec $\lambda\in\Omega_p\}$

$Z_\Lambda(X) = \{\lambda\in Z_\Lambda ; |\lambda|\le X\}$ on recherche majoration de $\# Z_\Lambda(X)$ en fct des volume des Ω_p.

Mesure de Haar sur $\mathbb{Z}_p$: masse totale $=1$.

petit crible : mesure (Ω_p) à peu près en moyenne c/p

G^d crible : mes (Ω_p) en moyenne à peu près $c>0$

Reprenons exemple. $t=\boxed{2}$. $t=\prod p^{e_p} \iff \forall p\equiv -1\ (4)$ e_p est pair

$\Omega_p = \emptyset$ si $p=2$ ou $p\equiv 1\ (4)$

$\Omega_p = t : v_p(t)\equiv 1\ (2)$ si $p\equiv -1\ 4$

mesure 0 ou $\frac{1}{p}$, $c=\frac{1}{2}$

On suppose que l'on a un petit crible + hypothèse de régularité sur Ω_p : il existe un entier $e\geq 1$ et une partie (ouverte compacte) $\Omega'_p\subset\Omega_p$, réunion finie de classe mod p^e et une fonction Frobenienne $f(p)$ de p de moyenne $c>0$ telle que

$\text{mes}(\Omega'_p) = \dfrac{f(p)}{p} + O\left(\dfrac{1}{p^{1+\delta}}\right)$, $\delta>0$:

Th Sous cette hypothèse $Z_\Lambda(X) << X^n/\log(X)^c$ (c indépendant de p. ici $c = 2$)

explication et vocabulaire; fonction Frobénienne en p : s'il existe ext. finie galoisienne $L/_\mathbb{Q}$ telle que, pour p assez grand, $f(p)$ ne dépend que de la classe de conjugaison de σ_p $(L/_\mathbb{Q})$

$$p \longmapsto \sum_{\lambda_i \in \mathbb{C}}' \lambda_i \chi_i(\sigma_p)$$

χ_i caract de $\mathrm{Gal}(L/\mathbb{Q})$

exemple $f(p)$ ne dépend que de p mod m, (m donné)

autre cas 1/ $f(p) = \begin{cases} 1 & \text{si } p = x^2 + 63y^2 \\ 0 & \text{sinon.} \end{cases}$ $\Big| \; L/_{\mathbb{Q}(\sqrt{-21})} \; / \; \mathbb{Q}$

2/ $K/\mathbb{Q}$ ext finie $f(p) = \{\#$ idéaux premiers de O_K de norme $p\}$.

3/ $P = X^m + \dots + a_m$, $a_i \in \mathbb{Z}$ $f(p) = \#$ sol de $P(x) \equiv 0$ (p)

4/ formes modulaires, niveau, poids fixe. mod m fixé.

$p \nmid$ niveau $\longmapsto T_p \in \mathrm{End}(S)$ T_p est fonction frobénienne en p (Représentation l-adique de Deligne)

moyenne de fct. Frobénienne. $c(f) = \lim_{x \to \infty} \sum'_{p \le x} f(p) \Big/ \left(X/\log(x)\right)$

avec la décomp. en caractère c'est λ_1.

Le théorème dit que si c, $\mathrm{mes}(\Omega_p) = \frac{f(p)}{p} + O\left(\frac{1}{p^{1+\varepsilon}}\right)$

$| \quad | << X^n/(\log(X))^c$ c moyenne de f.

Méthode de crible standard : $Z_\Lambda(X)$ a une majora° explicite à partir de c et $\mathrm{mes}(\Omega_p)$

Serre : $Z_\Lambda(X) \le (2X)^n/L$ où $L = \sum'_{\substack{q \text{ sans fact. } \square \\ q \le X^{1/2c}}} \prod_{p|q} \frac{\mathrm{mes}(\Omega_p)}{1 - \mathrm{mes}(\Omega_p)}$

reste un travail analytique :

$L(Y) = \sum'_{\substack{q \le Y \\ s f \square}} \prod_{p|q} \frac{\mathrm{mes}(\Omega_p)}{1 - \mathrm{mes}(\Omega_p)}$ montrer que $L(Y) >> (\log(Y))^c$

qui se fait par la technique des séries de Dirichlet. On pose $a_p = \frac{\mathrm{mes}(\Omega_p)}{1 - \mathrm{mes}(\Omega_p)} = \frac{f(p)}{p} + O\left(\frac{1}{p^{1+\varepsilon}}\right)$

$a_q = \begin{cases} 0 & \text{si } q \text{ a un fa } \square \\ \prod_{p|q} a_p & \text{sinon} \end{cases}$, on construit $\sum' a_q q^{-s} = \phi(s)$

or $\phi(s) = \prod_p (1 + a_p p^{-s})$, comportement de $\phi(s)$ en $s = 0$

On peut utiliser un Théorème de Hardy & Littlewood (Oe. Vol 6 p 526, Th

Soit $\phi(s) = \sum a_n n^{-s}$ à coef > 0., converg pour $\mathrm{Re}(s) > 0$

on suppose de + que $\phi(s) = \gamma s^{-c}$ pour $s \to 0$

alors la fct sommat. $\sum'_{n \le Y} a_n = \frac{\gamma}{\Gamma(1+c)} \log(Y)^c$ ~~restera~~ Tout y est

$a_p = \frac{f(p)}{p} + O\left(\frac{1}{p^{1+s}}\right)$ $f = \sum \lambda_i \chi_i$ $\Phi(s) = \prod_i L(s+1, \chi_i)^{\lambda_i}$ $\mathrm{Re}(s) > 0$.

$\Phi(s) \underset{s \to 0}{\sim} c^t \left(\frac{1}{s}\right)^{\lambda_1}$ / les exposants λ_i ne sont pas genants, bon domaine. /

10h30. Reste a voir que l'on peut bien appliquer ce th. à la specialisation de α. — Renvoi à la note pour le cas general.

Cas Particulier $\mathbb{P}_1$, $\alpha \in Br_2(\mathbb{Q}(t))$, $t \in \mathbb{Q}$, t $\alpha(t) = 0$?

definissons un $\Omega_p \subset \mathbb{P}_1(\mathbb{Q}_p)$ / pôles et residus de α

$P_1, \dots, P_d$ residus $r_1 \dots r_d$ à P_i corps residuel $K_i/\mathbb{Q}$.

$r_i \in K_i^*$ mod carres, $\longleftrightarrow$ L_i/K_i quadratiques.

d = nbre de Poles.

pour chaque p, $\mathbb{Q}_p$, K_i se decomp. $K_i = \prod K_{i,p,j}$, pour chaque L_i:

$L_{i,p,j} = \begin{cases} K_{i,p,j} \times K_{i,p,j} \\ \text{ext. quadrat.} \end{cases}$

On ne s'interesse qu'aux couples (i,j) tel que $\begin{vmatrix} L_{i,j,p}/\mathbb{Q}_p \text{ quadratique} \\ K_{i,p,j} = \mathbb{Q}_p \end{vmatrix}$

ils correspondent aux poles de $\alpha_p \in Br_2(\mathbb{Q}_p(T))$ qui sont rationnels sur $\mathbb{Q}_p$.

Definit des points $P_{i,j,p} \in \mathbb{P}_1(\mathbb{Q}_p)$. On peut demontrer que pour p assez grand on peut exhiber $\alpha(t) \in Br_2(\mathbb{Q}_p) \simeq \{0, 1/2\}$

Recette Soient $\tilde{P}_{i,j,p}$ la reduction mod p (des points $P_{i,j,p}$) $\in \mathbb{P}_1(\mathbb{F}_p)$

- si $\tilde{t} \neq \tilde{P}_{i,j,p}$ $\alpha(t) \neq 0$
- les $\tilde{P}_{i,j,p}$ sont distincts (p assez grand) $\Big\}$ liste des conditions à preciser

si $\underset{\text{non pôle}}{\tilde{t} = \tilde{P}_{i,j,p}}$ soit e le max. tel que $t \equiv P_{i,j,p}$ (p^e)

on note $e = v(t, P_{i,j,p})$ alors $\alpha(t) = 0$ si e est pair $\neq 0$ sinon.

le mauvais Ω_p est donc defini par des congruences modulo p^2

D'où $e = 2$, et $\mathrm{mes}(\Omega_p) = \frac{f(p)}{p} + O\left(\frac{1}{p^2}\right)$

et $f(p) = \#$ point $P_{i,j,p}$: presque le nombre des ideaux de degré 1 de K_i au-dessus de p (attention il faut en plus $L_{i,j,p}$ quadratique)

ce qui donne moyenne de $f(p) = \frac{d}{2}$.

Problème qui se pose :

1. On aimerait avoir des minorations, (pour voir que les majora. ne sont pas trop stupides) hypothèse la + optimiste, Dans le Th 2 sur les $\mathbb{P}_n$.

on a $Z_d^{proj}(X) >> X^{n+1}/\log(X)^{d\,proj/2}$ si $Z(d) \neq \emptyset$ | même $n=1$ n'est pas connu.

On peut tester sur machine (Mestre, Coray, non concluant !)

exemples de Coray $(-1, f(t))$ $\mathbb{P}_1$, $f(t) =$ ① $t(t^2+2)$
② $t(t^2+5)$
③ $t(t^4+2)(t^4+3)(3t^4+1)(2t^4+3)(3t^4+2)$

$(-t, t^3+t+1)$

① $t(t^2+2)$ $0, \pm\sqrt{-2}, \infty$ pôle : 3 $Z(X) >> X^2/\log(X)^{3/2}$

② $t(t^2+5)$ $0, \pm\sqrt{-5}, \infty$ pôle : 3.

③ ________________ $Z(X) >> X^2/\log(X)^{7/2}$

pour le 3 ça colle.

pour ① et le ② la machine semblerait donner 1,25 ?

Dernier cas $(-t, t^3+t+1)$ $t=0$ pas un pôle, ∞ non plus, 1 seul pôle, semble coller numériquement.

Cas particulier affine : (x, y), $1 \leq x, y \leq X$ tels que $(x, y) = 0$

conique $(1, -x, -y)$ a un pt. rationnel. Soit $N(X)$ leur nombre.

le Th. dit que $N(X) << \frac{X^2}{\log(X)}$ (avec le plan)

en sens inverse ordinateur semble sceptique - Voir dans la note

résultat partiel : $N(X) >> X^2/\log(X)^2$: pour cela on prend (x, y) premiers $\equiv 1 \mod (4)$ $\alpha(x, y) = 0$ si $\left(\frac{x}{y}\right) = 1$ -

Naïvement : $\simeq \left(\frac{X}{\log(X)}\right)^2 \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2}$? pour cela il faut prouver que le symbole de Legendre est distribué au hasard :

$$\sum_{\substack{x, y \text{ premiers distincts} \\ \equiv 1 (4)}} \left(\frac{x}{y}\right) \overset{?}{=} o\left(\frac{X^2}{\log(X)^2}\right)$$

en fait Heilbronn montre nettement mieux $O(X^\delta)$ $\delta = 7/4$?

Quelques autres cas amusants :

$(a, b, c) \in \mathbb{Z}^3$ $|a, b, c| < N$ tel que $aX^2 + bY^2 + cZ^2 = 0$ ait un pt rationnel, combien y en a-t-il ? pour $N \to \infty$ donner estimation ?

(prendre le symbole $(-ab, -ac)$)

même problème pour la conique générale

$$ax^2 + bxy + cy^2 + dyz + exz + fz^2 = 0$$

$|a, b \dots| \leq X \qquad N(X)? \ll X^6/\log(X)^{1/2}$

Beaucoup de questions ouvertes s'ouvrent sous nos pas (!)

mais le plus intéressant comprendre le premier exemple de Leray.

- Voir les exemples $(-1, t) + (5, t+1)$

(prendre le symbole $(-ab, -ac)$

même problème pour la conique générale

$$ax^2 + bxy + cy^2 + dyz + exz + fz^2 = 0$$

$$|a, b \ldots| \leq X \quad N(X) ? \ll X^6 / \log(X)^{1/2}$$

Beaucoup de questions ouvertes s'ouvrent sous nos pas (!)

mais le plus intéressant comprendre le premier exemple de Coray.

Voir les exemples $(-1, t) + (5, t+1)$

20-1.92 : Application de la Conjecture de Schinzel.

hypothèse (H) de Schinzel ⟹ Th. de densité à la Hasse-Manin

k corps de nombre $\underline{\alpha} = (\alpha_i)_{i \in I \text{ fini}}$ $\alpha_i \in Br(k(T))$ $n\alpha_i = 0$ n fixé ($\alpha_i \in H^2(k(T), \mu_n)$

? $t \in \mathbb{P}_1(k)$ où les α_i s'annullent. (t non pôle et $\alpha_i(t) = 0$ $\forall i$ dans $Br_n(k)$)
noté $\underline{\alpha}(t) = 0$.

On appelle V_k ensemble des places de k, $v \in V_k$, k_v complété de k en v, $\mathbb{A}_k$ anneau des adèles $= \prod k_v$, $\mathbb{P}_1(\mathbb{A}_k) = \prod_v \mathbb{P}_1(k_v)$ topologie produit qui en fait un espace compact. $(x_v) \in \mathbb{P}_1(k_v)$, x_v non pôle pour $\underline{\alpha}/k_v$; $\underline{\alpha}(x_v) \in H^2(k_v, \mu_n)^I$

$N_\alpha \subset \mathbb{P}_1(\mathbb{A}_k)$; $N_\alpha = \{(x_v), x_v \in \mathbb{P}_1(k_v)$ $\underline{\alpha}(x_v) = 0$ dans $H^2(k_v, \mu_n)^I$

$N_\alpha(k) \subset N_\alpha$; principe de Hasse ⟺ $N_\alpha(k)$ dense dans N_α.

Ensemble subordonné. k corps $\underline{\alpha} = (\alpha_i) \in Br_n(k(T))$
y pt fermé de $\mathbb{P}_1/k$

$$res_y\, \alpha_i \in H^1(k/y, \mathbb{Z}/n\mathbb{Z})$$

$$\text{Hom}(G_{k/y}, \mathbb{Z}/n\mathbb{Z}) = \text{caractère du corps résiduel.}$$

on $res_y\, \alpha_i$ p.p $\forall y$; $\sum_y' \text{cor}_y(res_y\, \alpha_i) = 0$

$\beta \in Br_n(k(T))$ β est subordonné à $\underline{\alpha} = (\alpha_i)$ si

$\forall y$ pt fermé de $\mathbb{P}_1(k)$ $r_y(\beta)$ combinaison $\mathbb{Z}$ linéaire des $r_y(\alpha_i)$

Exemples triviaux:

- β constant $(\in Br_n(k))$
- β combinaison linéaire des α_i

ce qui est intéressant c'est quand il y en a d'autres.

interprétation : V variété lisse irréduct. et π morphisme dominant $V \xrightarrow{\pi} \mathbb{P}_1$

$K = k(V) \supset k(T)$ on a des $\alpha_{i,K}, \beta_{i,K} \in Br_n(K)$.

Si les "$\alpha_{i,K}$" sont non ramifiés" i.e $\in Br(V)$ et si β est subordonné à $\underline{\alpha}$ alors

β_k est non ramifié sur $\bar{V}$.

Revenons au cas. Soit β subordonné à $\underline{\alpha}$. Si $x = (x_v) \in \mathbb{A}^1_\cdot(\mathbb{A}_k)$, x_v non pôle de α. regardons la quantité $e_\beta(x) = \sum'_{v \in V_k} \mathrm{inv}_v\, \beta(\pi_v)$ où $\beta(x_v) \in Br_n(k_v) \hookrightarrow \mathbb{Q}$ en fait dans $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ qu'on identifie à $\mathbb{Z}/n\mathbb{Z}$

Lemme Si β subordonné à $\underline{\alpha}$ la fonction $e_\beta : N_\alpha \longrightarrow \mathbb{Z}/n\mathbb{Z}$ est local^t cte.

et même mieux : il existe une partie finie $S(\beta, \alpha) = S \subset V_k$ telle que $v \notin S \Rightarrow \underline{\alpha}(x_v) = 0$ implique $\beta(x_v) = 0$.

et il est clair que $e_\beta(N_\alpha(k)) = 0$. On introduit donc l'espace Manin :

$$\underline{M}_\alpha \underset{def}{=} \{ x \,/\, x \in N_\alpha \,,\ e_\beta(x) = 0 \text{ pour tout } \beta \text{ subordonné à } \underline{\alpha} \}$$

M_α est ouvert et fermé dans N_α. (se ramener au cas constant ...

Conjecture 1 : H.M $N_\alpha(k)$ est dense dans $\underline{M}_\alpha$.

Conséquence si $\underline{M}_\alpha \neq \emptyset$ alors $N_\alpha(k) \neq \emptyset$.

le Théorème $(H) \Longrightarrow$ conj 1 ; Rappel de l'hypothèse H.

Soit (P_j) des poly irréduc sur $\mathbb{Q}$, à coef entiers, en nombre fini à termes dominant > 0 et tels que $\forall p$ premier, il existe $x \in \mathbb{Z}/p\mathbb{Z}$ tel que tous les $P_j(x)$ sont $\neq 0$ dans $\mathbb{Z}/p\mathbb{Z}$ alors il existe une infinité d'entiers $n > 0$ tels que le $P_j(n)$ soit premier quel que soit j

Cas particulier Colliot Thélène Sansuc $k = \mathbb{Q}$; $n = 2$ $\alpha_i = (a_i, P_i(T))$ $a_i \in \mathbb{Q}^*$

P_i irréductible (les β subordonnés sont triviaux) alors $M_\alpha = N_\alpha$ sur $\mathbb{A}^1$. existence de solutions rationnelles dans les adéliques. c'est donc Hasse.

cas particulier le P_i sont unitaires ; $\underline{M}_\alpha \neq \emptyset$. à l'$\infty$ t grand > 0 =) carrés

p premier $t = \frac{1}{p^{2N}}$ pour N grand donc carré.

Donc, sous (H), on peut résoudre $(a_j, P_j(t)) = 0$ ex $a_j = -1$, $P_j(t) = \square + \square$

ex P_j $t, t+1, \dots, t+5$ sous H $\exists$ xt à rationnels dense dans $\mathbb{R}^+$

t_j $t, t+1, \dots, t+5$ soit $\square + \square$ dans $\mathbb{Q}$

pour $t, t+1, t+2$ Coll. Th. sait faire

Comment faire sans H ? p premier $\equiv 1 \ (4) \Rightarrow p = \square + \square$

facteur de forme $t, t + A^2, \dots, t + 5A^2$

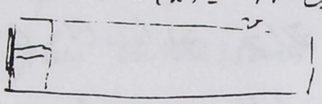
ensuite $t = 1 + 4x$ on veut rendre premier $1+4x$, $1+4x+A^2, \dots, 1+4x+5A^2$

pour les nombres premiers + grand, on peut éviter

Nous devons partir de $(x_v) \in M_\alpha \subset \mathbb{P}_1(\mathbb{A}_k)$ on veut prouver que dans tout voisinage il existe un rationnel. Base de voisinage, S fini $\subset V_k$, chaque $v \in S$ U_v voisinage de x_v pour la topologie v-adique. Alors voisinage de $(x_v) = \prod_{v \in S} U_v \times \prod_{v \notin S} \mathbb{P}_1(k_v)$

il faut trouver $x \in \mathbb{P}_1(k)$ ds ce voisinage -

Notons $\mathcal{U}(x) = \prod_v U_v$ $\qquad U_v = \mathbb{P}_1(k_v)$ pour p.p. v



on voit les pôles comme des sections

$\overleftrightarrow{S}$ —— Spec (O_k)

-hypothèse de Schinzel permet de trouver des x qui rencontrent exactement une fois chaque variété polaire. On retrouve déjà ce genre d'astuce dans la démonstration du principe de Hasse (remarque de Colliot Thélène)

Démonstration dans un cas particulier. $k =$ corps de nombres, un seul α, n quelconque.

- On se donne $(x_v) \in M_\alpha$ et un voisinage. On peut agrandir à volonté S et diminuer les U_v
  - On peut supposer α constant sur U_v $\quad \alpha = 0$
  - On peut supposer $S \supset$ places archimédiennes, et U_v ouvert pour ces places

il existe point rationnel de $\mathbb{P}_1$ qui $\forall v$ archimédien $\in U_v$. Par un automorphisme que point est à ∞ ; en particulier ∞ n'est pas un pôle. Les conditions archimédiennes : $x \in k$ doivent être arbitrairement grand en les places archimédiennes.
  - les pôles sont des entiers

- Rappel de Faddeev : $Y =$ réunion des pôles de α, ss schéma fermé de $\mathbb{P}_1$

Si y pt fermé de Y. $k(y)$ corps résiduel $d_y = [k(y):k]$, $\infty \notin Y$ Tension $\longmapsto$

$t_y \in k(y)$ $\qquad r_y(\alpha) \in H^1(k(y), \mathbb{Z}/n\mathbb{Z})$

Soit $t \in k$, t non pôle de α $\qquad \underset{t \neq \infty}{\alpha(t)} = \alpha(\infty) + \sum_y' \underset{H^1(\ ,\mu_n)}{\mathrm{Cor}(t - t_y)} \cdot \underset{H^1(\mathbb{Z}/n\mathbb{Z})}{r_y(\alpha)}$

on peut aussi écrire $\alpha(\infty) + \sum_y' \mathrm{Cor}_y \left(1 - \frac{t_y}{t}\right) r_y(\alpha)$
$n\ t \neq 0$

- Conditions sur S, $S = S(k, N)$ $\quad N \geq 1$
$\qquad =$ places archimédiennes $\cup$ places ultram. à carac. résid $\leq N$

avec propriétés suivantes :

ⓐ $N \geq n$ $\quad$ (n de Br_n)

ⓑ $N \geq [k:\mathbb{Q}] \cdot \sum_{y \in Y}' d_y$

ⓒ Si $v \notin S$, dis. du poly carac. P_y de t_y sont entiers en v -

- on veut égal^t que les revêt^{ts} de 2 d'entre eux soient distincts

(d) les inv. de $\alpha(\infty)$ en les places $v \notin S$ sont 0.

(e) les caractères $res_y(\alpha)$ sont non ramifiés en toute place de $k(y)$ de caract. résid. $\neq n$.

(f) $S^{-1}O_k$ principal

Entiers que si $v \notin S$ et si $x_v \in \mathbb{P}_1(k_v)$ non pôle on a

$\alpha(x_v) = 0$ dans $Br_n(k_v)$ si $\tilde{x}_v$ (red mod v de x_v) distinct des réduction mod v de pôles.

Si $\tilde{x}_v$ est la réduc mod v d'un pôle : $\alpha(\tilde{x}_v) = - v(x_v, y_v) . inv_{\tilde{v}} \, r_{y_v}(\alpha)$ le plus proche

$k_v(y_v) = k_v$

$k_v^* \longrightarrow \mathbb{Z}/n\mathbb{Z}$

Ceci montre clairement que les β s'annulent sur ces gens là. On introduit les invariants $\varepsilon(y)$, $y \in Y$ (plutôt $\varepsilon(y, (x_v))$) définis par

$$\varepsilon(y) = \sum_{v \in S}' inv_v \left(t - t_y\right) . r_y(\alpha) \quad \in \mathbb{Z}/n\mathbb{Z}$$

(on aurait dû en introduire 1 pour chaque α_i si plusieurs α.)

<u>Lemme</u> : Soient n_y, $y \in Y$ des entiers tels que

$$\sum_y{}' n_y \, Cor_y \, r_y(\alpha) = 0 \quad \text{Alors } \sum{}' n_y \, \varepsilon(y) = 0$$
dans $H^1(k, \mathbb{Z}/n\mathbb{Z})$.

<u>On en déduit</u> (Čebotarev)

$\exists \, w \notin S$ telle que pour $\forall y \in Y$, inv_w de $Cor_y \, r_y(\alpha)$ est égal à $- \varepsilon(y)$
∞ de t.

On peut choisir $q \in O_k$ tel que $w(q) = 1$, $v(q) = 0$ $v \notin S$ $v \neq w$.

$A = \prod_{p \in N} p$, cherchons $x \in k$ (liant α)

$$x = \frac{a}{qA^n} \quad \text{avec } a \in O_k \quad \text{(un seul pôle en } q \text{, en dehors de } S)$$

conditions sur a :

1) $a \equiv a_0$ (à fixer) mod (A^{n+m}) de telle sorte que $x \in U_v$ $\forall v \in S - S_\infty$

2) $\forall v \in S_\infty$ $|a|_v \gg 0$

3) $P_y\left(\frac{a}{qA^n}\right)$ a une valu^o nulle $\forall v \notin S^{\cup\{q\}}$ à l'exception d'une valu^o v_y où elle rendue arbitrairement grande où cette valuation est égale à 1.

(3) est possible par H

---

il faut connaître $inv_v \, \alpha(x)$ — $v \in S$ $inv_v(\alpha(x)) = 0$. par ...

$v \notin S$ $Cor \, (x - t_y) . r_y(\alpha)$ x entier sauf pour w $x_w = \infty$.

$inv_w \, \alpha(x) = 0$

~~Hypothèse~~ : $\mathrm{Cor}_y(x-t_y).r_y(\alpha)$ ~~= 0 en tt place v ∉ S~~ $\in Br_n(k)$

~~il y a ... v et t_y~~

calculons la somme des inva. $=0$,

(2) termes dans S $\qquad \varepsilon(y)$

(1) en v : $-\varepsilon(y)$ grâce au choix de v

(1) en v_y $= -\mathrm{inv}(r_y(\alpha))$ en v_y

D'où l'on déduit $\mathrm{inv}(r_y(\alpha))$ en $v_y = 0$.

En revenant à α. $\mathrm{Cor}_y(x-t_y).r_y(\alpha)$ est nulle en v_y.

Indication sur la façon d'obtenir (H) ~~sur k~~ dans les corps de nombres.

Si P irred. sur k ; il suffit de prendre la norme.

k/k_0. P irr sur k $\exists$ Nbre fini d'hyperplans k_0 affine de k

tels que $\forall a \notin \bigcup$ hyperplan $N_{k/k_0}(P(t-a))$ est k_0-irreductible.

On peut donc generaliser à un Nbre fini de P_j

$k(y)$ remplacer y par $y-a$ pour avoir un generateur sur k_0.

$$\begin{array}{c} k(y) \\ | \\ k \\ | \\ k_0 \end{array}$$

Consequence de H pour les corps de nombres

$S(k,N)$ $\qquad P_j$ poly k-irred. de d° d_j

$N \geq [k:\mathbb{Q}]\,\sum_i d_j$

Soit $M \geq N$, alors sous (H) il existe $x \in C_k$

$|x|_\sigma > M$ $\quad$ tte place archi.

$\forall j$ $\quad \exists v_j \notin S$ tq $v(P_j(x)) = 0$, $v \notin S$ $\quad v \neq v_j$

$v_{v_j}(P_j(x)) = 1$

caract. resi $v_j \geq M$.