

COURS DE JEAN-PIERRE SERRE

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_>](http://www.numdam.org/item?id=CJPS_1992__13_>)

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

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

NUMDAM

*Notes numérisées par l'IHP et diffusées par le programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>*

- 4 FEV. 2000

Cours 1991-1992

Corps de fonctions et cohomologie galoisienne

Notes de E. Bayer

L. Fainsilber

J. Cougnard

N° Cote : PB 929 9 am
Institut Henri Poincaré BIBLIOTHÈQUE 11, rue P.-et-M.-Curie 75231 PARIS CEDEX 05
N° Inventaire : 28660 B

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



92^e année

PARIS

11, place Marcelin-Berthelot (V^e)

Alfred et Geneviève

M. Jean-Louis de la Roche
(A. de la Roche de la Roche)

ANNUAIRE

DE

COLLÈGE DE FRANCE
1991 - 1992

RÉSUMÉ
DES COURS ET TRAVAUX



1991

PARIS

11, place Marcelin-Berthelot (V)

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 transcendentes pures. Il a comporté deux parties.

I. COHOMOLOGIE DE $k(T)$

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 :

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

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

$$(1.2) \quad \dots \rightarrow H^i(\Gamma, C) \rightarrow H^i(G, C) \xrightarrow{\sim} H^{i-1}(\Gamma, \text{Hom}(N, C)) \rightarrow H^{i+1}(\Gamma, C) \rightarrow \dots$$

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

Si α est un élément de $H^i(G, C)$, on peut représenter α par un cocycle $a(g_1, \dots, g_i)$ 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 $\gamma_2, \dots, \gamma_i$ de $g_2, \dots, g_i$ dans Γ . Pour $\gamma_2, \dots, \gamma_i$ fixés, l'application de N dans C définie par

$$n \mapsto a(n, g_2, \dots, g_i) \quad (n \in N),$$

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

Faisons l'hypothèse supplémentaire :

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

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

$$(1.4) \quad 0 \rightarrow H^i(\Gamma, C) \rightarrow H^i(G, C) \xrightarrow{\sim} H^{i-1}(\Gamma, \text{Hom}(N, C)) \rightarrow 0.$$

§2. Le cas local

Si K est un corps, on note K_s une clôture séparable de K , et l'on pose $G_K = \text{Gal}(K_s/K)$. 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 $D \cong G_{K_v}$ et $D/I \cong G_{k(v)}$.

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

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

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 $G_K \rightarrow G_k$, 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 $H^i(\text{Gal}(\bar{L}/K), C_L)$, 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 » :

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

où $\text{Cor}_k^{k(x)} : H^{i-1}(k(x), C(-1)) \rightarrow H^{i-1}(k, C(-1))$ 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 $G_F \rightarrow G_E$) par le degré inséparable $[F:E]_i$. Le composé $\text{Cor}_E^F \circ \text{Res}_E^F$ 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

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

On déduit de (3.2) la formule suivante :

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

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 ;

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

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

$$\alpha(D) = 0,$$

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 $H^i(k, C)$; 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 $K = k(T)$

C'est celui où X est la droite projective P_1 . Du fait que X possède un point rationnel, l'homomorphisme canonique $H^i(k, C) \rightarrow H^i(K, C)$ est injectif. Un élément de $H^i(K, C)$ est dit *constant* s'il appartient à $H^i(k, C)$. On démontre :

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

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

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

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

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

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

Remarque — Soit $\alpha \in H^i(K, C)$, 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 $\infty \notin P$:

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

où :

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

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

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

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

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

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

Généralisation à plusieurs variables

Soit $K = k(T_1, \dots, T_m)$ 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 $H^2(K, C) = \text{Br}_n K$, noyau de la multiplication par n dans le groupe de Brauer de K . La suite exacte (4.3) s'écrit alors :

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

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

Soit $\alpha \in \text{Br}_n K$, et soit $P(\alpha) \subset X$ 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 $\text{Br}_n k$. 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 $\alpha \in \text{Br}_n K$, avec $K = k(T)$ comme ci-dessus. Soit $f(T')$ une fonction rationnelle en une variable T' ; supposons f non constante. Si l'on pose $T = f(T')$, on obtient un plongement de K dans $K' = k(T')$. D'où, par changement de base, un élément $f^*\alpha$ de $\text{Br}_n K'$. On dit que α est *tué par* K'/K (ou par f) si $f^*\alpha = 0$ dans $\text{Br}_n K'$. S'il en est ainsi, on a $\alpha(t) = 0$ pour tout $t \in X(k)$ 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, $V(\alpha)$ 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 $V(\alpha)$ 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 $t_0 \in V(\alpha)$. Existe-t-il f comme dans (6.1), telle que t_0 soit de la forme $f(t'_0)$, avec $t'_0 \in \mathbf{P}_1(k)$?*

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 :

$$(6.3) \quad d(\alpha) = \deg P(\alpha) = \sum_{x \in \mathbf{P}_1(k)} [k(x):k].$$

(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 $d(\alpha) \leq 4$.*

(ii) *La question (6.1) a une réponse positive lorsque $n = 2$, $d(\alpha) = 5$, et que tout élément de $\text{Br}_2 k$ 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 $K' = k(T')$ qui tuent α : par exemple, on peut choisir K' tel que $[K':K] = 8$ dans le cas (i), et $[K':K] = 16$ dans le cas (ii).

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

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

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

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 A l'*anneau des adèles* de k , autrement dit le produit restreint des k_v ($v \in \Sigma$).

Soit $X(A) = \prod_v X(k_v)$ 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 $V_A(\alpha)$ défini de la façon suivante :

un point adélique $x = (x_v)$ appartient à $V_A(\alpha)$ 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, $V_A(\alpha)$ 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 :

$$V(\alpha) \subset V_A(\alpha),$$

et l'on peut se demander quelle est l'*adhérence* de $V(\alpha)$ dans $V_A(\alpha)$. 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 $V_A(\alpha)$, 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 :

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

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 $V_A(\alpha)$ et s'annule sur $V(\alpha)$; de plus, elle ne dépend que de la classe de β mod $\mathrm{Br}_n k$. Notons $V_A^M(\alpha)$ le sous-espace de $V_A(\alpha)$ défini par les « conditions de Manin » :

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

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

$$(7.3 ?) \quad V(\alpha) \text{ est dense dans } V_A^M(\alpha).$$

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 $\text{Sub}(\alpha) = \text{Br}_n k$ (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 $P_1(T), \dots, P_m(T)$ 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 $i = 1, \dots, m$. Alors il existe une infinité d'entiers $n > 0$ tels que $P_i(n)$ soit un nombre premier pour $i = 1, \dots, m$.]

Remarque

Le th. 7.6 peut être étendu aux *systèmes d'équations* $\alpha_i(x) = 0$, où les α_i sont des éléments de $\text{Br}_n K$ en nombre fini. On doit alors remplacer $\text{Sub}(\alpha)$ par l'ensemble des $\beta \in \text{Br}_n K$ 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 $H \rightarrow \infty$, le nombre des x tels que $H(x) \leq H$ 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 $H(x) \leq H$. On aimerait connaître la croissance de $N_\alpha(H)$ quand $H \rightarrow \infty$. 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 $N_\alpha(H) \ll H^2/(\log H)^{\delta(\alpha)}$ pour $H \rightarrow \infty$.*

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 $N_\alpha(H) \gg H^2/(\log H)^{\delta(\alpha)}$ 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), 2^e 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

1	Résumé du cours
21	<u>Cohomologie des extensions de groupes</u> : $1 \rightarrow N \rightarrow G \rightarrow \Gamma \rightarrow 1$.
23	On suppose $H^1(N, \mathbb{C}) = 0$: résidu ε : $H^m(G, \mathbb{C}) \rightarrow H^{m-1}(\Gamma, \text{Hom}(N, \mathbb{C}))$.
26	<u>Application aux corps locaux</u> ; Scindage.
37	Cas particulier de $\text{Br}_2 K$
40	Calcul des résidus ε à partir des symboles.
44	Fonctorialité.
47	Critère de nullité du résidu.
51	Lien avec K -théorie (de Milnor) et formes quadratiques.
55	Corestriction et résidus.
60	<u>Corps de fonctions d'une variable</u> . Les théorèmes.
66	Variante du th. d'Abel.
67	Calcul de $\text{Br}_2 K$ pour $K = \mathbb{R}(T)$ et $K = \mathbb{C}(X, Y)$.
70	Résidu d'un produit
71	Correction — et redémonstration
76	$\mathbb{Z}$ impair.
79	Formules variées.
90	Critère d'Albert
95	<u>Tout les symboles</u> ; Tancherski
98	Maître (4 ou 5 pôles)
107	Extensions de $\mathbb{Q}(T)$ à groupe de Galois $\text{SL}_2(\mathbb{F}_7)$, $6A_6$, $6A_7$.
110	<u>Obstruction de Manin</u> et exemples.
114	Problème : Schinzel $\Rightarrow$ Manin? (en fait : oui).
116	Majorections données par le critère.

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 $\mathbb{P}_1^1$.

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

Ceci a été fait pour la première fois par Faddeev ~ 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 :

(2)

On peut ~~se~~ 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)

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

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

(a) $H^q(N, C) = 0$, $q \geq 2$
(bouquet de cerclés).

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

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

Hypothèse supplémentaire sur C :

(b) N opère trivialement sur C . Alors

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

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

La suite spectrale dégénère en une suite

$$H^p(\Gamma, C) \rightarrow H^p(G, C) \xrightarrow{r} H^{p-1}(\Gamma, \text{Hom}(N, C)) \quad (3)$$

$$\rightarrow H^{p+1}(\Gamma, C) \rightarrow \dots$$

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 :

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

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 ,

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

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

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

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

La théorie élémentaire ~~des~~ des corps locaux nous dit que

$$1 \rightarrow \underset{\substack{\text{inerte} \\ I}}{I} \rightarrow G_K \rightarrow \Gamma \rightarrow 1$$

~~THEOREME~~

① Si: car $k=0$, alors I est isomorphe à $\varprojlim \mu_n$, $\mu_n =$ 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 Si: car $k=p > 0$, on a

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

I_1 = groupe d'inertie sauvage

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

$\text{cd } I = 1$, 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 $1 \rightarrow I \rightarrow G_k \rightarrow \Gamma$ 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 :

$$0 \rightarrow H^p(\Gamma, C) \rightarrow H^p(G_k, C) \rightarrow H^{p-1}(\Gamma, \text{Hom}(I, C))$$

$$\quad \quad \quad \parallel \quad \quad \quad \parallel$$

$$\quad \quad \quad H^p(k, C) \quad \quad \quad H^p(k, C)$$

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

Hypothèse : $n \neq 0$, pour un n premier à la caractéristique résiduelle.

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

$$\begin{array}{c} \mu_n^{\otimes (-1)} \\ C \otimes_{\mathbb{Z}/n\mathbb{Z}} \mu_n^{\otimes (-1)} \\ \parallel \\ \text{dual de } \mu_n \end{array}$$

La suite exacte prend la forme suivante:

(6)

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

r : résidu.

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

(α est holomorphe)

En termes de cohomologie étale:

$\text{Spec } A$ consiste en 2 points $\begin{matrix} \text{Spec } k \\ \text{Spec } K \end{matrix}$

C est vu comme un faisceau sur $\text{Spec } A$.

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:

$$0 \rightarrow \text{Br}_2 k \rightarrow \text{Br}_2 K \xrightarrow{r} H^1(k, \mathbb{Z}/2\mathbb{Z}) \rightarrow 0$$

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

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

Par le thm de Mordukgey, tout élé
de Br_k est somme de symboles.

$$(x, y) \quad x, y \in k^*$$

$$v: (x, y) \mapsto 1 \quad \text{si} \quad x, y \text{ unités} \quad (v(x)=v(y)=0)$$

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

où $\tilde{x}$ est ~~l'image~~ ^{l'image} de x dans k

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

On peut donc calculer tous les résidus.

Propriétés de fonctions

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

La flèche résidu.

$$H^p(K, \mathbb{C}) \rightarrow H^{p-1}(k, \mathbb{C}(-1))$$

est définie même si K n'est pas complet.

$$\downarrow \quad \uparrow$$
$$H^p(\hat{K}, \mathbb{C})$$

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 fr. rat du point corr.

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

$C = \Gamma$ -module annulé par n , $(n, \text{car}(k)) = 1$
si $\text{car}(k)$ est pair

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:

$$\sum_v \text{Cor}_{k(v)}^k r_v(\alpha) = 0$$

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

$$\text{Cor}_{k'}^k: H^p(k', \text{module}_{\Gamma_{k'}}) \rightarrow H^p(k, \text{module})$$

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

Hypothèse $X \simeq \mathbb{P}^1$ $\begin{cases} g=0 \\ \text{a un point rationnel} \end{cases}$

$$H^p(k, C) \rightarrow H^p(K, C)$$

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

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

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

D'un point de vue concret, ceci signifie :

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

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

On peut évaluer les classes de cohomologie en les points.

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

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

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

Dans l'exemple du groupe de Brauer :

on a une alg. d'Azumaya sur X .

On s'intéressera au quotient : élé' de $H^q(K, \mathbb{C})$ modulo $H^q(k, \mathbb{C})$.

Est-ce que ce quotient est isomorphe à

$$E_{X+q}(J, \mathbb{C}) \quad (C \text{ lin.})$$

$q=1$ action triviale de $\mathbb{C}$

$H^1(K, \mathbb{C})$ classe les $\mathbb{C}$ -alg. gal. sur K

(ext. ~~gals~~ de K)

Théorie de Riemann-Roch donne : $H^1(J, \mathcal{C})$.

(11)

Cas particulier :

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

$K = k(T) =$ corps de fonctions de $\mathbb{P}^1$.

$$0 \rightarrow \text{Br}_2 k \rightarrow \text{Br}_2 K \xrightarrow{r} \bigoplus_v k(v)^*/k(v)^{*-2}$$

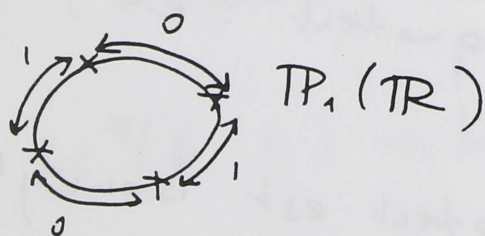
$\downarrow$
 k^*/k^{*-2}
 $\downarrow$
 1

$\prod_N \frac{k(v)}{k}$

Exemple : $k = \mathbb{R}$

v complexe : résidu = 0

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



nombre pair de pôles

$$\text{Br}_2 \mathbb{R} = \mathbb{Z}/2\mathbb{Z}$$

$\alpha \in \text{Br}_2 K$, on peut prendre sa valeur sur l'intervalle $\mathbb{R}$. Par continuité, cette valeur est constante. La valeur change lorsqu'on passe un pôle.

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

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

Th (Merte): 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 $\tilde{A} = 2 \cdot A_n$

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

Pour $n = 6, 7$

$$1 \rightarrow C_6 \rightarrow 6 \cdot A_n \rightarrow A_n \rightarrow 1$$

Première étape:

$$\begin{array}{c} E \\ | \\ A_n \\ \mathbb{Q}(T) \end{array}$$

que l'on aimerait plonger dans ext. gal.

$$\begin{array}{c} \tilde{E} \\ | \\ E \\ | \\ \mathbb{Q}(T) \end{array}$$

$$C = C_2 \text{ (6)}$$

14: Construire une telle extension
revient à

(13)

$$\begin{array}{ccc}
 & & A_n^{u,v} = C \cdot A_n \\
 & \nearrow & \downarrow \\
 G_K & \xrightarrow{\text{surj}} & A_n
 \end{array}$$

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

$$H^2(K, \mathbb{C}).$$

A démontrer: Si α est cette classe,

que $v_v(\alpha) = 0$ 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: la classe de cohomologie $\alpha \in H^2(K, \mathbb{C})$.

Mais $2 \neq 0$!

(14)

On voudrait changer de variable.

Question (conjecture):

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

$$\alpha \in H^2(k(\mathbb{P}_1), (2)) = \text{Br}_2(k(\mathbb{P}_1)).$$

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 $\mathbb{P}_1$, ce serait trivial.

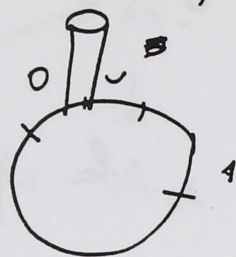
$\alpha \in H^2(K, (2))$ est tuée par une extension

Résultats partiels:

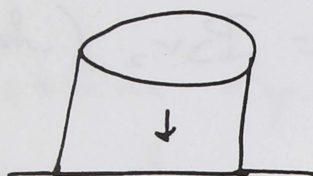
(15)

C'est vrai pour un corps local.

TR :



on peut demander
que l'image soit
petite, tombe
dans l'intervalle
 $\frac{0}{1}$.



TL (Mestre) : 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.

$$\begin{array}{ccc} E' & E & \text{(extensions} \\ \text{PSL}_2(\mathbb{F}_7) & | \text{ } \text{PSL}_2(\mathbb{F}_7) & \text{disjointes)} \\ | & & \\ k' = k(T') - k = k(T) & & \end{array}$$

↑ l'obstruction est nulle.

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

(2)

Surfaces rationnelles fibrées en coniques

(16)

(16)

 $\bar{k}$ -rationnelles S $\downarrow$ $\mathbb{P}^1$ fibre générique: conique
(courbe de genre 0)fibre exceptionnelle: 

$$K = k(\mathbb{P}^1)$$

$$S \rightarrow \alpha(S) \in H^2(K, \mathbb{Z})$$

 $\text{Br}_2 K$

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

Deux droites ne sont pas rat.

restes correspondent 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
exceptionnelles)

Conjecture:

(17)

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

Autrement dit, il existe une application rationnelle surjective $\mathbb{P}^2 \xrightarrow{\sim} S$

(et on peut exiger que $P \in \text{image de } \mathbb{P}^2(k)$)

La Conjecture précédente entraîne celle-ci.

$\alpha \in \text{Br}_2 k$ correspond à S

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

$$\begin{array}{ccc} S_1 & \rightarrow & S \\ \downarrow & & \downarrow \\ \mathbb{P}^1 & \xrightarrow{\sim} & P \in \mathbb{P}^1 \end{array}$$

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 de $\mathbb{P}^2$)

$\alpha \in \text{Br}_2$

$\alpha = (x, y)_L$ décomposables

$\rightarrow$ fibres coniques.

Exercice:

Soit k un corps pour lequel la conjecture d'annulation dans $\alpha \in \text{Br}_2(k(T))$ est valable.

(18)

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

Autre conséquence

$$\alpha \in \text{Br}_2 k(T), \quad k \text{ i-h-i}, \quad \text{car } (k) \neq 1.$$

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

$$\begin{array}{c} \text{---} \cdot \text{---} \\ \quad v \end{array} \quad v \in TP_1(k)$$

Conjecture : . 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 : Estimer

le nombre des v avec $\alpha(v) = 0$.

$$TP_1, \quad v \in TP_1(\mathbb{Q}) \quad (k = \mathbb{Q})$$

$$\alpha \in \text{Br}_2 \mathbb{Q}(T).$$

On s'intéresse à l'ensemble des v tels que

$$\alpha(v) = 0. \quad \text{Manin voudrait une borne}$$

supérieure pour $\#\{v \mid \alpha(v) = 0, H(v) < N\}$.

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

$$H(v) = \sup(p, q)$$

Théorème

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

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

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 Mestel.

Variante: Prendre TP_n au lieu de TP_1 .

Prendre Aff^n .

Exemple: Aff^1 T

$$\alpha = (-1, T)$$

$$T \rightarrow t \in \mathbb{Z}$$

$$(-1, t) = 0$$

$\Leftrightarrow$ t est somme de 2 carrés

Estimer le nombre de t sommes de 2 carrés,

$t \leq N$. Conjecture donc:

$$\ll \frac{N}{\log N}$$

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

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

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

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

Définir notion de résidu.

(1) Cohomologie des extensions de groupes.

G groupe profini.

N s/g invariant (fermé) de G

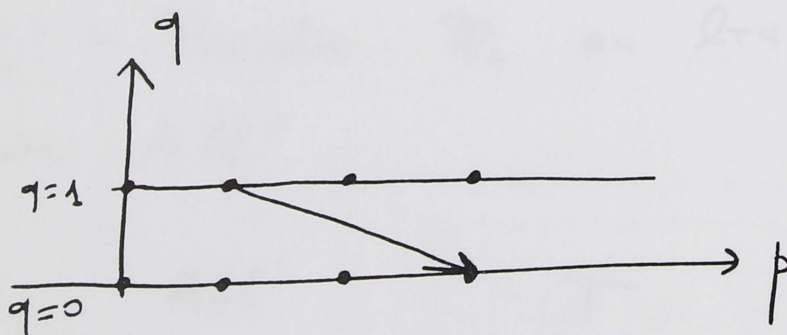
$$\Gamma = G/N$$

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

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

$$\dots \rightarrow H^n(\Gamma, C) \rightarrow H^n(G, C) \xrightarrow{\sim} H^{n-1}(\Gamma, \text{Hom}(N, C))$$

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

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'expliquer.

Construction de Hochschild :

Filtration des cocycles sur G , à valeurs de $\mathbb{C}$ (en fait, de "cocycles normalisés")

$f(g_1, \dots, g_n)$ à valeurs de $\mathbb{C}$
normalisé si: $f=0$ chaque fois que l'un des g_i est l'élément neutre.

Le k 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 T .

$$\begin{aligned} \text{(i.e. } f(g_1, \dots, g_{n-k}, g_{n-k+1}^{v_1}, \dots, g_{n-k+1}^{v_k}) \\ = f(g_1, \dots, g_n) \\ \text{pour } v_i \in N. \end{aligned}$$

Il résulte de cette construction (sous

l'hypothèse ①) que tout n -cocycle f sur G est ~~cohomologue~~ à val. de $\mathbb{C}$

est cohomologue à un cocycle f tel que
 f normalise', et $f(g_1, g_2, \dots, g_n) \equiv$
 (*) | dépend que des classes de $g_2, \dots, g_n \pmod N$

Description de r .

Si α est la classe de f dans $H^n(G, \mathbb{C})$,
~~l'élément~~ $r(\alpha)$ contient le $(n-1)$ -cocycle

$r(f)$ défini par:

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

$\gamma_i \in \Gamma \quad v \in N$

où les g_i sont des éléments des γ_i
 dans G .

Cas particuliers:

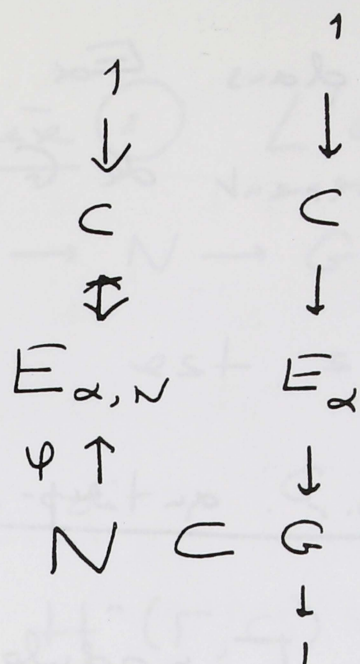
$n=1$ $H^1(G, \mathbb{C}) \rightarrow H^0(\Gamma, \text{Hom}(N, \mathbb{C}))$

homomorphisme croisé $G \rightarrow \mathbb{C}$	restr. à N	$\rightarrow$	homomorphisme $N \rightarrow \mathbb{C}$
---	--------------	---------------	---

invariant par Γ

"Flèche de restriction"

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



La restriction de α à N est 0

On a un élément de N à E_{α} .

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

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

O - a un Γ -groupe $\text{Hom}(N, C)$
P - Γ -principal homogène sous $\text{Hom}(N, C)$

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

Théorème: Cet invariant est $-v(\alpha)$.

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

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

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

$$C_1 \times C_2 \rightarrow C$$

Γ -modules

$$H^n\left(\frac{N}{B}, C_1\right) = 0, \quad n \geq 2$$

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

d'où par inflation

$$p: G \rightarrow \Gamma \quad p^*(\alpha)$$

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

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

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

$$\text{Hom}(N, C_1) \times C_2 \rightarrow \text{Hom}(N, C)$$

Formule pour définir le cup-produit:

φ, ψ ~~de~~ n_1, n_2 -cocycles

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

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

Hypothèse (2) $\angle$ extension

$$1 \rightarrow N \rightarrow G \rightarrow \Gamma \rightarrow 1$$

est scindée ;

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

D'où $H^n(\Gamma, c) \rightarrow H^n(G, c)$ est injective.

(et même facteur direct).

D'où

$$0 \rightarrow H^n(\Gamma, c) \rightarrow H^n(G, c) \xrightarrow{\gamma} H^{n+1}(\Gamma, \text{Hom}(N, c)) \rightarrow 0$$

Ces suites exactes sont scindées, mais pas canoniquement.

Deuxième étape : 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

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

G_K

Structure de G_K

$$1 \rightarrow I \rightarrow G_K \rightarrow G_k \rightarrow 1$$

I = groupe d'inertie.

$$1 \rightarrow I_1 \rightarrow I \rightarrow I^{\text{mod}} \rightarrow 1$$

où I est un pro- p -groupe

I^{mod} est isom (pas canonique) à

$$\prod_{l \neq p(k)} \mathbb{Z}_l$$

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

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

Soit L/K une extension finie galoisienne.

A_L , k_L — entiers, corps résiduel.

$$G \rightarrow \text{Gal}(k_L/k)$$

k_L extension normale de k (pas nec. séparable
 (ext. gal. d'une ext. radiale))

$$G \rightarrow \text{Gal}(k_L/k) \text{ surjectif,}$$

noter 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

$I_1 \rightarrow I_G \rightarrow k_L^*$, image ρ_n
(racines de 1)

↑
noyau

On montre que I_1 est un p -groupe.

Normalisateur de l'isomorphisme $I^{\text{mod}} \simeq \varprojlim \rho_n$.

k_s : clôture séparable de k .

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

$\mapsto K'/K$ non variable, d'ext.és.
 k'/k .

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

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

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

K_s
|
 K_{nr}
|
 K

$I = \text{Gal}(K_s/K_{nr})$
 $= \text{Gal}(\hat{K}_s/\hat{K}_{nr})$.

Si $(n, p(k)) = 1$, on définit une

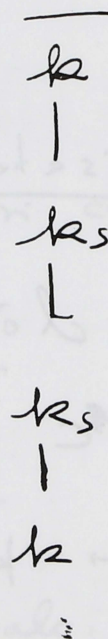
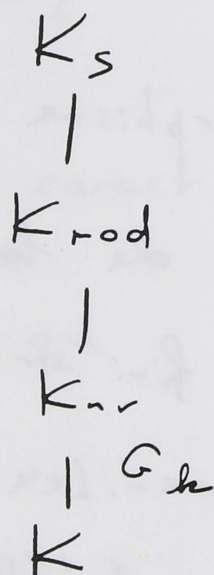
extension $K_{nr, n} = K_{nr}(\sqrt[n]{\pi})$

indépendante du choix de π

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

$s \in \text{Gal} \quad s(\pi_n)/\pi \longrightarrow$ des corps résiduels

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



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

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

I_1 pro- p -groupe.

Théorème:

L'extension $1 \rightarrow I \rightarrow G_k \rightarrow G_{k-1} \rightarrow 1$ est scindée

1^{ère} étape: on peut relever mod I_1 .

L'extension

$$1 \rightarrow I^{\text{mod}} \rightarrow G_k / I_1 \rightarrow G_k \rightarrow 1$$

est scindée

"Non-démonstration" (convaincant).

$$\in H^2(G_k, \varprojlim \mu_n) \quad \text{Ds} \quad H^2(G_k, \mu_n) \ni \sigma_n$$

" $\text{Br}_n(k)$

Prouver par propr. de fonctorialité que obst. = 0
non-démonstration $\rightarrow$ démonstration.

Démonstration (difficile)

$$K_n \quad K_n(\pi^{1/n})$$

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

$K(\pi_n)$ est linéairement disjoint de

$$K_n / K, \quad K(\pi_n) K_n = K_n(\pi^{1/n})$$

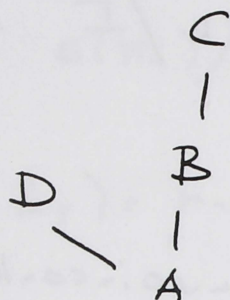
$$\rho_n \rightarrow \text{Gal}(K_n(\pi^{1/n})/K) \rightarrow G_k \rightarrow 1$$

Scindage: le s/g $\text{Gal}(K_\infty(\pi^{1/n})/K(\pi_n))$

donne un élément de G_k .

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

Idee:



$$C = D \otimes B.$$

Ext. scindée: le s/g correspondant étant forme' des st G_k/I_i qui fixent tous les π_n .

Proposition: Toute extension de G_k par un pro- p -groupe est scindée.

Théorème: Si k est de car. $p > 0$,
on a $\text{cd}_p(G_k) \leq 1$.

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 $i=2$ (devissage).

$$0 \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow k_s \xrightarrow{\varphi} k_s \rightarrow 0$$

$$\varphi(x) = x^p - x$$

$$H^i(G_{\bar{k}}, k_s) = 0 \quad \text{pour tout } i \geq 1$$

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. radicales donnent des choses non

triviales. Par ex. $\text{Br}_p(k)$ peut être $\neq 0$

$$1 \rightarrow N \rightarrow G \rightarrow \Gamma \rightarrow 1$$

$$1 \rightarrow I \rightarrow G_k \rightarrow G_{\bar{k}} \rightarrow 1$$

Théorème:

(a) $\text{cd}_\ell I = 1$ si $\ell \neq p$

(b) $\text{cd}_p I = 1$ si $\text{car } K = p$
 ou si $\text{car } K = 0$
 et k parfait

≥ 2 si $\text{car } K = 0$ 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 $\text{car } K = p$, $I = \text{Gal}(K_s / \underline{\underline{K_{\text{ur}}}})$
 on a $cd_p I \leq 1$, car p
 d'où $= 1$ car $I_1 \neq \{1\}$.

b') Si $\text{car } K = 0$, k parfait.
 Quitte à remplacer K par $\bar{K_{\text{ur}}}$,
 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. de K de degré $<$ nombre de variables a une solution non triviale)

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

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

34

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 -ième.

Soit z une racine primitive p -ième de 1.
Soit $(\pi, u) \in \text{Br}_p(K)$.

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

$$\text{Br}_p(K) \neq 0 \Rightarrow \text{cd}_p(\mathbb{Q} G_K) \geq 2$$

Cas considéré par la suite:

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

(voir Kato)

On définit $C(-1) = \text{Hom}(\mu_n, C)$.

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

Théorème: $0 \rightarrow H^m(G_k, C) \rightarrow H^m(G_k, C) \rightarrow$

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

Scindage de l'extension

$$H^i(I, C) = 0, \quad i \geq 2 \quad \text{cd}_\ell I \leq 1.$$

$$C(-1) = \text{Hom}(I, C)$$

$$\text{Hom}(I/I_1, C)$$

$$\text{Hom}(J_1, C).$$

Remarque: r peut être défini même si K n'est pas complet.

K muni de v , $k(v) = \text{corps résiduel}$

C un G_K -module, annihilé par v

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

On a alors un homomorphisme

$$r: H^m(G_K, C) \xrightarrow{r_v} H^{m-1}(G_{k(v)}, C(-1))$$

$$\downarrow \quad \quad \quad \nearrow \hat{r}_K$$

$$H^m(G_K, C)$$

En termes de topologie étale:

A anneau de val,

$$T = \operatorname{Spec} A \quad \text{"trait"}$$

$$\text{point fermé} \quad \operatorname{Spec}(k) = 1_k$$

$$\text{ouvert} \quad \operatorname{Spec}(K) = 1_K$$

$$j : 1_K \rightarrow T$$

On regarde C comme faisceau étale sur A .

Supposons A complet.

$$R^q_{j*} C = \begin{cases} C & q=0 \\ C(-1) & q=1 \\ 0 & q \geq 2 \end{cases} \quad \begin{array}{l} \text{concentré} \\ \text{au pt} \\ \text{fermé} \\ 1_K \end{array}$$

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, $H^p(T, C) = H^p(1_K, C)$

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

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.

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

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

"

$$r: \text{Br}_n(k) \rightarrow \text{Hom}(G_k, \mathbb{Z}/n\mathbb{Z})$$

Calcul de $\text{Br}(k)$ 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

$$1 \rightarrow U_{nr} \xrightarrow{\pi} K_{nr}^* \xrightarrow{\text{tr}} \mathbb{Z} \rightarrow 0$$

$\downarrow \pi^*$

surlevée (par le choix de π).

Donc suite exacte

$$0 \rightarrow H^2(U_{nr}) \rightarrow \text{Br}(k) \rightarrow H^2(G_k, \mathbb{Z})$$

"

$$\text{Hom}(G_k, \mathbb{Q}/\mathbb{Z})$$

$$H^2(\bar{k}^*)$$

"

$$\text{Br}(k)$$

Suite exacte de Witt :

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

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

Proposition : $r_w = -r$.

Cas particulier $n=2$ (et $r = r_w$).

$$r : Br_2(K) \longrightarrow Hom(G_k, \mathbb{Z}/2\mathbb{Z})$$

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

Formule pour r :

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

$$(u, v) \quad u, v \text{ unités}$$

$$(u, \pi) \quad u \text{ unité}$$

$$(\text{car } (\pi, \pi) = (\pi, -1)).$$

$$r(u, v) = 0$$

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

où $\bar{u}$ est l'image de u dans k .

Résidu 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

$$0 \rightarrow H^m(G_k, C) \rightarrow H^m(G_k, C) \xrightarrow{\sim} H^{m-1}(G_k, C(-1))$$

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

$$0 \rightarrow H^n(k, \mathbb{Z}) \xrightarrow{i} H^n(K, C) \xrightarrow{r} H^{m-1}(k, C(-1)) \rightarrow 0$$

$$1 \rightarrow I \rightarrow G_k \rightarrow G_k \rightarrow 1$$

Suite exacte scindée (par le choix d'une uniformisante).

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

$$(x) \xleftarrow{\psi} x$$

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

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

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

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

$$r((\pi) \cdot i(\alpha)) = \alpha$$

r pour $n=1$:

$$H^1(K, C) \rightarrow H^0(k, C(-1))$$

(40)

Preons $C = \mu_n$.

$$H^1(K, \mu_n) \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$$

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

$\parallel$

$$K^*/K^{*n}$$



$$\text{La flèche } K^*/K^{*n} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$$

est donnée par la valuation:

$$x \mapsto v(x) \pmod{n}.$$

$$\text{On a } v(\alpha, i^*(\alpha_2)) = v(\alpha_1) + \alpha_2$$

(formule de projection).

$$\text{D'où } v((\pi) \cdot i(\alpha)) = 1 + \alpha = \alpha.$$

Ceci donne une autre façon de voir v :

$$H^n(K, C) = H^n(k, C) \oplus (\pi) \cdot H^{n-1}(k, C(-1)).$$

Application aux symboles galoisiens dans

$$\text{Br}_n(K) = H^2(K, \mu_n).$$

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

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

(41)

$$(x, y)_n \in \text{Br}_n(K) = H^2(K, \mu_n)$$

$$\parallel$$

$$(x)(y)$$

$$(x), (y) \in H^1(K, \mu_n) \quad \text{Donc}$$

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

$$\text{on a} \quad (x) \cdot (y) = - (y)(x)$$

$$\text{Br}_n(K) = \text{Br}_n(k) \oplus (\pi) H^1(k, \mathbb{Z}/n\mathbb{Z})$$

$\parallel$

$$H^1(k, \mu_n)$$

$\parallel$

$$k^*/k^{*n}$$

Si u_1, u_2 sont des unités de K

$(u_1, u_2) \in \text{Br}_n(K)$, appartient à $\text{Br}_n(k)$.

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

u unité de K

$$(\pi, u) \in \text{Br}_n(K)$$

$$(\pi, u) = (\pi)(\bar{u})$$

$$\bar{u} \in H^1(k, \mathbb{Z}/n\mathbb{Z})$$

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

Ceci permet de calculer v pour tous les symboles.

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

Il suffit de calculer ce résidu lorsque

$$x = \pi, y = u \quad v = (\tilde{u})$$

$$x = u_1, y = u_2 \quad v = 0$$

$$x = u, y = \pi \quad v = -(\tilde{u})$$

$$x = \pi, y = \pi \quad v = (-1)$$

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

(Cas particulier $n=2$, $p_2 \cong \mathbb{Z}/2\mathbb{Z}$)

Comparaison de la suite exacte avec celle de Witt.

Supposons k parfait.

Comparaison avec la décomposition de Witt du groupe de Brauer.

$$(Witt) \quad 0 \rightarrow Br(k) \rightarrow Br(K) \xrightarrow{r_W} Hom(G_k, \mathbb{Q}/\mathbb{Z}) \rightarrow 0.$$

K_{nr} extension non ramifiée maximale de k .

$$\begin{array}{c} K_{nr} \\ | \\ G_k \\ | \\ K \end{array} \quad Br(K) = H^2(G_k, K_{nr}^*).$$

$$1 \rightarrow U_{nr} \rightarrow K_{nr}^* \xrightarrow{\varphi} \mathbb{Z} \rightarrow 0$$

Donc

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

$$\cong \downarrow$$

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

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

(43)

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

$$\cong \downarrow \delta$$

$$H^2(G_k, \mathbb{Z})$$

On obtient ainsi la suite exacte de Witt

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

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

~~n , premier à p car.~~

$$0 \rightarrow \text{Br}_n(k) \rightarrow \text{Br}_n(K) \xrightarrow{r_w} \text{Hom}(G_k, \mathbb{Z}/n\mathbb{Z})$$

Proposition :

$$r_w = -r$$

pour tout n
premier à $p(k)$

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

$$\cap \\ \text{Hom}(G_k, \mathbb{Z}/n\mathbb{Z})$$

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

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

π uniformisante de K . On peut voir π comme

$$\pi \in H^0(K, G_n)$$

$$\pi \cdot \delta_x \in H^2(K, \mathbb{Q}_n) = B_v(K)$$

(44)

$$\pi \cdot \delta_x \in B_{v_n}(K).$$

$$\text{On a : } v_w(\pi \cdot \delta_x) = X.$$

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

"

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

$$X \cdot (\pi)$$

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

"

$$-(\pi) \cdot X$$

$$X \cdot (\pi) \in H^2(K, \mu_n) = B_n(K).$$

$$v((\pi) \cdot X) = X$$

D'où le signe - dans la formule.

Changement de corps local

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

$$v_2|_{K_1^*} = e \cdot v_1$$

$$e \in \mathbb{N}, e \geq 1$$

indice de ramification.

$k_1 \subset k_2$ corps résiduels.

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

$$G_{k_2} \rightarrow G_{k_1}$$

(On ne suppose pas K_2 fini sur K_1).

C un G_{k_1} -module.

(45)

$$H^n(K_1, C) \xrightarrow{r_1} H^{n-1}(k_1, C(-1))$$

$$\downarrow \text{Res}$$

$$\downarrow e.\text{Res}$$

$$H^n(K_2, C) \xrightarrow{r_2} H^{n-1}(k_2, C(-1))$$

diagramme commutatif.

Proposition: Ce diagramme est commutatif.

$$1 \rightarrow N_1 \rightarrow G_1 \rightarrow \Gamma_1 \rightarrow 1$$

$$\uparrow$$

$$\uparrow$$

$$\uparrow$$

$$1 \rightarrow N_2 \rightarrow G_2 \rightarrow \Gamma_2 \rightarrow 1$$

$$r: H^n(G_1, C) \rightarrow H^{n-1}(\Gamma_1, \text{Hom}(N_1, C))$$

$$\downarrow$$

$$\hookrightarrow$$

$$\downarrow$$

$$\longrightarrow$$

On a fait l'identification

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

"

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

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

$$I_{2,n}^{\text{mod}} \rightarrow I_{1,n}^{\text{mod}}$$

$$\begin{array}{ccc} \parallel & & \parallel \\ \mu_n & \xrightarrow{e} & \mu_n \end{array}$$

car on a

regarde'

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

et ceci donne l'ison.

Or, $\pi_1 = \pi_2^e \cdot u$ u unite'
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, $V \cong \mathbb{Z}$)

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

$w \in V$

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

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

$$I_n^{\text{mod}} \rightarrow \text{Hom}(V_K, \mu_n)$$

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

Ceci permet de voir la factorielle en K :

$$\begin{array}{ccc} & & K_2 \\ & \swarrow & \\ K_1 & & \\ & \searrow & \\ & & V_{K_2} \\ V_{K_1} & \xrightarrow{\quad} & \\ \mathbb{Z} & \xrightarrow{\quad} & \mathbb{Z} \end{array}$$

K corps muni d'une valuation discrète v .

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

$$\begin{array}{c} \text{"} \\ k(v) \end{array}$$

Critère de nullité 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 $\varphi: G_k \rightarrow G$ un homomorphisme.

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

Hypothèse :

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

(" C est non ramifiée en v ")

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

(Dans l'exemple de Mestre: $K = \mathbb{Q}(\tau)$,
 $G = \text{PSL}_2(\mathbb{F}_3)$, $C = \mathbb{Z}/2\mathbb{Z}$, v place
 $\bar{a}$ l'infini, $e_\psi = 3$ (ou 9?))

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

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

Théorème: $e_\psi \cdot r(\psi^* \alpha) = 0$

Corollaire: Si $(e_\psi, n) = 1$, $r(\psi^* \alpha) = 0$.

(Mestre: $\alpha \in H^2(C, \mathbb{Z}/2\mathbb{Z})$, $\tilde{G} = \text{SL}_2(\mathbb{F}_3) \rightarrow G$
 classe de cette extension = α .

Le corollaire dit qu'il n'y a pas de résidu
 $\bar{a}$ l'infini)

On peut supposer K complet

① Cas particulier " ψ non ramifié"
 ψ trivial sur I_K .

$$\begin{array}{ccc} G_K & \xrightarrow{\psi} & G \\ & \searrow & \swarrow \\ & G_K & \end{array}$$

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

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

On a alors $v(\psi^* \alpha) = 0$

(49)

(2) Cas général

Lemme: Il existe $K' \subset K_S$, $[K':K] = e$
de corps résiduel k' avec k' ~~radical~~ radiciel
sur k .

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

On admet le lemme.

On applique au couple K, K' la ~~propriété~~
proposition:
 $e_\psi = |\psi(I_K)|$.

$$v_{K'}(\psi^* \alpha) = e v_K(\psi^* \alpha)$$

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

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

$$e_\psi = e \cdot p^s$$

$$p^s = [k':k]$$

Par (1) appliqué à K' , on a

$$v_{K'}(\psi^* \alpha) = 0.$$

D'où $e \cdot v(\psi^* \alpha) = 0$

et a fortiori $e_\psi \cdot v(\psi^* \alpha) = 0$.

$$\varphi: G_K \rightarrow G$$

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

$$I'_K = \text{Ker } \varphi: I_K \rightarrow \varphi(I_K).$$

I'_K est un s/g ouvert de I_K
d'indice $e\varphi$.

Ce s/g est normal dans G_K .

On a un 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 $e\varphi$.

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

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

Radical sur k .

$$1 \rightarrow I_K \rightarrow G_K \rightarrow G_k \rightarrow 1$$

$$G_{K'} \nearrow \text{surjectif}$$

Ceci entraîne que k'/k est radical
(mais pas nec. $k=k'!!$).

Parethese:

Comparison 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:

$$K_*^M F = \bigoplus_{n \geq 0} K_n^M F$$

$$K_0 F = \mathbb{Z}$$

$$K_1 F = F^\times$$

eng. par $K_1 F$

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

$$(x)(1-x) = 0 \quad x \in F^\times, x \neq 1$$

ds $K_2 F$

On prend l'algèbre engendrée sur $\mathbb{Z}$ par F 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

$$\begin{array}{ccc} (\pi, u_1, \dots, u_{n-1}) & \longmapsto & (\tilde{u}_1, \dots, \tilde{u}_{n-1}) \\ \cap & & \cap \\ K_n(K) & & K_{n-1}(k) \end{array}$$

π uniformisant

$u_1, \dots, u_{n-1}$ unités

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

On travaille avec $K_n(K)/n \cdot K_n(K)$

et on construit un homomorphisme

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

n premier à $\text{car}(K)$.

L'existence résulte d'un théorème de Tate

I. M. 1976

$n=2$, Milnor 1970.

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

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

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

θ commute au résidu.

(53)

K local.

$$\begin{array}{ccc} K_n(K)/_n K_n(K) & \xrightarrow{\sigma_K} & H^n(K, \mu_n^{\otimes n}) \\ \downarrow \nu^M & & \downarrow \nu \\ K_{n-1}(k)/_n K_{n-1}(k) & \xrightarrow{\sigma_k} & H^{n-1}(k, \mu_n^{\otimes n-1}) \end{array}$$

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

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

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

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 .

Ide'el fondamental : I_K .

$$0 \rightarrow I_K \rightarrow W_K \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$$

K corps local, π uniformisant.

(54)

f corps quadratique sur K

f anisotrope (ne représente pas 0)

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

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

u_i unités

aniso. après réduction sur k

Plongement naturel

$$W_k \hookrightarrow W_K$$

on relève les coeff. (i.e. de p du relèvement)

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

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

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

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

$$I_K^m / I_K^{m+1} = I_k^m / I_k^{m+1} \oplus I_k^{m-1} / I_k^m$$

$$0 \rightarrow I_k^m / I_k^{m+1} \rightarrow I_K^m / I_K^{m+1} \rightarrow I_k^{m-1} / I_k^m \rightarrow 0$$

(indépend. du choix de π).

$$\begin{array}{ccc} & & \downarrow e \\ & \downarrow e_m^k & \downarrow e \\ 0 \rightarrow & H^m(k, \mathbb{Z}/2\mathbb{Z}) \rightarrow & H^m(K, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^{m-1}(k, \mathbb{Z}/2\mathbb{Z}) \rightarrow 0 \end{array}$$

Si les flèches existent, le diagramme est commutatif (dans les 2 théories,

$$(\pi, u_1, \dots, u_{n-1} \rightarrow u_1, \dots, u_{n-1})$$

Flèches existent pour $m \leq 4$ (Jacob-Roth. I.M. 1989).

Corestriction et résidus :

$K' \supset K$ ext. finie,

C un G_K -module, on veut définir

$$\text{Cor}: H^m(G_{K'}, C) \rightarrow H^m(G_K, C)$$

$$\overline{K} - K' - K$$

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

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

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

Définition : $\text{Cor}_{K'/K} = [K':K] \cdot \text{Cor}_{G_{K'}/G_K}^{G_{K'}}$

Pourquoi est-ce raisonnable ?

$$H^0 \longrightarrow \text{trace}$$

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

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

$$\text{Cor}_{K'/K} : K'^\times / K'^{\times n} \longrightarrow K^\times / K^{\times n}$$

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

Cas local complet :

C. G_K -module

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

Proposition:

Le diagramme suivant est commutatif :

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

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

Il nous restera voir qd dans toute la suite exacte :

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

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

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

Démonstration la prochaine fois.

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

$$G' \subset G \quad \text{indice fini} \quad H' \subset H \quad G'/H' \subset G/H$$

$$H^*(G', C) \xrightarrow{\text{Cor}} H^*(G, C) \quad (G = G_k, H = \text{inerti})$$

28 oct 91

cours 4

pas de cours
les 4 et 11 nov.Restait à démontrer lemme de compatibilité
coréstriction/residu. K'/K corps locaux, ext séparable. k'/k : corps résiduels $C : G_K$ -module annulé par n ($n, p(k)) = 1$.

lemme

$$\begin{array}{ccc} \text{on a diagramme} & H^n(K, C) & \xrightarrow{\pi_K} H^{n-1}(k, C(-1)) \\ \text{commutatif} & \uparrow \text{Cor} & \uparrow \text{Cor} \\ & H^n(K', C) & \xrightarrow{\pi_{K'}} H^{n-1}(k', C(-1)) \end{array}$$

$$(\text{on rappelle : } \text{Cor}_{k'}^k : H^*(k') \rightarrow H^*(k))$$

$$i = [k' : k]_{\text{inert}}$$

$$H^*(G_K) \xrightarrow{i} H^*(G_{K'})$$

pf : Il suffit de traiter 2 cas

- 1 K'/K non-ramifiée ($e=1$ et $[k' : k]_i = 1$)
- 2 k'/k est radiciel.

$$\begin{array}{ccc} 0 \rightarrow H^n(k, C) \rightarrow H^n(K, C) \xrightarrow{\pi_K} H^{n-1}(k, C(-1)) & \left| \begin{array}{l} \text{où pr} \\ \alpha \in H^n(k', C) \\ \pi_{K'}(\alpha) = 0 \end{array} \right. \\ \uparrow e \cdot \text{Cor} \quad \uparrow \text{Cor} & & \\ 0 \rightarrow H^n(k', C) \rightarrow H^n(K', C) \rightarrow H^{n-1}(k', C(-1)) & \left| \begin{array}{l} \text{Cor } \alpha : \\ \pi_K(\text{Cor } \alpha) = 0. \end{array} \right. \end{array}$$

Cas 1 - π unif de K , est une unif de K' . $\alpha \in H^n(K', C)$. Peut s'écrire

$$\alpha = \alpha_0 + (\pi) \cdot \beta \quad \begin{array}{l} \text{où } \alpha_0 \in H^n(k', C) \\ \text{sup prod} \quad \beta \in H^{n-1}(k', C(-1)) \\ \left\{ \begin{array}{l} (\pi) \in H^1(K', \mu_n) \\ \text{unif} \end{array} \right. \end{array}$$

$$\pi_{K'}(\alpha) = \beta$$

$$\text{formule connue : } \text{Cor } \alpha = \text{Cor } \alpha_0 + (\pi) \cdot \text{Cor } (\beta)$$

$$\text{d'où } \pi_K(\text{Cor } (\alpha)) = \text{Cor } (\beta).$$

Cas 2: π' unif de K' .

$$N\pi' = \pi' \cdot u$$

où π' est une unif de K
 u unité

$$i = [k_s : k]_i$$

$$\text{réduct} \Rightarrow H^*(k, C(-1)) \simeq H^*(k', C(-1))$$

$$\text{on écrit } \alpha = \alpha_0 + (N\pi') \cdot \beta$$

$$\text{où } \beta \in H^{n-1}(k, C(-1))$$

(identifiée par restriction
 à un elut de k' , de k)

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

$$\iota((N\pi') \cdot \beta) = i\beta = \text{Cor}_{k'}^k \beta$$

□

Désormais on laissera tomber les art radicielles,
 on pourra récupérer cas unsep à la fin à
 partir du cas separable.

III Corps de fonction d'une variable

~~($\bar{k} \subset k \subset K$ avec k alg. fermé ds K)~~

k parfait

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

$K = k(X)$: corps des fonctions sur X

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

$$\begin{array}{c} K_S \\ \downarrow N \\ \bar{k} \otimes K = \bar{k} \cdot K \\ \downarrow G_k \\ K \end{array} \quad G_K$$

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

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

$$N = \text{Gal}(K_S/\bar{k}K)$$

Corps des fct de X sur $\bar{k}$.

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

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

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

Soit $G_w \subset G_K$ le gpe de décomp de w

(l'ens des $s \in G_K$, $sw = w$).

$G_w \cong \text{Gal}(K_{S,w}/K_S)$ où $K_{S,w}$ = complétion de K pour v .

(on a clairement $G_{K_S} \twoheadrightarrow G_w$)

don: pas évident. lemme d'approx. -
ou Krasner).

par la théorie locale: on a relevé
de G_k ds G_{K_S}

$$\begin{array}{ccc} G_w & \cong & G_{K_S} \\ & \searrow & \downarrow \uparrow \\ & & G_k \end{array}$$

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

(61)

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

Prop : $cd_k N = 1$

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

$H^n(G_k, C) \rightarrow H^n(G_K, C)$ est injective
(et m une injection directe i.e. "split injection" : $\exists$ relv)

Prop Soit δ le pgcd des degrés des pls formés de X
(sens des schémas)

Si $(\delta, n) = 1$, les flèches

$H^n(k, C) \rightarrow H^n(K, C)$ sont injectives.

pf On va à couper C en morceaux, on peut supposer
 $n = \ell^{\alpha}$, ℓ premier.

Par hypothèse, il y a un $P \in X$, deg P premier à ℓ

$k(P) = \bar{k}$, $[k' : k] = d$, $(d, \ell) = 1$.

Sur k' : $H^n(k', C) \rightarrow H^n(k'K, C)$ est inject, par N.B

$H^n(k, C) \xrightarrow{\text{inject car } (d, \ell) = 1} H^n(k', C) \xrightarrow{\quad} H^n(K, C)$

$\square$

Ça nous suffit, mais ça laisse entier des tas de pbs :

(contre) e.g car $\neq 2$

X courbe de genre 0 sans pt rat

$\uparrow$
 $\alpha \in \text{Br}_2(k)$, α décomposable
 $H^1(k, \mathbb{Z}/2\mathbb{Z})$

$$L = \mathbb{Z}/2\mathbb{Z} \quad , \quad \text{Ker} \left(H^m(k, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^m(k, \mathbb{Z}/2\mathbb{Z}) \right) = ?$$

$$\text{Ker} = 0 \quad \text{si } m=1$$

$$\text{Ker} = \{0, \alpha\} \quad \text{si } m=2$$

$$\text{Ker} = \{0, \alpha\} \cdot H^1(k, \mathbb{Z}/2\mathbb{Z}) \quad \text{si } m=3 \quad (\text{Arason})$$

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

On va maintenant s'occuper des résidus -

v val discrète de K triviale s/b_k

$\Leftrightarrow$ pb forme de courbe X

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

$k(v) =$ corps résiduel corresp.

$\uparrow$
orbites de G_k agissant sur $X(\bar{k})$

Pour chaque v , on a

(rappel $C(-1) = C \otimes (p_n)^\vee = \text{Hom}(p_n, C)$)

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

residu :

On démontre (aujourd'hui) :

Pour $\alpha \in H^m(K, C)$ donné :

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

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

Thm 2 : Si $X = \mathbb{P}^1$, on a une suite exacte

$$0 \longrightarrow H^m(k, C) \xrightarrow{(r_v)} \bigoplus H^{m-1}(k(v), C(-1)) \xrightarrow{\sum \text{Cor}} H^{m-1}(k, C(-1)) \longrightarrow 0$$

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

$$0 \longrightarrow H^{m-1}(k, J_n \otimes C(-1)) \longrightarrow H^m(K, C) / H^m(k, C) \longrightarrow$$

$$\bigoplus H^{m-1}(k(v), C(-1)) \longrightarrow H^{m-1}(k, C(-1)) \longrightarrow 0$$

$\uparrow$
 $\text{Ker de } \theta \rightarrow$

voir errata :
page 10
18 nov.

où J_n est le G_K -module $\text{Ker } n: J(\bar{k}) \rightarrow J(k)$
 $J_n \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ 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

$$1 \rightarrow N \rightarrow G_K \rightarrow G_{\bar{k}} \rightarrow 1$$

$$N = G_{\bar{k}/K}, \quad \text{cd } N = 1.$$

par suite spectrale, on sait

$$\cdots \rightarrow H^n(k, \mathbb{C}) \rightarrow H^n(K, \mathbb{C}) \xrightarrow{\sim} H^{n-1}(G_K, \text{Hom}(N, \mathbb{C})) \rightarrow \cdots$$

pb : étudier $\text{Hom}(N, \mathbb{C})$. C'est un G_K -module.

C'est de la poudre aux yeux : peut sauter.

$$\text{Hom}(N, \mathbb{C}) \cong \text{Hom}(N, \mu_n) \otimes \mathbb{C}(-1).$$

Provenant de ce que N^{ab} est isom à un prod
 de gres $\mathbb{Z}_\ell$ (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

$$\begin{aligned} \text{Hom}(N, \mu_n) &= H^1(G_{\bar{k}/K}, \mu_n) \\ &= (\bar{k}K)^* / (\bar{k}K)^{*n} \end{aligned}$$

$$N = G_{\bar{k}/K} \quad \bar{k} \text{ contenant } \mu_n$$

On a une suite exacte :

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

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

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

$$\begin{aligned} \uparrow \\ \text{f} \longmapsto (f) = \sum_{w \in X(\bar{k})} w(f) \cdot w \\ \downarrow \\ (\bar{k}K)^* \end{aligned}$$

montrons surjectivité :

on prend $\Delta \in D/nD$ choisi (q) $\deg \Delta = 0$

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

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

on est ramené au cas $[\Delta] = 0$

d'où $\Delta = (f)$.

(peut aussi se voir avec lemme du serpent :

$$\begin{array}{ccccccc} 0 & \rightarrow & (\bar{k}/k)^* & \xrightarrow{\text{div de degré 0}} & D^0 & \rightarrow & J \rightarrow 0 \\ & & \downarrow n & & \downarrow n & & \downarrow n \end{array}$$

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

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

(s'il y a un pt rat, c'est scindé)

comme G_k -modul : $\bigoplus_w \mathbb{Z}/n\mathbb{Z}$

~~on se pose~~

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

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

On pose $C(-1)$:

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

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

par suite spectrale avec IV,

on avait $n : H^m(K, C) \rightarrow H^{m-1}(G_k, \text{Hom}(W, C))$

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

$$\begin{array}{ccc} & \downarrow & \\ (\pi_v) \nearrow & & \downarrow \\ \text{s'annule} & \rightarrow & \bigoplus_v H^{m-1}(G_{k(v)}, C(-1)) \end{array}$$

lemme : ce triangle est commutatif.

$$H_f: \begin{array}{ccccccc} 1 & \rightarrow & N & \rightarrow & G_K & \rightarrow & G_{\bar{K}} \rightarrow 1 \\ & & \uparrow & & \uparrow & & \uparrow \\ 1 & \rightarrow & I_w & \rightarrow & G_{K_w} & \rightarrow & G_{\bar{K}(v)} \rightarrow 1 \end{array} \quad \begin{array}{l} \text{diag court} \\ \text{par les } v. \end{array}$$

permet de se convaincre (avec pbs d'écriture)
que la composée du triangle est bien
donnée par π_v (c'est triangle court),
 $\square$.

composée avec $\bigoplus_i H^{n-1}(G_{\bar{K}(v)}, \mathbb{C}(-1))$

$$\begin{array}{c} \searrow \text{Cor} \\ H^{n-1}(G_K, \mathbb{C}(-1)) \end{array}$$

composée est 0.

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

Donc Thm 2.

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

Exemple 1

$X = \mathbb{P}_1$

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

- * on a formule des résidus ("comme Girs") : $\sum \text{Cor}(\pi_v(\alpha)) =$
- * Si ts les $\pi_v(\alpha)$ sont 0, alors α est "constant".

i.e. $\alpha \in H^n(k, \mathbb{C})$.

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

(marque des cas local). défini en passant au cas local
appartient à $H^1(k(v), \mathbb{C})$.

(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 $\alpha = 0$).

(Analogie du thm d'Abel sur les diviseurs)

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

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.

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

$\searrow$ $f_* (\alpha) = \text{Cor}(\alpha)$ par l'ext de corps $\begin{matrix} K \\ | \\ k(f) \end{matrix}$

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

les résidus de β sont 0.

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

or ils vont tous à 0. (et $r_{v_0}(f_* \alpha) = \sum_{v/v_0} \text{Cor } r_v(\alpha)$)

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

la somme est 0.

$\Rightarrow \beta$ est cot, et $\beta(0) = \beta(\infty)$

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

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

d'où (?) $\alpha(v) = 0$.

□

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

Soit $\alpha \in H^1(K, \mathbb{C})$, sans pôles, et $\alpha(0) = 0$

(si on avait une courbe de genre 0, α serait cot, i.e. $\alpha=0$).

Alors la fleche $P \in E(k) \mapsto \alpha(P) \in H^1(k, \mathbb{C})$,
est un homomorphisme.

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

pf: Il faut démontrer: $P_1, P_2, Q = P_1 + P_2$
 $\Rightarrow \alpha(Q) = \alpha(P_1) + \alpha(P_2)$

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

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

$$\text{d'où: } \underbrace{\alpha(0)}_0 + \boxed{\alpha(Q) - \alpha(P_1) - \alpha(P_2)} = 0$$

□

ou expérimentalement par Fact (surprise!)

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

4 pts ramifiés.

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

Exemple de détermination de $Br_2 K$.

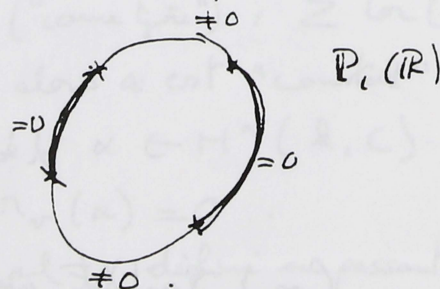
(v. 1^{er} cours:

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

le nbre de pts $\equiv$ 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: $K = \mathbb{C}(\mathbb{P}_2)$.

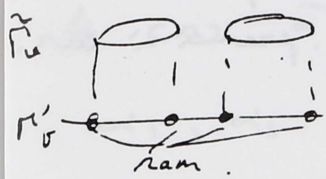
$\alpha \in Br_2 K$

$V =$ ens de val discretes de K associées aux
courbes vraies de $\mathbb{P}_2$.

$v \in V \longleftrightarrow \Gamma_v$: courbe vied, resp fct: $\mathbb{C}(\Gamma_v)$
 $\pi_v(\alpha) \in H^1(\mathbb{C}(\Gamma_v), \mathbb{Z}/2\mathbb{Z})$ } Γ'_v : normalis  e de Γ_v
 donc un el  t $\neq 0$ correspond
    un rev  t quad de Γ'_v
 (el  t de Br_2)
 $0 \rightarrow Br_2 K \longrightarrow \bigoplus_v H^1(\mathbb{C}(\Gamma_v), \mathbb{Z}/2\mathbb{Z})$

on se donne plusieurs courbes.    quelles conditions y a-t-il
 un el  t de $Br_2 K$ qui y correspond ? (c'est d  termin   $In Br_2$)

rev  t quad $\tilde{\Gamma}_v \rightarrow \Gamma'_v$



$ram(\tilde{\Gamma}_v \rightarrow \Gamma'_v)$: la divis  n de ramification
 sur Γ'_v .

Pour tt v t enu fin, soit $\tilde{\Gamma}_v \rightarrow \Gamma'_v$ un rev  t quad
 $\sum_v \text{image des } ram(\tilde{\Gamma}_v \rightarrow \Gamma'_v) = \text{ram totale}$.

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

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

" 2 droites " "

3 droites : sa marche



$x=0$
 $y=0$
 $z=0$

  crire    comme un
 simple $\alpha(\frac{x}{y}, \frac{z}{y})$.

courbe ell : cubique non-sing
 3 rev  t quad

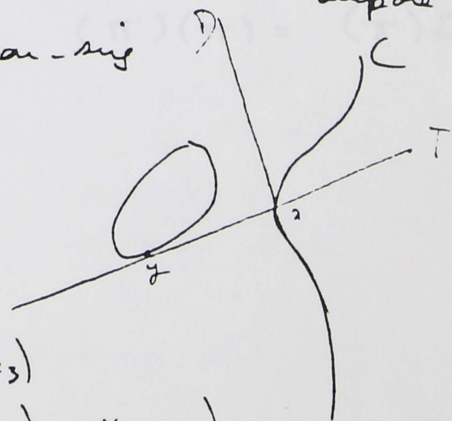
C, T, D

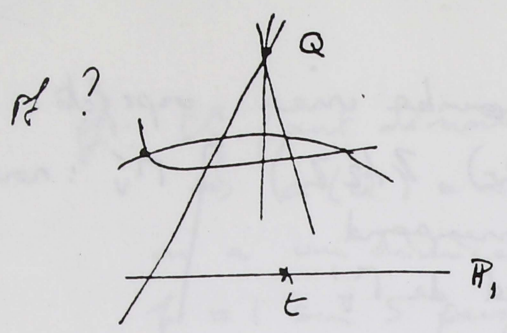
symbole $\alpha = (\frac{C}{T^3}, \frac{D}{T})$

ou, si $y^2 = (x-e_1)(x-e_2)(x-e_3)$

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

Et el  t de Br_2 est un (x, y) pour $x, y \in K^*$: symbole pur.
 ces formes quad    5 vbls repr  sent  es.)





on choisit Q en position gale.
 K : corps de fct d'une droite
proj sur $t = \mathbb{C}(t)$

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

$$\text{Car } \alpha(\alpha) \in H^1(\mathbb{C}(t), \mathbb{Z}/2\mathbb{Z})$$

"et la somme de t ces machines - la est zero" -

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

decrivent $Br K / Br(Surfaces)$ pr surface simplement connexe
partie de Br premier a car.

Réidu d'un produit cas local

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

Def: π un. f. de k

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

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

$$v((\pi) \cdot \gamma) = \gamma$$

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

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

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

$$v(\alpha_1) = \gamma_1, v(\alpha_2) = \gamma_2 \quad \alpha_1 \alpha_2 = (\pi) \gamma_1 (\pi) \gamma_2 =$$

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

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

$$v(\alpha_1 \alpha_2) = \varepsilon \gamma_1 \gamma_2$$

Cas particulier:

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

$$m_1 = m_2 = 1$$

$$\alpha_1 \in H^1(k) = k^*/k'^2$$

$$\alpha_2$$

$$\alpha_1 = (a_1) \quad a_1 \in K^* \quad \alpha_2 = (a_2) \in K^* \quad (71)$$

$$a_2 \in K^*$$

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

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

$$v((a_1)(a_2)) \in H^1(K)$$

$$v((a_1)(a_2)) = (x), \quad \text{où}$$

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

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

Calcul du résidu de H^3

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

$$v((a_1)(a_2)(a_3)) = \sum_{\substack{\text{somme} \\ \text{par perm. circ.}}} v(a_1)(a_2)(a_3) + [Sv(a_1)v(a_2)(a_3)] \varepsilon$$

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

$$(-1)(-1)$$

Fin du supplément !

Correction du dernier cours :

"Thm 2" est faux.

Retour à la situation du thm 2 :

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 ,

(72)

n premier à $p(k) = p(k)$.

$\bar{k}$: clôture algébrique de k .

$$\begin{array}{c} K_s \\ \left(\begin{array}{c} | \\ \bar{k} K \\ | \\ K \end{array} \right) N \\ G_k \end{array} \quad \text{cd } N \leq 1$$

$$1 \rightarrow N \rightarrow G_k \rightarrow G_k \rightarrow 1$$

$$\dots \rightarrow H^n(G_k, C) \rightarrow H^n(G_k, C) \xrightarrow{\sim} H^{n-1}(G_k, \text{Hom}(N, C)) \rightarrow \dots$$

$$\text{Hom}(N, C) = \underbrace{\text{Hom}(N, \mu_n)}_{''} \otimes C(-1)$$

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

$$0 \rightarrow J_n \rightarrow \text{Hom}(N, \mu_n) \rightarrow D/nD \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 0$$

$D = \text{diviseurs de } X/\bar{k}$

$\leftarrow$
du à P (*)

(compatible avec l'action de G_k)

On a trouvé la formule des résidus

(comp. 2 flèches = 0)

(Hyp) X a un point rationnel $/k$, $P^{(*)}$

$$D = D_0 \oplus \mathbb{Z}P.$$

(73)

$$0 \rightarrow J_n \rightarrow \text{Hom}(N, \mu_n) \rightarrow D_0 / \sim D_0 \rightarrow 0$$

$$G_k \begin{matrix} \xrightarrow{\quad} \\ \xleftarrow{\quad} \end{matrix} G_k.$$

On a donc des suites exactes courtes

$$0 \rightarrow H^n(G_k, \mathbb{C}) \rightarrow H^n(G_k, \mathbb{C}) \rightarrow H^{n-1}(G_k, \text{Hom}(N, \mathbb{C}))$$

$$H^n(G_k, \mathbb{C}) / H^n(G_k, \mathbb{C}) \cong H^{n-1}(G_k, \text{Hom}(N, \mathbb{C}))$$

$$H^{n-1}(G_k, \text{Hom}(N, \mu_n) \otimes \mathbb{C}(-1))$$

On tensorise la suite $0 \rightarrow J_n \rightarrow \dots$ par $\mathbb{C}(-1)$

et on trouve:

$$0 \rightarrow J_n \otimes \mathbb{C}(-1) \rightarrow \text{Hom}(N, \mu_n) \otimes \mathbb{C}(-1) \rightarrow D_0 / \sim D_0 \otimes \mathbb{C}(-1)$$

$$\dots \rightarrow H^{n-1}(k, J_n \otimes \mathbb{C}(-1)) \rightarrow H^n(k, \mathbb{C}) / H^n(k, \mathbb{C})$$

$$\rightarrow H^{n-1}(k, D_0 / \sim D_0 \otimes \mathbb{C}(-1)) \rightarrow \dots$$

$$H^{n-1}(k, D_0 / \sim D_0 \otimes \mathbb{C}(-1)) \cong$$

Il manque la page 74 dans le document original.

$$P \in X(k)$$

$$(P) - (O)$$

(75)

$$X(k) \rightarrow D^0(X, k) / \sim D^0(X, k)$$

$$P \mapsto (P) - (O).$$

$$X(k) \xrightarrow{\sigma} H^1(k, X_n)$$

Théorie de la descente fournit :

$$0 \rightarrow X_n \rightarrow X \xrightarrow{\sim} X \rightarrow 0$$

$$0 \rightarrow X(k) / \sim X(k) \xrightarrow{\sigma'} H^1(k, X_n)$$

$$\text{calcul : } \sigma = -\sigma'.$$

Trouver courbe elliptique t.q. $X(k) / \sim X(k) \neq 0$

— très facile.

Donc $\sigma' \neq 0 \Rightarrow \sigma \neq 0$ en général.

k imparfait

(76)

X courbe proj. lisse abs. irréd. sur k

La formule des résidus est vraie pour X

$$K = k(X).$$

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

$$\sum_v \text{Cor}_{k(v)/k} r_v(\alpha) = 0$$

$$\text{dans } H^{n-1}(k, \mathbb{C}(-1))$$

On remplace k par $k^{p^{-\infty}}$. On applique la
formule des résidus à α sur $k^{p^{-\infty}} = k'$

$$k', k'(v).$$

Applicateurs à TP_1, TP_n

$$S: X = TP_1.$$

$$H^n(K, \mathbb{C}) / H^n(k, \mathbb{C})$$

$\parallel_S$

$$\bigoplus_v H^{n-1}(k(v), \mathbb{C}(-1))$$

$\parallel_S$

$$\bigoplus_{v \neq \infty} H^{n-1}(k(v), \mathbb{C}(-1)).$$

$$v \neq \infty$$

Toute classe de cohomologie dont les résidus
sont nuls (∞ excepté) est "constante", i.e.
 $\in H^n(k, \mathbb{C})$.

Corollaire: 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 , $\alpha \in H^n(k/v), \mathbb{C}$

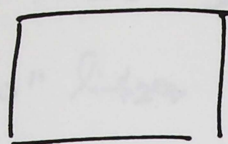
"
 $\alpha(v)$ "valeur de α en v ".

$$Y = \text{Aff}^n / k$$

$$K = k(Y) = k(t_1, \dots, t_n).$$

Th: Toute classe de cohomologie dans $H^n(K, \mathbb{C})$
($\mathbb{C}$ G_K -module annulé par n) dont les
résidus (p.r. aux diviseurs irrédl. de Y)
sont 0, est constante (i.e. $\in H^n(k, \mathbb{C})$)

Démonstration: par récurrence sur n .


 Aff^N

fibre dte affine


 Aff^{N-1}

$$K = K_N$$

|

$$K_{N-1} = k(t_1, \dots, t_{N-1})$$

1^{ère} étape : $\alpha \in H^n(K_{N-1}, \mathbb{C})$

A voir : les résidus de α p.r. aux points
fermés de la droite affine $\text{Spec } K_{N-1}[t_N]$
sont 0.

→ div. irred. de Aff^N non "verticaux"

2^{ème} étape : voir que les résidus de
 $\alpha \in H^n(K_{N-1}, \mathbb{C})$

par rapport aux div. irred. de Aff^{N-1} sont 0.



div. irred. de Aff^N

corps résiduels
pas les rés

div. irr. de A^{N-1}

$$K_N(v) = K_{N-1}(v)(t_N)$$

$$K_{N-1}(v)$$

$$r_v(\alpha) \in H^{n-1}(K_{N-1}(v), (-1)) = 0 ?$$

↓ se tue ds $H^{n-1}(K_N(v), (-1))$

$$\text{injectif} \rightarrow r_\alpha(\alpha) = 0.$$

$$\text{Soit } \alpha \in H^n(k(t_1, \dots, t_N), (-1))$$

on peut regarder sur $\mathbb{P}^{N-1}$

(mais inutile - suffit de regarder l'espace affine).

Applications (à la vérification des formules)

$$\text{Ex: } m=2, C = \mathbb{Z}/2\mathbb{Z}, H^2(K, C) = \mathbb{B}_2(k).$$

Ex 1 (trivial)

$$(x)(y) = (x+y)(-xy) \quad \text{si } x, y, x+y \neq 0.$$

facile à montrer directement.

Ici on fait une démo plus compliquée :

$$\alpha = (x)(y) + (x+y)(-xy)$$

$$\alpha + H^2(h(x,y), ($$

$$h \begin{cases} \text{pas de résidus} \\ \text{valeur 0 en un pt} \end{cases} \quad \begin{matrix} x=y=1 & (1)=0 \\ (2)(-1)=0. \end{matrix}$$

$$\begin{cases} x=0 \\ y=0 \end{cases} \quad \begin{matrix} (x)(y) \rightarrow (y) & \text{vu comme} \\ & \text{fonction sur } x=0. \\ (x)(x+y) \rightarrow (y) \\ (x+y)(-y) \rightarrow 0 \\ \hline 0 \end{matrix}$$

$$x+y=0$$

$$(x)(y) \rightarrow 0$$

$$(x+y)(-xy) \rightarrow -xy \quad \text{sur } xy=0$$

$$x^2$$

$$(x^2)=0 \quad !$$

$$\underline{\text{Ex 2}}: \quad x, y, z \quad \sigma_1 = x+y+z \quad \sigma_2 = xy+yz+zx \\ \sigma_3 = xyz$$

$$(x)(y) + (y)(z) + (z)(x)$$

$$= (-\sigma_2)(\sigma_1\sigma_2 - \sigma_3) + (\sigma_2)(-\sigma_3)$$

$$\underline{\text{Ex 3}}:$$

$$= (\sigma_1)(-\sigma_3) + (\sigma_1\sigma_2 - 3\sigma_3)(-\sigma_1\sigma_3)$$

Ex 2

~~Sonk~~ 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

(81)

$$x = y = z = 1$$

$$\sigma_1 = \sigma_2 = 3$$

$$\sigma_3 = 1$$

$$0 = (-3)(2) + (3)(-1) = (3)(2) + (-1)(2) + \\ + (3)(-1) = (3)(-2) = (3)(1-3) = 0.$$

re'x'idus

$$0 = \sigma_1 \sigma_2 - \sigma_3 = (x+y)(y+z)(z+x).$$

$$x=0$$

$$(y+z) = \sigma_2 \quad \text{par } x=0 \text{ i.e. } (y+z) \neq$$

$$y=0$$

$$z=0$$

$$\sigma_2 = 0$$

$$0 \stackrel{?}{=} (-\sigma_3) + (-\sigma_3) = 0 \quad \checkmark$$

$$x+y=0$$

$$0 = (-\sigma_2) \text{ sur } x+y=0$$

$$x+z=0$$

$$= (-xy) \quad "$$

$$y+z=0$$

$$= (+xz) = 0.$$

Ex 3 : difficile à vérifier par cette méthode

$$\sigma_1 \sigma_2 - 9\sigma_3 \text{ irr'el.}$$

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 à $\hat{a}$?

qui donne la formule cherchée par w_2 .

$$e_1 = (1, 1, 1) \quad q(e_1) = x + y + z = \sigma_1$$

$$e_2 = (y - z, z - x, x - y) \quad q(e_2) = 5x(y - z)^2 = \sigma_1 \sigma_2 - 9\sigma_3$$

$$e_3 \quad q(e_3) = \delta$$

$$x(y - z) + y(z - x) + z(x - y) = 0$$

$$5x(y - z)^2 = 5x(y^2 - 2yz + z^2) = \sum xy^2 - 6xyz = \sigma_1 \sigma_2 - 9\sigma_3$$

$$\langle x, y, z \rangle \cong \langle \sigma_1, \sigma_1 \sigma_2 - 9\sigma_3, \delta \rangle$$

$$xyz = \sigma_3$$

$$\delta = \sigma_1 \sigma_3 (\sigma_1 \sigma_2 - 9\sigma_3)$$

$$w_2 = (\sigma_1)(\sigma_1 \sigma_3) + (\sigma_1 \sigma_2 - 9\sigma_3)(\sigma_1 \sigma_3 (\sigma_1 \sigma_2 - 9\sigma_3))$$

$$(x)(x) = (x)(-1) = (\sigma_1)(-\sigma_3) + (\sigma_1 \sigma_2 - 9\sigma_3)(-\sigma_1 \sigma_3)$$

(83)

X courbe proj. lisse sur k

$\alpha \in H^n(k, \mathbb{C})$ hyp. habituelles

S : ensemble fini de places contenant les pôles
de α

$$D = \sum_{v \notin S} n_v v$$

$$\alpha(D) = \sum_v n_v \text{Cor}_k^{k(v)} \alpha(v)$$

$$\alpha(v) \in H^n(k(v), \mathbb{C})$$

$$\downarrow \text{Cor}$$

$$H^n(k, \mathbb{C})$$

$$D = (f) \quad f \in K^*$$

$$f(v) \neq 0, \infty \quad \text{si } v \in S$$

$$f(v) \in k(v)^*$$

Formule :
$$\alpha(D) = \sum_{v \in S} \text{Cor}_k^{k(v)} ((f(v))_v, \alpha)$$

$$f(v) \in k(v)^*$$

$$(f(v)) \in H^1(k(v), \mu_n)$$

$$r_v(\alpha) \in H^{n-1}(k(v), (-1))$$

(84)

$$\text{cup produit} \in H^n(k(v), \mathbb{C})$$

Corollaire : $S: f(v)=1$ pour tout $v \in S$,
alors $\alpha(D)=0$. (formule de la Abel).

Corollaire $S: S=\emptyset, \alpha(D)=0$ (—)

$P \in X(k), \alpha(P) \neq 0$ alors $\alpha(P)$ ne
depend que de l'image de P dans la
jacobienne généralisée J_S rel. à S .

$$1 \rightarrow L_S \rightarrow J_S \rightarrow J \rightarrow 1$$

||

$$(T R_{k(v)/k} G_m) / G_m$$

Préliminaire: Autre formule

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

$$C_1 \times C_2 \rightarrow C$$

S_1, S_2 ens. fin. de places, $S_1 \cap S_2 = \emptyset$

$$\sum_{v \in S_1} \text{Cor}_k^{h(v)} (v_v(\alpha_1) \cdot \alpha_2(v)) + (-1)^{m_1} \sum_{v \in S_2} \text{Cor}_k^{h(v)} (\alpha_1(v) \cdot v_v(\alpha_2)) = 0$$

dans $H^{m_1+m_2-1}(k, C(-1))$.

Démonstration.

On applique la formule des résidus à α_1, α_2

On applique la formule à $C_1 = \mathbb{A}^1, C_2 = C$

$$\mathbb{A}^1 \times C \rightarrow C(1)$$

$$m_1 = 1, \alpha_1 = (f) \in H^1(K, \mathbb{A}^1)$$

$$m_2 = n, \alpha_2 = \alpha \in H^n(K, C)$$

$$S_1 = \text{zéros et pôles de } f, S_2 = S$$

$$\underbrace{\sum_k \text{Cor}_k^{h(v)} (\alpha_2(v) \cdot \underbrace{v(f)}_{=v})}_{\alpha(\mathbb{D})} + \sum (f(v))$$

donne la formule.

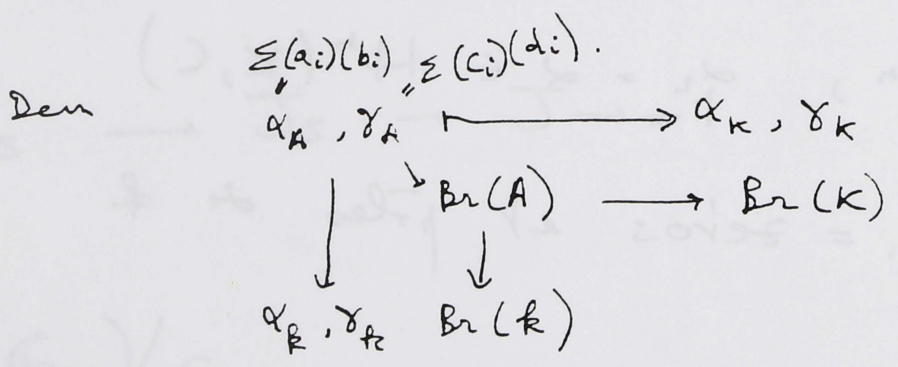
* Remarque sur la dernière fois :
 25 Nov 91 On avait joué "vrai généralement".
 cours 6 $(X+Y, -XY) = (X, Y)$ ds $Br_2 k(X, Y)$

par spécialisation, c'est vrai $\forall x, y \in k$
 $\exists x, y, x+y \neq 0$
 (c'est joué à un sens)

expliquer cette spécialisation :

A local régulier, corps res. k , de car $\neq 2$ (faux pr anneau quelconq)
 $K =$ 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.
 $u = \sum (a_i)(b_i), \sum (c_i)(d_i) \in Br_2(K)$
 $\sum (\tilde{a}_i)(\tilde{b}_i), \sum (\tilde{c}_i)(\tilde{d}_i) \in Br_2(k)$

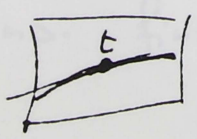
lemme de spécialisation : $\sum (a_i)(b_i) = \sum (c_i)(d_i)$
 $\Rightarrow \sum (\tilde{a}_i)(\tilde{b}_i) = \sum (\tilde{c}_i)(\tilde{d}_i)$



Th (Groth. : "10 exposés s/ la th des schemas")
 $Br(A) \rightarrow Br(K)$ est injectif
 pr A local régulier.

ou : autre méthode : récurrence sur la dim de A
 $\dim A = 1$: ann. de val discrète ($\dots$)
 on a $Br(A) \hookrightarrow Br(K)$

$\dim A + 1$: prend var. une ss-var
 $t \in M - m^2$, passer à $A/tA \dots$
 et on induit situation sur les ss-var.



* retour aux formules

$$K = k(X)$$

$$\alpha(D) = \sum_{v \in S} \text{Cor}_k^{k(v)} \left(\underbrace{(f(v))}_{\in H^1} \cdot \underbrace{r_v(\alpha)}_{\in H^{n-1}} \right) \in H^n$$

$$\text{ou } \alpha \in H^n(K, \mathbb{C})$$

S ens fini de places contenant les pôles de $f \in K^*$, $f(v) \neq 0, \infty$ si $v \in S$

$$D = (f) = \sum v(f) v \quad \text{div. pinc}$$

$$\alpha(D) = \sum_{v(f) \neq 0} v(f) \text{Cor}_k^{k(v)} \alpha(v)$$

$$r_v(\alpha) \in H^{n-1}(k(v), \mathbb{C}(-1))$$

$$f(v) \in k(v)^*$$

$$\text{si } \alpha \in k(v)^* \xrightarrow{\text{soit}} (\alpha) \in H^1(k(v), \mu_n)$$

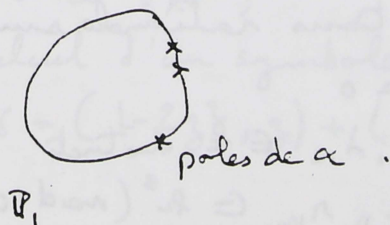
fonct a un sens ds $H^n(k, \mathbb{C})$.

$$\text{on note } \alpha(D) = \text{Cor}_S \left((f(S)) \cdot r_S(\alpha) \right)$$

$$\text{et } k(S) = \prod_{v \in S} k(v)$$

son Spec est produit
de corps

On suppose maintenant que $X = \mathbb{P}_1$
 $K = k(T)$.



S : ens fini contenant
pôles de α , $\infty \notin$

$$x, y \in \mathbb{P}_1(k) - (S \cap \mathbb{P}_1(k))$$

$$\alpha(x) - \alpha(y) = \sum_{v \in S} \text{Cor}_k^{k(v)} \left(\left(\frac{x - t_v}{y - t_v} \right) \cdot r_v(\alpha) \right)$$

(88)

places de $\mathbb{P}_1$:rationnelles : élts de k vrat : pr $T \in k$. $T \mapsto t_r \in k(v)$.diviseur : $D = \{x\} - \{y\}$

$$D = (f) \quad \text{où } f = \frac{T-x}{T-y}$$

 $\hat{m}$ hyp, On suppose $\alpha(\infty) = 0$

$$\alpha(x) = \sum_{v \in S} \text{Cor}_{k(v)}^k \left((x - t_v) \cdot r_v(x) \right)$$

(appliquer la formule $\alpha(D) = \dots$

$$\text{à } f = x - T \quad (\text{où } \alpha \sim \lambda(T-x))$$

Cas particulier $m=2$, $C = \mathbb{Z}/2\mathbb{Z}$.

$$C(-1) = C.$$

$$\text{alors } H^2(k) = Br_2(k)$$

$$H^2(K) = Br_2(K).$$

$$r_v(\alpha) \in H^1(k(v)) = k(v)^* / k(v)^{*2}$$

$\alpha \in Br_2(k)$ est déterminé (à l'addition près d'un élts de $Br_2(k)$) par ses résidus

Détermination explicite de α à partir de ses résidus

e.g. tous les rationnels sur k , $\neq \infty$.

$$\alpha(\infty) = 0$$

$$d_1, \dots, d_n \in k \text{ distincts}$$

$$r_1, \dots, r_n \in k^* \text{ (mod carrés)}.$$

$$\alpha(x) = \sum (x - d_i) \cdot (r_i) \quad x \in k, x \neq \infty, d_1, \dots, d_n$$

$$\alpha = \sum (T - d_i) (r_i) \quad : \text{somme de symboles explicites}$$

pôles pas to rat, e.g : 1 pole quadratique.
 k'/k . $(x)(y) \in Br_2(k')$. $x, y \in k'^*$

Comment écrire $Cor_{k'}^{k'}(x)(y)$ comme comb lin de
 symboles $x_i, y_i \in k'^*$?

ça peut se faire, v. article Rosser-Tate
 K-théorie de Milne

e.g α , pôles $\{ \sqrt{2}, -\sqrt{2} \}$ au 3, résidu = -1
 $k = \mathbb{Q}$, $\alpha(\infty) = 0$ (pr faire marcher
 formule des résidus).
 résidus de $\mathbb{Q}(\sqrt{2})$

e.g ("au hasard") $r = 1 + \sqrt{2} = "1 + t"$

conjugue $r' = 1 - \sqrt{2}$

norme $rr' = -1$

$1 + \sqrt{2}$: eqn

on écrit $(t^2 - 2, 1 + t) = \gamma \frac{x}{y}$

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
 $\begin{cases} -1 : \text{res.} -1 \end{cases}$

$\alpha + \gamma = \gamma(\infty) + (-1, t-3) + (-1, t+1)$

$\Rightarrow \alpha = (t^2 - 2, 1 + t) + (-1, (t-3)(t+1)) + \text{cste}$

pr déterminer la cste : calculer en 1 pt connu : α

calcul de $\gamma(\infty)$:

calcul d'un symbole en un pole apparent, $z=0$

$\gamma = (1 - 2z^2, z) + (1 - 2z^2, 1+z)$

$\hookrightarrow 0$

comment calculer $(z, 1 + \mathcal{L}(z))$

au termes de $\mathcal{L}$
 ordre $d \geq 1$

$1 - 2z^2 \sim (1 - 2z^2)(1 + 2z + z^2)$ mod cané,
 i.e divisible par z .

$= 1 + 2z - z^2 - 4z^3 - 2z^4$

$$(a, b) + (c, T) = (axb) + (cxT)$$

(90)

$$\text{or } (x, 1-x) = 0 \quad (\text{c'est une forme!})$$

$$\text{d'où } (1+2z - z^2 \dots, -2z + z^2 + 4z^3 + 2z^4) = 0$$

$$z(-2 + z + 4z^2 + 2z^3)$$

$$\text{d'où, exp chercher } = (1+2z - z^2 \dots, -2 + z + \dots)$$

$$= 1 \quad \text{pr } z=0.$$

!
ça donne coté = 0.

Questions

pr $\mathbb{Q}(T)$: Y a-t-il un entier N t.q tt elmt de $Bz_2(\mathbb{Q}(T))$ soit somme de N symboles si oui, quel est le meilleur? $(x, y;)$

$N=1$: 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 (plus $\exists d \in k^* \text{ t.q. } (a, b) = (c, d)$)
et donc $\alpha = (c, dT)$.

Thm : Si $k(\sqrt{c})$ ne se décompose pas (a, b) , alors α n'est pas un symbole (est la somme de 2 symboles)

forme normale
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).

(91)

appliquons le critère d'Albert :

$$\langle -a, -b, ab, c, T, -T \rangle \\ = \langle -a, -b, ab, c \rangle \oplus T \langle 1, -c \rangle.$$

or : leme : g_1, g_2 anisotrope $\Rightarrow g_1 + Tg_2$ est anisotrope
sur k 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 $\stackrel{?}{\Rightarrow} (a, b) + (c, d)$ est un symbole

$\Downarrow$

$$H_{a,b} \otimes H_{c,d} \cong H \otimes H_2$$

alg centrales simpl.

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 gél : $g_1 \oplus g_2$ 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. 0.
 $\Rightarrow$ on prend un elmt
t.q $g_2(x_2) \neq 0$, et x_1
t.q $g_1(x_1) = \dots$

$\Rightarrow f(\sqrt{e})$ décompose (a, b)

$$\Leftrightarrow (a, b) = (e, f)$$

et $k(\sqrt{e})$ déc $(c, d) \Leftrightarrow (c, d) = (e, g)$.

$$\Rightarrow (a, b) + (c, d) = (e, f+g).$$

$$(\Leftarrow) (a, b) + (c, d) = (e, f)$$

$$\text{soit } k' = k\sqrt{e}$$

$$(a, b) = (c, d) \text{ sur } k'$$

$$\Rightarrow (-a, -b, ab) = (-c, -d, cd) \text{ sur } k$$

$$\text{sur } k', f_6 = \mathcal{U}_3 \oplus -\mathcal{U}_3 \text{ où } \mathcal{U}_3 \text{ forme de rang 3}$$

et on a supposé f_6 forme hyperbolique de rang 6.

$$\Rightarrow f_6 \simeq_k \psi_3 \otimes \langle 1, -e \rangle \simeq \langle d_1, -ed_1, d_2, -ed_2, d_3, -ed_3 \rangle$$

$$\text{discr}(f_6) = -e \in k^*/k^{*2}$$

$$\text{or discr } f_6 = -1 \text{ mod carrés (par } f_6 = \langle -a, -b, ab, c, d, -cd \rangle)$$

$$\Rightarrow e = 1 \quad \because e \text{ est un carré.} \Rightarrow k' = k$$

$$\Rightarrow ab = cd$$

$$\Rightarrow f_6 \text{ repr } 0.$$

□.

autre explication du critère d'Albert "à la Tits"

$$\alpha = (a, b) + (c, d) \quad \alpha \in \text{Br}_2(k)$$



f_6 : forme à 6 vbls

(f_6 est déterminée par α au prod près par un élt de k)

$$\begin{matrix} A_3 : & \bullet \text{---} \bullet & \leftrightarrow & SL_4 \\ D_3 : & \bullet & \hookrightarrow & SO_6 \end{matrix}$$

$$M_2 \quad (H^1(M_2) = k^*/k^{*2})$$

$$PGL_2 = SL_2/(\pm 1)$$

$$SL_2/(\pm 1) \times SL_2/(\pm 1) \rightarrow SL_4/(\pm 1)$$

$$\begin{matrix} (a, b) \\ \in H^1(k, SL_2/(\pm 1)) \end{matrix} \Rightarrow \begin{matrix} (c, d) \\ \in H^1(k, SL_2/(\pm 1)) \end{matrix}$$

$$SL_4/(\pm 1) \xrightarrow{\sim} SO_6 \quad (\text{de la forme quad de dim } 6)$$

par comparaison des dim.

$$\alpha \in PSL_4 = SL_4/\mu_4 \hookrightarrow \in H^1(\cdot) \subset \text{Br}_4 \hookrightarrow \in H^1(SO_6) \simeq \text{quad à 6 de dim } -1$$

appl $SL_4 \rightarrow SO_6$:

V de dim 4, $e \in \wedge^4 V$ fixe, $\neq 0$.

$$\wedge^2 V \times \wedge^2 V \rightarrow \wedge^4 V \simeq k$$

dim 6

* Propriété d'un corps k ("hamiltonien" ?)

si $a, b, c, d \in k^*$

(H) alors $(a, b) + (c, d)$ est un symbole

i.e : la forme $\langle a, -b, ab, c, d, -cd \rangle$ est isotrope..

$\Leftrightarrow$ (Herkunjer) 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-dégén de rang 5 est de discr. 1, représentée.

At $(\Rightarrow)$: 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 $x_1, x_2, \dots, x_5$ carré).

montrons $\exists \lambda, a, b, c, d$

$$t.q. q_6 \simeq \lambda \langle -a, -b, \dots \rangle$$

$$\text{on eq. } \langle \lambda x_1, \lambda x_2, \lambda x_3, \lambda x_4, \lambda x_5, -\lambda \rangle$$

$$\begin{matrix} -a & -b & ab \end{matrix} \text{ en posant } \lambda = x_1 x_2 x_3$$

$$-a = x_2 x_3$$

$$-b = x_1 x_3$$

on pose $d x_4 = c$, $d x_5 = d$

est-ce que $-d = -cd$?

par calcul des différentielles :

$$x_1 x_2 x_3 = d^2 x_4 x_5 \mod \text{caract.}$$

OK.

$$(\Leftarrow) \quad \langle c, d \rangle \otimes \langle -a, \dots, -cd \rangle, \text{ OK.}$$

Calcul et assassinat des symboles
on veut "tuer" les elmts de $Br_2 K$ (obstruction)
où k infini $\Rightarrow K = k(T)$.
situation : $\alpha \in Br_2(K)$ (symbole ou somme de symboles)
e.g. cherches des pts $x \in \mathbb{P}_1(k)$, x non-pôle,
où $\alpha(x) = 0$ de $Br_2(k)$.

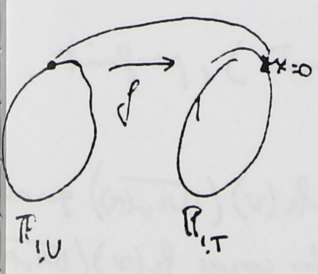
Question S'il existe un $x \in \mathbb{P}_1(k)$ où α s'annule,
en existe-t-il d'autre? none infinie? Card k ?
pas comme $\tilde{m}$ sur $\mathbb{Q}$.
on va parler des conjectures associées à cette question.

Changement de base

e.g. : α ayant 2 pôles rat/ k
supposons ces poles sont $0, \infty$,
le résidu $r \in k^*/k^{*2}$ (le $\tilde{m}$ par finale résidu)
et que $\alpha(1) = 0$.
alors $\alpha = (r, T)$. (a les deux poles et 0),
Si on force T à être un carré, α devient 0.

$$\begin{array}{ccc} f: \mathbb{P}_1 & \longrightarrow & \mathbb{P}_1 \\ U & \longmapsto & T = U^2 \end{array} \quad k(T) \hookrightarrow k(U)$$

$f^*(\alpha) = 0$ de $Br_2(k(U))$.
et $Im f$ est un ensemble de pts rat s/lequel α est 0.



Question: soit $\alpha \in Br_2(k(T))$,
soit $x \in \mathbb{P}_1(k)$ avec $\alpha(x) = 0$,
Existe-t-il $f: \mathbb{P}_{1,U} \rightarrow \mathbb{P}_{1,T}$ non-const
t.q. (1) $f^*(\alpha) = 0$: α est tué de $Br_2(k(U))$
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.

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.

$$r_w(f^*\alpha) = e_{w/v} \cdot (r_v(\alpha))$$

$$r_v(\alpha) \in k(v)^* / k(v)^{*2}$$

la condition $r_w(f^*\alpha) = 0$

équivaut à : au tri $e_{w/v}$ est pair.

ou bien $r_v(\alpha)$ devient un carré
 de $k(v)$

$$\text{i.e. } k(w) \ni \sqrt{r_v(\alpha)}$$

$$\begin{array}{c} k(v) (\sqrt{r_v(\alpha)}) \\ | \\ k(v) \end{array}$$

Résultats

(1) Tanchevski : la question ci-dessus a une
 réponse positive si $k = \mathbb{R}$ ou si k est hensel
 (e.g. corps local)

(2) Mestre : réponse positive si $\sum_{v \text{ pôle de } \alpha} \deg(v) \leq 4$

(3) Mestre : ~~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 henselien (e.g. complet pr une val discrète), parfait.

α symbolique, S pôles, $\alpha(\infty) = 0$.

pr $v \in S$ on a $k(v)$ est finie de k , et $k(v) (\sqrt{r_v(\alpha)})$ quel
 soit k' ext gal finie de k contenant to 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 $f_N = P(U) / \pi^N$ où π unif, N assez grand.

lemme : f_N a les propriétés (1) et (2) pour N assez grand

$$\begin{array}{c} \text{4} \quad \begin{array}{c} \overset{w}{\downarrow} ? \\ v \in S \\ \uparrow \\ t_v \in k(v) \end{array} \end{array}$$

$$P(U) = \pi^N t_v \xrightarrow{N \rightarrow \infty} 0$$

lemme de Krasner : corps hensélien :

les eqns voisines d'une ext sep définissent le m corps.

on aura $k(w) = k'$, sur lequel le résidu est trivial : $\pi_v(a)$ est un carré.

□.

2 décembre 91 1^{ère} heure : thms de Mestre pr tuer des elts de Br_2
cours 7

k corps, $\text{car} \neq 2$, infini (essaie de généraliser à k fini)

$$\alpha \in Br_2 K(T)$$

$$S = \text{ens des pôles de } \alpha \subset \mathbb{P}_{1/k}$$

hypothèses :

- ① $\deg S \leq 4$ ($\deg S = \sum_{\sigma \in S} \deg(\sigma)$)
- ② $\infty \notin S$ et $\alpha(\infty) = 0$

Théorème (Mestre₄)

Il existe un morphisme $f: X \rightarrow \mathbb{P}_1$, ^{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, lap de choix.)

Mestre₅ : pr $\deg S \leq 5$, on peut obtenir 1: $f^*(\alpha) = 0$.

2 méthodes : 1 explicite, 2 courbes elliptiques.

Méthode explicite

on a fixé pt base : ∞ .

agrandi $S := \text{pôles} \cup \{Q_1, \dots, Q_h\}$, $Q_i \in \mathbb{P}_1(k) - \infty - S$
i.e. $\deg S = 4$ (on aura $\text{Res } Q_i = 0$ en not multi)

$$S \iff P = T^4 + a_1 T^3 + a_2 T^2 + a_3 T + a_4$$

$S = \text{ens des zéros de } P$

résidus : pr chaque pt de S , un elt du corps résiduel mod can

ou: on prend $k(S) := k[T]/(P)$ base: $1, T, T^2, T^3$

$$\text{Res}_S(\alpha) = r \in k(S)^* / k(S)^{*2}$$

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 denses pr la top de Zariski ds l'esp. des polys de $\deg \leq 3$ (vue comme esp. affine de dim 4 sur k).

Dem $G := \prod_{S/k} G_m$ or $X \mapsto x^2$ surjectif.
 (gpe mult de l'esp affine) $\Rightarrow$ dense.

on peut donc éviter les relations générées en remplaçant $\square$

Choisissons R .

$$\begin{aligned} P(T) &= T^4 + a_1 T^3 + \dots \\ R &= r_0 T^3 + \dots \end{aligned}$$

$$P(T) + X^2 R(T) = T^4 + (a_1 + r_0 X^2) T^3 + \dots$$

$$= \underbrace{(T^2 + b_1(X^2) T + b_2(X^2))^2}_{\text{"hamécanie formelle"}} + \underbrace{b_3(X^2) T + b_4(X^2)}_{\text{"reste"}}$$

si $b_3(X^2) \neq 0$, on pose $f(X) = -\frac{b_4(X^2)}{b_3(X^2)}$.

pr corps finis

A démontrer : si R est assez général (i.e on évite certains cas)

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 $\deg 8$, $\infty \mapsto \infty$: pt rationnel.

pourquoi $f^*(\alpha) = 0$?

on a changé vbls : $T = -\frac{b_4(X^2)}{b_3(X^2)}$

$X \xrightarrow{f} \mathbb{P}_1$

donc : res $f^*(\alpha) = 0$

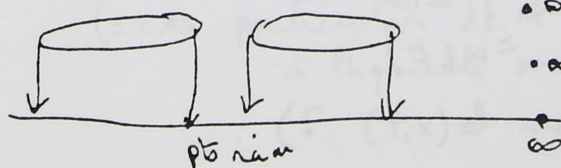
regarder pts au-dessus des zéros de P , $R(T)$.

on a écrit : $\square \times R = \square \Rightarrow R$ est un carré.

Méthode à courbes elliptiques.

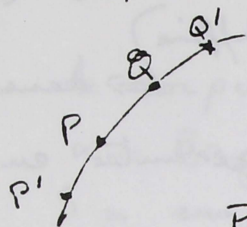
Points sur les C.E. (v. Euler)

méthode classique $Y^2 = P(T)$ Pde deg 4, unitaire



∞_1 éclate à l' ∞ en 2 branches
 $Y = T^2 + \dots$ 2 pts rationnels
 $Y = -T^2 + \dots$

pr trouver d'autres pts rats : symétriques.

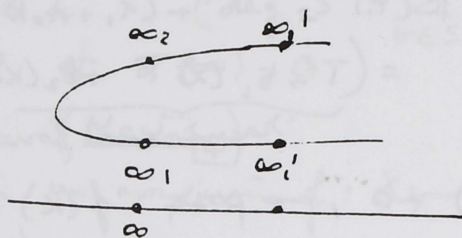


symétriques des pts α_i , on trouve 2 autres pts rats (au-dessus de α_i pt).

$$P(T) = T^4 + \dots = (T^2 + \dots)^2 + cT + d$$

$$T = -\frac{d}{c} : \text{pt rat}$$

(on continue, si ce n'est pas un pt d'ordre fini on obtient ∞ de pts rats)



Énoncé + général :

courbe E
 $f \mid \deg 2$.



, tq. $\infty \in P_1(k)$ est image de 2 pts rationnels $\alpha_1, \alpha_2 \in E(k)$.

soit $t = -\frac{d}{c}$ (au-dessus duquel on a aussi des pts rats.).

Thm Soit $\alpha \in Br_2(k(T))$, Supposons $\alpha(\infty) = 0$ et que les résidus de $f^*(\alpha)$ soient 0. Alors $\alpha(t) = 0$

Dém Utiliser props de corps de fcts.

$$\alpha_E = f^* \alpha$$

par hyp : les résidus de α_E sont 0, et $\alpha_E(\alpha_i) = 0$

Choisissons α_1 comme origine de E .

on avait démontré : si $e \in E(k)$, $e \mapsto \alpha_E(e)$

est un homom de $E(k)$ ds $Br_2(k)$.

de plus α_2 est aussi au-dessus de 0. $\alpha_E(\alpha_2) = 0$

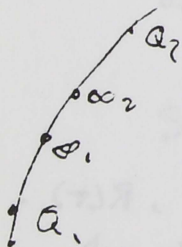
donc $\alpha_E(-\alpha_2) = 0$ mais, si α_1 est l'origine

$-\alpha_2 = Q_1$ (symétrique de α_2 & α_1)

$$\text{d'où } \alpha_E(Q_1) = 0 \\ = \alpha(t).$$

(en fait : C.E. sur $k(x, T)$?).

□.



Pour $\deg S = 5$

hypothèse sur k : (H1) : formes quad de rang 6, $\det = -1$ représentent 0

($\Leftrightarrow$ si $a, b, c, d \in k^*$, alors $(a, b) + (c, d)$ est égal à (e, f) , avec $e, f \in k^*$
(i.e. $\sum$ symboles est 1 symbole)

Thm (Mestre₅) On suppose que k satisfait à (H1)
soit $\alpha \in B_{12} k(T)$ t.q. $\deg S = 5$ et $\alpha(\infty) = 0$.
Il existe alors $f: \mathbb{P}_1 \rightarrow \mathbb{P}_1$, 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 $d \leq 4$ (ou ≤ 4 , mais mod $\square$,
il faut utiliser fonct des résidus. $\Rightarrow$ on peut prendre deg 4).

Si $S = \{P_1, \dots, P_5\}$: 5 pts rest.

$\prod_{i=1}^5 R(P_i)$ est un carré : fonct des résidus.

en gén: $k(S) := k[T]/(P)$.

fonct des résidus: $N_{k(S)/k} R \in k^{*2}$.

Cas particuliers:

R unitaire de $d \leq 4$: $R = T^4 + a_1 T^3 + \dots$

$$R = \left(T^2 + \sum_{i=1}^2 b_i T + b_2\right)^2 + b_3 T + b_4$$

Lemme: Si $t \in k$ est t.q. $b_3 t + b_4 = 0$,
alors $\alpha(t) = 0$.

(= cas particulier de l'argument d/ courbes ell, $Y^2 = R(T)$
à laquelle on applique lemme gén.)

On regarde $V =$ variété dans Aff^5 (le poly de $d^\circ \leq 4$ en T).

Choisissons R_0 un poly représentant le résidu de α
(pas forcément unitaire).

$$R_w = R_0 w^2 \pmod{P} \quad \text{où } w: \text{poly de } d^\circ \leq 4$$

soit $\mathcal{W}$: la var. des w t.q. R_w soit unitaire de $d^\circ \leq 4$.

$$w \in \mathcal{W}^{\text{ét}}(k') \mapsto t(w) \in k' \quad \text{appl. rationnelle}$$

$$k': \text{ext de } k \quad \text{où } t(w) = -\frac{b_4(w)}{b_3(w)}$$

$$\text{On a } \alpha(t(w)) = 0.$$

$\mathcal{W}$ est une quadrique affine dans Aff^5
(défini par forme quad = 1)

on a donc défini $\mathcal{W} \xrightarrow{F} \mathbb{A}^1$ appl. rat
 $w \mapsto t(w)$

$$\text{avec } F^*(\alpha) = 0$$

on applique ça au pt gen (d'où le k°)

Lemme: (H) $\Rightarrow$: la quadrique $\mathcal{W}$ a un pt rat.

(d'où : $\mathcal{W}^{\text{ét}}$ est $\propto$ variété k -rat.

ça termine le thm (mais $\Leftarrow$: on ne voit pas si $\exists$ pt d'img ∞)

Dém. du lem. : $\mathcal{W}$, w un poly de $d^\circ \leq 4$, $R_0 w^2$.

$$\lambda : k(S) \rightarrow k \quad k(S) : \text{base } 1, T, T^2, T^3, T^4$$

$$G \mapsto \text{coeff de } T^4 \text{ ds } G.$$

$$\mathcal{W} = \{ w \mid \lambda(R_0 w^2) = 1 \}$$

$\lambda(R_0 w^2)$ est une forme quad non-dég en 5 vbles.

Lemme : son discriminant est 1 (mod carrés)

alors : $q \oplus \langle -1 \rangle$ représente 0, forme à 6 vbles de discr. -1.

Dém. du lem. $A := k(S)$, de rang 5 sur k .
 $= k[T]/(P(T))$ algèbre étale.

calcul du discriminant. (Euler ? corps locaux)

$$\lambda(G) = \text{Tr} \left(\frac{G}{P'(T)} \right) \quad (\text{par calcul})$$

$$\text{et } q(w) = \text{Tr} \left(\frac{R_0}{P'(T)} w^2 \right)$$

en g^{al}, A algèbre étal, a ∈ A*, w ↦ Tr(aw²)

a pour disc = (N_{A/k} a) · disc(A).

calcul... disc q = disc(P) = 1/NP'(t) = 1 mod car,
pas finale des résidus : NR₀ = 1

NP'(t) = (-1)^{n(n-1)/2} disc P
= disc P. (n=5).

□

N.B: si α = (x)(y) = (x, y) est un seul symbole x, y ∈ k(t)*.

interprétation par fibre en coniques Y

z² - x x² - y y² = 0



trouver P₁ → IP₁ surj qui tire α



Y est k-unirational.

Y₁ → Y

Y₁ → IP₁

Application à la construction d'extensions
galoisiennes de Q(t).

1^{er} cas (thm hypothétique: hypothèses rarement satisfaites)

Thm k de car 0, t.q le pb (*) : ∀ α ∈ B_h k(t)

(*) { et ∀ t pt rat ∈ P₁(k) avec α(t) = 0,
∃ f: IP₁ → P₁ non-const, qd f*(α) = 0
et t₀ ∈ f(P₁(k)) -

ait t₀ une solution, alors:

si G est un 2-groupe, il existe une ext
gal-régulière L/k(t), de gpe de Galois G,
avec un "pt-base" (i.e un pt rat de P₁, 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 qd pt-base pr G sporadique.
 (m pas Cq pts au-dessus soient reals : toutes ext
 comes ont pts complexes).

N.B : Si $L/k(T)$ vérifie ces cond, $\exists L'/k(T)$
 vérifiant les m cond (pr le m gpe G) et C.q.
 le genre de ce corps K , $L' \supset K \supset k(T)$, $K \neq k(T)$
 soit ≥ 1 (ou $\geq n$ dans) } i.e genre de courbe
 correspondant.

pour ce : $Y_F \rightarrow Y$
 $\downarrow G \quad \downarrow G$
 $P_1 \xrightarrow{f} P_1$
 $\downarrow \psi \quad \downarrow \psi$
 $\infty \rightarrow \infty$
 certains courbes ont $g=0$,
 on les évite en changeant
 de vble pr augmenter le
 ramification pr les corps
 intermédiaires.
 O non-ram de Y
 prendre $f(x) = x^N$

Deux cas :

① : G élémentaire de type $(2, 2, \dots, 2)$

Soient $P_1, \dots, P_n$ des polys unitaires de degré pair ≥ 4 ,
 premiers entre eux.

$$K = k(T) (\sqrt{P_1}, \dots, \sqrt{P_n})$$

② G non élémentaire Récurrence sur $|G|$

$$G^* := \text{Fratt}(G) = \bigcap (\ker(G \rightarrow \{\pm 1\})) \quad G^* \neq 1.$$

alors G/G^* est élémentaire de type $(2, \dots, 2)$.

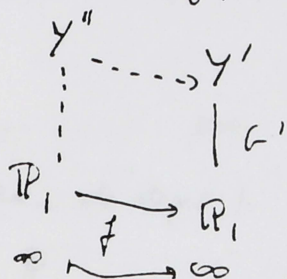
$\exists x \in G^*, x^2 = 1, x \neq 1, x \in Z(G)$: centre.

$$1 \rightarrow \underbrace{\mathbb{C}_2}_{\langle 1, x \rangle} \rightarrow G \rightarrow G' \rightarrow 1$$

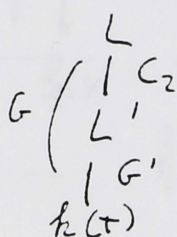
$$G' = G/\mathbb{C}_2$$

par hyp. de recense, on sait construire $L' \text{ sur } G'$ $y' \xrightarrow{\text{décomp}} \infty$
 on veut étendre à L $G' \downarrow$
 on se hante à $\alpha \in H^2(k(T))$.
 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 , $f^*(\alpha) = 0$



et les corps intermédiaires son de
 genre ≥ 1 . évite décomposition
 donc ext lin disjointe



On peut supposer $\alpha = 0$: obstruction
 liquidée.

donc $Gal(K_s/k) \xrightarrow{\text{surjet}} G'$ se relève
 $\nearrow G$
 $\downarrow$

$G_1 \subset G$, image de $Gal(K_s/k)$.
 Par les propriétés du Frobenius, $G_1 = G$
 c'est surjet.

il faut encore arranger ∞ pr qu'il soit
 complètement décomp de L (pas de ram ni d'inv de L' à L).

on relève de $Gal(K_s/k) \xrightarrow{\text{surjet}} G'$ est défini
 à mult. près par $Gal(K_s/k) \rightarrow C_2$,

i.e. c un caractère quadratique ε de $K = k(T)$
 $\varepsilon \leftrightarrow k(\sqrt{\varepsilon}) / k(T)$

si ramifié : $L \text{ sur } k(\sqrt{\varepsilon})$; on prend $\varepsilon \leftrightarrow k(\sqrt{\varepsilon})$.

□.

a marche bien
 en corps de nrbres:
 a d'autre places
 sur corps locaux.

Le thm n'a pas d'applications:
 en les cas $k = \mathbb{R}, \mathbb{Q}$, on avait eu.

Prochaine fois: $SL_2(\mathbb{F}_7)$, GA_6 , GA_7

9-12-91 - Construction par Mestrie d'extensions régulières de $\mathbb{Q}(t)$ de groupes de Galois G avec

(109)

$$G = \begin{cases} SL_2(\mathbb{F}_7) \\ G.A_7 \\ G.A_7 \end{cases} \quad (\text{Mestrie, non publié})$$

Cas $SL_2(\mathbb{F}_7)$

$$SL_2(\mathbb{F}_7)/\pm 1 \simeq PSL_2(\mathbb{F}_7) \simeq SL_3(\mathbb{F}_2)$$

groupe simple d'ordre 168,

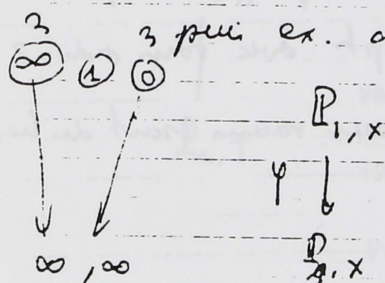
On construit des extensions à groupe $PSL_2(\mathbb{F}_7)$, pb. de plongement quadratique.

Construction de La Macchia : $P_0(x) = x^7 + \dots$

$$Q_0(x) = x^3(-1)$$

$$\text{pour } P_0 - T Q_0 \quad T \text{ indet.}$$

3 puis ex. de degré 7 de $\mathbb{Q}(a, T)$ par $P_0 - T Q_0 = 0$ est $PSL_2(\mathbb{F}_7)$



$T = P_0(x)/Q_0(x)$ revêt de degré 7, à glorie galoisienne

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 dépen. $k = \mathbb{Q}(T)$ $Gal(\bar{k}/k) \rightarrow PSL_2(\mathbb{F}_7)$
peut-on relever?

$$\begin{array}{ccc} ? & \rightarrow & SL_2(\mathbb{F}_7) \\ & \searrow & \downarrow \\ Gal(\bar{k}/k) & \rightarrow & PSL_2(\mathbb{F}_7) \end{array}$$

$\Delta \in H^1(k, C_2)$ obstruction au relèvement invariant de Hasse-Witt de la forme $Tu(x^2)$, mais pas besoin de calculer :

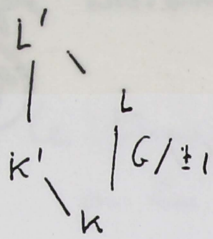
Δ a au plus 4 pôles (+ exact. degré (4 pôles) ≤ 4)

On utilise le Th. de Mestrie pour trouver Δ . On doit chercher un valeur $a \in \mathbb{Q}$, $t \in \mathbb{Q}$ telles que Δ_a s'annule au point t . On en connaissant (Tests sur machine : Mestrie, Muller $a=49, t=0$?)

il semble difficile de faire autrement qu'utiliser la machine.

Mais alors, on peut trouver, on copie $P_{1,T} \xrightarrow{f} P_{1,T}$
avec $\deg(f) = 8$, $f^*(x) = 0$, couvrant le point base. $t = f(t')$

vérifier que les extensions sont disjointes
il n'y a plus d'obstruction de l'/k' (108)



C. peut donner les équations.

Second Cas. extension centrale de A_6 par C_6 .

Dh. d'ext. est $d_2 \in H^2(K, C_2)$ $d_3 \in H^2(K, C_3)$

II. Construit un ext. de $K = \mathbb{Q}(T)$ à ram d'ordre 2 et 5.
à groupe A_6 .

$$\begin{array}{c} P_{1,X} \\ \downarrow \\ P_{1,T} \end{array} \quad T = P(X)/Q(X) \quad \begin{array}{c} P \text{ polynôme de } d^5 6 \\ Q \text{ } d^5 5 \end{array}$$

tel que $P'(2 - PQ') = R^4 S$ où R et S polynômes quadratiques
donnera 2 pt avec Ram. ord 5 et 2 pt avec ram ord 2.

cf. détermination. $[R, S] = 1$, & T corresp aux racines sont des racines

$$P(X) = X^6 + a_1 X^4 + a_2 X^2 + a_3$$

$$Q(X) = X(X^4 + b_1 X^2 + b_2)$$

$$R(X) = X^2 + c, \quad S(X) = X^2 + d$$

On se donne Q, R , et on essaie de déterminer les coef de P et de S .

(On peut le prendre arbitraires car $6-5=1$!!)

$$\text{Condition } 9b_1^2 + 100b_2 = \square.$$

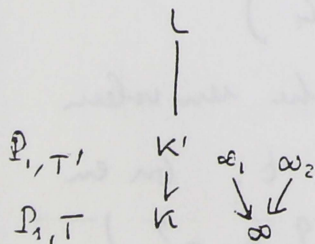
On obtient un revêtement avec groupe galatéenne S_6 .

ramifié (1,2) 2 fois
(1, - 5) 2 fois

1^{er} chang^t de base pour tomber sur A_6

K' a encore genre 0, on cherche $\text{dis}(Q) = \square \Leftrightarrow b_2 = \square$.

la fibre de $T = \infty$ formée de $\infty, 0$ et racines de $X^4 + b_1 X^2 + b_2$.



sur K' , la ramification de L est d'ordre 5 en 4 pts
(doublet).

On regarde $d_2 \in H^2(K', C_2)$ et d_3 . Comme $(5,2)$ et $(5,5) = 1$

un élément est soit de pôle $\Rightarrow$ constants.

pour un annuleur non nul en pt où il s'annulent

$$\text{Calcul de } W_2 \text{ associé} = Q \times Q \times Q[1 \times 1] / (x^4 + b_1 x^2 + b_2)$$

(109)

on s'arrange pour avoir $d_2 = 0$

Pour d_3 , en un pt $= 0$ (Groupe de Galois $\subset D_4$)

général Cas $G = G A_2$.

$$\text{On part de } P(x) = x^7 + a_1 x^5 + \dots$$

$$Q(x) = x^4 + b_1 x^2 + b_2$$

$$T = \frac{P(x)}{Q(x)}, \quad P'(2 - Q)P = 3 R^4 S(x)$$

On revient comme précédemment - bien prendre le calcul, et faire
un test en la matière!

$P_{1,x}$

$P_{2,T}$

ram. ordre 5 2 fois (1,2...5)

ram. ordre 2 2 fois (1,2)

ram. $2 \infty 3$ 1 fois (1,2,3)

faire le calcul du genre.

$$-2 = 7 \times (-2) + 2 \times 4 + 2 \times 1 + 1 \times 2$$

Groupe de Galois S_7 . (regarder les cycles)

L

A_2

K'

$1, 2$

K

$K' \approx Q(T')$ avec un pt fixe.

Calcul par d_1, d_3

K_2 est C^k (ramifié d'ordre impair), suffit de l'annuler

si invariant de Wilt de P est 0. (calcul par Recherche de

$$\text{testé : } P = x^7 + a_1 x^5 + a_2 x^3 + a_3 x \quad a_1 = 1/100, \quad a_2 = \frac{24499}{3500}, \quad a_3 = -\frac{6125}{25}$$

Lemme : $d_3 = 0$

On demande que en 1 pt. de ramification d'ordre 3, le groupe de
décomposition n'est pas divisible par 3 (en fait D/C_3 2-groupe)

et donc $u \in H^2(A_2, C_3)$ alors $u/H = 0$ ou $9 \nmid |H|$

car cycle (A_2) 3×3 élément $\Lambda^2()$ sur champ de 10 groupes ord 3

la propriété du groupe de décomposition provient des polynômes unitaires

$\in X \mapsto -X$: 1 élément d'ordre 2 de S_7 qui centralise D .

rationnel - (et aurait fallu $\mathbb{P} \in \text{rauc de } \mathbb{Q}$)

(110)

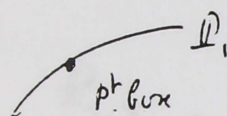
$\underline{S} \quad \begin{matrix} L \\ | \\ G \end{matrix} \quad \text{regulier avec } \mathbb{P}' \text{ box}$

$\mathbb{Q}(T)$

Th. correct. de Hilbert: $\forall S$ fin de place de $\mathbb{Q}$

$\exists L_S/\mathbb{Q}$ de groupe de Galois tel que places de S sont tot. decomposees (place ∞ tot. inerte).

algebre $(\mathbb{Q}_p \rightarrow \mathbb{Q})$.



t S -voisin lemme de Kronecker algebre attachee a t

est decomposee en la place de S on peut ajouter dans correct. de Hilbert

que L_t est un corps

Sch400

Annulation de d sur $\mathbb{Q}$

$\alpha \in Br_2(\mathbb{Q})$, ensemble des $t \in \mathbb{P}_1(\mathbb{Q})$, non poles de d pour lesquels $d(t) = 0$.

exemple $\alpha = (f)/(g) \quad f, g \in \mathbb{Q}(T)^+$

t : conique $X^2 - f(t)Y^2 - g(t)Z^2 = 0$ a un pt. rationnel.

$S_{f,g}$ define par equa. ci-dessus. $f, g(t) \neq 0, \infty$



surface fibre en conique.

image de $\mathbb{P}_1(\mathbb{Q})$ de pts rationnels de S .

$\mathbb{P}_1$ - {Nbre fin de pts}

Criteres 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 $\alpha = \beta + \gamma \quad \beta, \gamma \in Br_2(\mathbb{Q}(t))$ de pole disjoints (decomposition disjointe)

on peut ajouter $S \in Br_2(\mathbb{Q}) \quad (\beta + \delta) + (\gamma + \epsilon)$

modulo cette equivalence, il n'y a qu'un nombre fin de decomp onlin disjointe = partition des poles + formule de veredus.

on dit qu'un α est indécomposable si $\alpha = \alpha + 0$

(111)

Question 2 ? α est indécomposable le principe de l'anneau et approximation faible

mais.

i.e. Hom: $\forall p \in \mathcal{P}(\mathbb{Q}) \quad \exists t_p \in \mathbb{P}_1(\mathbb{Q}_p)$ qui "lie" α de $B_2(\mathbb{Q}_p) = \mathbb{Z}/2$ Alors $\exists t \in \mathbb{P}_1(\mathbb{Q})$ avec $\alpha(t) = 0$.

Approx. faible : si $\exists t, \alpha(t) = 0$. α - 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 $\alpha(t^{(n)}) \neq 0$ $t^{(n)} \rightarrow t_p$ pour S -topologie.

$\alpha = \beta + \gamma$ $\beta + \gamma$ = pôles disjoint, donne des coefficients pour les valeurs p -adiques.

Adèle de $\mathbb{Q}$ $\xrightarrow{\quad} \mathbb{P}_1(\mathbb{A}_{\mathbb{Q}}) = \prod_p \mathbb{P}_1(\mathbb{Q}_p)$

$t = (t_p), \alpha(t_p) \in B_2(\mathbb{Q}_p)$

$H_A = \prod_p H_p, H_p = \{t_p \mid \alpha(t_p) = 0\}$, Symbole eulérien
ces ensembles sont ouverts et fermés de $\mathbb{P}_1(\mathbb{Q}_p) = \{\text{pôle}\}$.

Soit $H_{\mathbb{Q}} = \{t \mid \alpha(t) = 0\}$.

Hom + App. faible = $H_{\mathbb{Q}}$ est dense de H_A

$\alpha = \beta + \gamma \Rightarrow H_A(\beta, \gamma) \subset H_A \quad t = (t_p) \in H_A(\beta, \gamma)$

$\Leftrightarrow t \in H_A$ et $\sum_p \text{ord}_p(\beta(t_p)) = 0$.

(par besoin de regarder γ , valabilité v . (formule de $\sum \alpha_i B_i$)

Proposition :

① $H_A(\beta, \gamma)$ est ouvert et fermé dans H_A

② $H_{\mathbb{Q}} \subset H_A(\beta, \gamma)$

Corollaire $\overline{H_{\mathbb{Q}}} \subset \bigcap_{\alpha = \beta + \gamma} H_A(\beta, \gamma)$

La conjecture qui remplace l'hom de la cas général : $H_{\mathbb{Q}}$ est dense dans l'intersection de $H_A(\beta, \gamma)$.

Proposition Supposons β et γ à supports disjoints. Alors pour tout p sauf un nombre fini. et $\forall t_p \in \mathbb{P}_1(\mathbb{Q})$ - Pôles on a soit $\beta(t_p) = 0$ soit $\gamma(t_p) = 0$.

idél

lemme soit $d \in Br_2(\mathbb{Q}(t))$, pour tout p assez grand, on a $d(t_p) = 0$ pour tout t_p dont la réduction de $\mathbb{P}_1(t_p)$ n'est pas la réduction d'un pol. (Résultat de formule explicite avec la co-contruction)

Doit la neutralité des pôles différents.

Soit S ensemble fini tel que la prop. s'applique à $\mathbb{P} \notin S$.

Soit $p \notin S$; $t = (t_p) \in H_A \rightarrow \beta(t_p) = 0$

donc $H_A(\beta, \gamma) = \{t \in H_A \mid \sum_{p \in S} \text{inv}_p(\beta(t_p)) = 0\}$

Doit ouvert et fermé.

Rem la proportion est toujours fautive si le support est fini.

Ex $d = (f)(g)$ $\forall$ surface arith. compactifié

$$\begin{array}{ccc} 0 & & V_{f,g} \\ \uparrow & & \downarrow \\ d & & \mathbb{P}_1 \end{array}$$

β et $\gamma \mapsto$ classe de Br_2 (cours de ject. de $V_{f,g}$) non vaine.

donc $\in Br_2$ (variété $V_{f,g}$ sur $\mathbb{Q}$ Groth.) modulo $Br_2(\mathbb{Q})$.

Iskovskii: on trouve tout $\in Br_2$

Exemples de Sw. D. contre Harx et App. faible.

+ Th. (modulo conj. Buriaikovski) si d a un seul pôle alors $(H) + \text{App. faible}$ vraie

Exemples:

$$\alpha = \beta + \gamma$$

$$\beta = (-1)(T^2 - 3)$$

$$\gamma = (-1)(2 - T^2)$$

$$\alpha = (-1)(f(t)) \text{ où } f = (t^2 - 3)(2 - t^2)$$

(H) est faux: sol. locales mais pas globale.

$$(*) \left[\begin{array}{l} \text{pour } n \neq \infty \text{ et } H \quad t_p \in \mathbb{P}_1(\mathbb{Q}_p) - \text{pôle} \quad \beta(t_p) \text{ ou } \gamma(t_p) = 0 \text{ et d'excl. } t_p \text{ ou} \\ \infty \quad |t| \geq \sqrt{3}, \quad |t| \leq \sqrt{2} \quad \text{soient } \beta(t_p) \neq 0 \text{ soit } \gamma(t_p) \neq 0. \quad \beta(t_p) = \gamma(t_p) \end{array} \right.$$

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 α est nul. mais $\beta(t_\infty) \neq 0$. formule de somme n'est plus valable.

et par grand, on a
 que en $\mathbb{D}_1(\mathbb{H}_n)$ n'est pas
 (193)
 co-restriction)

un n D & S.

= 0

avec $(\beta(h)) = 0$

supplémentaire.

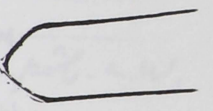
implémentaire

pas de jct. de $V_{f,g}$ un complexe.

Verifie $V_{f,g}$ une de Groth.)
 module $B_2(\mathbb{Q})$.

faible.

un seul p'de adan $(H) + H_{pp}$ forte
 ou



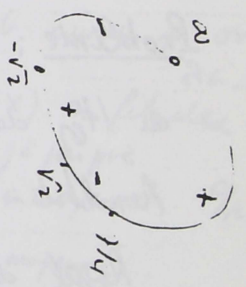
Hypothèses

faibles

$$\beta = (-1)(-1-1)$$

$$\delta = (-1)(7-2)$$

(PSU)



sur R tombe $[1/4, \infty[$, $J \cdot \sqrt{3}$, $\sqrt{3} \in$ n par de pt. isolés et ∞
 etant, par le même argument.

- Thème à la page.

- La compacité relative (pour $\mathbb{R}$ top) de $H_{\mathbb{Q}} \subset \mathbb{D}_1(\mathbb{Q})$ fournit des

nombre fini d'intervalles dont les extrémités sont des p'ds $1/\mathbb{Q}$ de $\mathbb{Q}$. Ici c'

une compacité de Mayer. Soit V un ouvert algébrique sur $\mathbb{R}$ ou $\mathbb{Q}$,

soit $V(\mathbb{Q})$ l'ensemble des $V(\mathbb{Q})$ pour $\mathbb{R}$ top. est ouvert et fermé

de $V(\mathbb{R})$: c'est une réunion de compacts connexes - En fait de convergence

exhaustive : " $\mathbb{Z}$ n'est pas épuisable j'ajoute des $\mathbb{Q}$ " :

$$\bigcup_{\mathbb{N}} V(\mathbb{Q}) \quad \pi(V(\mathbb{Q})) = \mathbb{Z} \quad \text{de l'équation } D(\underline{x}, t) : \text{ a une solution}$$

$$AH'$$

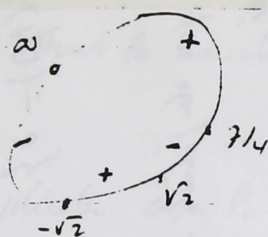
— par d'analyse p-adique.

Approximation faible

$$\beta = (-1)(4T-7)$$

$$\gamma = (-1)(T^2-2)$$

114



sur $\mathbb{R}$ semble $]7/4, \infty[$, $] -\sqrt{2}, \sqrt{2}[$ on peut pt. rationnel par 6
second, par le même argument.

- Théorème à la liasse.

- 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 pèles $1/\mathbb{R}$ de d_0 . Ici c'est
une conjecture de Mazur. Soit V un variété algébrique lisse sur $\mathbb{Q}$,
suppos. $V(\mathbb{Q})$ 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 convexes. Énoncé de conséquence
extraordinaire : " $\mathbb{Z}$ n'est pas définissable polynom. dans $\mathbb{Q}$ " :

$$V(\mathbb{Q})$$

$$\pi(V(\mathbb{Q})) = \mathbb{Z}$$

de l'équation $P(x, t)$: a une solution
en x de $\mathbb{Q}$ $\iff t \in \mathbb{Z}$.

$$\downarrow \pi$$

$$AH^1$$

par d'Analogie p-adique.

6-16-12-1991.

Problème : Démontrer que l'hypothèse H de Schinzel entraîne la conjecture "dense"

de $H_{\mathbb{Q}}$ dans $\bigcap_{\beta+r=d} H_A(\beta, r)$. Cas particulier pr Coll. Th. + densité.

Résultats récents de Ser HPP. en nombre fini, non proportionnels.

Rappel de hyp. de Schinzel

$P_i \in \mathbb{Z}[X]$, irred. sur $\mathbb{Q}$. t_9 Terme donné

$\forall p$ premier $\exists n$ tel que $\prod P_i(n) \neq 0 \pmod{p}$.

(H): il existe une infinité de $n > 1$ tel que $P_i(n)$ soit premier $\forall i$.

ex $P_1 = x, P_2 = x+2$ Nombres premiers jumeaux

difficulté x^2+1 ? ou les exemples !

version raffinée $n \leq X, P_i(n)$ premier $\forall i$ Conjecture nbe $\approx C \frac{X}{\log(X)}$
à vérification numériques.

L'hypothèse de Schinzel permet de simplifier les calculs de symboles.

Soient $t = (t_1, \dots, t_n) \in \mathbb{Z}^n$; $f_t(t), g_t(t)$ est défini $\neq 0$

(115)

$d(t) \in \mathbb{R}$ ou en sens,

$\mathbb{Z}_x = \{t \in \mathbb{Z}^n, d(t) = 0\}$; X nombre réel $\rightarrow \infty$

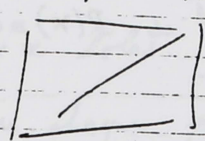
$\mathbb{Z}_x(X) = \{t \in \mathbb{Z}_x \mid |t| \leq X\}$, on s'intéresse à la taille

Cas particulier $n=1$; $d = (-1, 1)$, $t \in \mathbb{Z}$ $d(t) = 0$ $t \neq 0$ et $t = \square + \square$,

$\mathbb{Z}_x(X) = \# \{t \mid |t| \leq X, t = \square\}$

Landau: $\mathbb{Z}_x(X) \sim C \frac{X}{\sqrt{\log(X)}}$

Th 1 $\mathbb{Z}_x(X) \ll X^n / (\log(X))^{d/2}$ pour $X \rightarrow \infty$ où $d =$ Nbre de diviseurs induct de d sur l'espace affine Aff^n

 $w = \det \Omega$ une. $\rightarrow$ évaluation sans de prob de pôt. w ,

Donc le cas particulier $n=0$ pôt de d seul 0 est dans Aff

On peut travailler dans l'espace projectif.

Th 2 $\mathbb{Z}_x^{\text{proj}}(X) \ll X^{n+1} / (\log(X))^{d^{\text{proj}}/2}$

alors à pôt rationnels P_n de hauteur $\leq X$ qui annule t

Th 1 $\Rightarrow$ Th 2
Standard passage Proj. en affine de dim $+1$

$d=0$. Car où d est C^t . pas intéressant.

Conclusion: si $d \neq 0$, il y a une ∞ de $t \in \mathbb{Z}^n$ avec $d(t) \neq 0$.

Méthode de démonstration: Grand cube,

$\Lambda \subseteq \mathbb{Z}^n \subset \prod_p \mathbb{Z}_p^n = \Omega_p \subset \mathbb{A}_p$, $\mathbb{Z}_\Lambda = \{\lambda \in \Lambda \mid \text{il n'existe aucun } p \text{ avec } \lambda \in \Omega_p\}$

$\mathbb{Z}_\Lambda(X) = \{\lambda \in \mathbb{Z}_\Lambda; |\lambda| \leq X\}$ on recherche majoration de $\# \mathbb{Z}_\Lambda(X)$ en fait des volumes des Ω_p .

Mesure de Haar sur $\mathbb{Z}_p$: masse totale = 1. $\left. \begin{array}{l} \text{petit cube: } \text{mes}(\Omega_p) \\ \text{grand cube: } \text{mes}(\Omega_p) \end{array} \right\} \begin{array}{l} \text{à peu près} \\ \text{à peu près } C \geq 0 \end{array}$

Reprenons exemple. $t = \square$. $t = \prod p^{e_p} \Leftrightarrow \forall p \equiv -1 (4) \quad e_p$ est pair

mesure 0 ou $\frac{1}{p}$, $C = \frac{1}{2}$ $\Omega_p = \emptyset$ si $p \equiv 2$ ou $p \equiv 1 (4)$
 $t = \sqrt{t} \equiv 1 (2)$ si $p \equiv -1 (4)$

On suppose que l'on a un petit cube. + 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 contrôlée que $\text{mes}(\Omega'_p) = \frac{f(p)}{p} + O(\frac{1}{p^{1+\delta}})$, $\delta > 0$:

Th source hypothesis $\sum_{i=1}^n (x_i) \ll x^n / \log(x)^c$ (196) (e independent clp. i.e. e=2)

explication de vocabulaire: fonction Frobeniusienne de p : s'il existe ext. finie globalement U ,
telé que, pour p assez grand, $f(p)$ ne dépend que de la classe de conjugaison de $\sigma_p(L/\mathbb{Q})$

$$\mu \longmapsto \sum_{\chi \in \mathcal{C}} \chi(\sigma_p)$$

exemp⁶ $f(p)$ ne depend que de $p \bmod m$, (m divisi)

auto con // $f(p) = \left\{ \begin{array}{l} 1 \text{ se } p = x^2 + cy^2 \\ 0 \text{ caso contrário} \end{array} \right\}$ $\frac{1}{\sqrt{2\pi}}$

4. $K/\mathbb{Q}$ est fin $f(p) = \# \{ \text{valeurs propres de } G_K \text{ de norme } p \}$.

3) $P = X^m + \dots + a_n, a_i \in \mathbb{Z} \quad f(f) = \# \text{ Sol de } P(x) \equiv 0 \pmod{f}$

4/ forme modulaire, niveau, poids fixe. mod m fixe.

$p: X \rightarrow Y \mapsto T_p \in \text{End}(S)$ T_p est fonction fibrienne de p (cf. Deligne)

meanwert ab fct. Frobeniennorm. $c(f) = \lim_{x \rightarrow \infty} \frac{\sum_{p \leq x} f(p)}{(x / \log(x))}$

avec le decoup en caractères c'est $\mathcal{A}_1$.

Le theoreme dit que si ϵ , $\text{mes}(\Omega_p) = \frac{f(p)}{p} + O\left(\frac{1}{p^{1+\epsilon}}\right)$

$$| | < c \frac{x^n}{(\log(x))^c} \text{ c maxime def.}$$

Méthode de Cubic Spline : $Z_n(x)$ a une mesure explicite c'est pour ça et mes(Ω_p)

for even $Z_n(x) \leq (2x)^{n/2}$ as $L = \sum' \frac{T}{1 - \text{mes}(\Omega_p)}$
 $q \text{ m fact. } \square \quad \dagger \dagger \quad 1 - \text{mes}(\Omega_p)$
 $q \leq x^{1/2}$

reste en travail analytique :

$$L(Y) = \sum_{q \leq Y} \prod_{p|q} \frac{\text{mes}(\Omega_p)}{1 - \text{mes}(\Omega_p)} \quad \text{much greater than } L(Y) \gg (\log(Y))^c$$

qui se fait par la technique des séries de Dirichlet. On pose $a_p = \frac{m_s(\Omega_{p'})}{1 - m_s(\Omega_p)}$
 10 si q est un fa $\square$ $= \frac{1/p}{p} + O(\frac{1}{p^{1+s}})$

$$a_q = \begin{cases} 0 & \text{if } q \text{ is even} \\ \prod_{p|q} a_p & \text{min, on constant } \sum_i a_i q^{-s} = \phi(s) \end{cases}$$

ou $\phi(s) = \prod_p (1 + a_p p^{-s})$, comportement de $\phi(s)$ en $s=0$

On first volume in *Thermoelectric Hardy & Littlewood* (Oc. Vol 6 p 526, Th)

Soil $\phi(s) = \sum a_n n^{-s}$ $a_n \text{ coef.} > 0$, convy for $\text{Re}(s) > 0$

on suppose de + que $\phi(s) = \delta s^{-c}$ pour $s \rightarrow 0$

alors le 1^{er} sommait. $\sum_{n \leq Y} a_n = \frac{\delta}{\Gamma(1+c)} \log(Y)^c$ restes tout y est

1. - 1st P. 0 1 m. L. 100 m. P. 100 m. L. 100 m.

$$a_p = \frac{f(p)}{p} + O\left(\frac{1}{p^{1/2}}\right) \quad f: \sum \lambda_i \chi_i \quad \Phi \equiv \prod_i L(s+1, \chi_i)^{2i} \quad \Re(s) > 0.$$

$$\Phi(s) \sim O\left(\frac{1}{s}\right)^{21} \quad / \text{ les exposants } 2i \text{ ne sont pas g n raux, bon demand .}$$

le 30. R  ti    voir que l'on peut bien appliquer la th.    la sp cialisation de Δ . Remerci    la note pour le cas g n ral.

Cas Particulier $\mathbb{P}_1$, $\alpha \in \text{Br}_2(\mathbb{Q}(t))$, $t \in \mathbb{Q}$, $\alpha(t) = 0$?

definissons un $\Omega_p \subset \mathbb{P}_1(\mathbb{Q}_p)$ / p  les et r  sides de α

$P_1, \dots, P_n$ r  sides $r_1, \dots, r_n$    $\mathbb{P}_1$ corps r  siduel $k_i/\mathbb{Q}$.

$r_i \in k_i^* \text{ mod carr  s} \iff L_i/k_i$ quadratique.

$d = \text{nombre de p  les}$.

pour chaque p , $\mathbb{Q}_p$, k_i r  duits. $k_i = \prod k_{i,p,j}$, pour chaque L_i :

$$L_{i,p,j} = \begin{cases} k_{i,p,j} \times k_{i,p,j} \\ \text{ext. quadrat.} \end{cases} \quad / L_{i,p,j} / \mathbb{Q}_p \text{ quadratique}$$

On ne s'int  resse qu'aux couples (i,j) tels que $k_{i,p,j} = \mathbb{Q}_p$

ils correspondent aux p  les de $\alpha_p \in \text{Br}_2(\mathbb{Q}_p(t))$ qui sont rationnels sur $\mathbb{Q}_p$.

Definissons des points $P_{i,j,p} \in \mathbb{P}_1(\mathbb{Q}_p)$. On peut d  montrer que pour p

assez grand on peut exhiber $\alpha(t) \in \text{Br}_2(\mathbb{Q}_p) \approx \{0, 1/2\}$

R  sultat Soient $\tilde{P}_{i,j,p}$ la r  duction mod p (des points $P_{i,j,p} \in \mathbb{P}_1(\mathbb{F}_p)$)

si $\tilde{E} \neq \tilde{P}_{i,j,p}$ $\alpha(t) \neq 0$

si $\tilde{P}_{i,j,p}$ sont distincts (pour grand p) $\{ \text{liste des conclusions} \}$    prouver

si $\tilde{E} = \tilde{P}_{i,j,p}$ soit e le max. tel que $t \equiv P_{i,j,p} \pmod{p^e}$

non p  le

on note $e = v(t, P_{i,j,p})$ alors $\alpha(t) = 0$ si e est pair $\neq 0$ sinon.

Le nouveau Ω_p est donc d  fini par des congruences modulo p^2

D'o   $e=2$, et $\text{mes}(\Omega_p) = \frac{f(p)}{p} + O\left(\frac{1}{p^2}\right)$

et $f(p) = \# \text{ points } P_{i,j,p}$: pr  cis   le nombre de valeurs de degr   2 de k_i au-dessus de p (attention il faut    plus $L_{i,p,j}$ quadratique)

ce qui donne moyenne de $f(p) = \frac{d}{2}$.

Problème qui a posé:

118

1. On aimerait avoir de minoration, (pour voir que les majora, ne sont pas trop sharp) hypothèse la + optimiste, Don C. Th2 sur le P_n .

$$\text{on a } Z_d^{\text{proj}}(x) \gg x^{u+1} / \log(x)^{d \text{ proj}/2} \text{ si } Z(x) \neq \emptyset \quad \left| \begin{array}{l} \text{même } n=1 \\ \text{est pr} \\ \text{connu.} \end{array} \right.$$

On peut tester sur machines (Maths, Cray, non concluant!)

exemples de Cray $(-1, f(t)) \quad \mathbb{P}_1, \quad f(t) = \begin{array}{l} t(t^2+2) \\ t(t^2+5) \\ t(t^4+2)(t^4+3)(3t^4+1)(2t^4+3) \\ (3t^4+2) \end{array}$

$(-t, t^3+t+1)$

① $t(t^2+2) \quad 0, \pm\sqrt{-2}, \infty \quad \text{pôle} : 3 \quad Z(x) \gg x^2 / \log(x)^{3/2}$

② $t(t^2+5) \quad 0, \pm\sqrt{-5}, \infty \quad \text{pôle} : 3,$

③ $\underline{\hspace{10em}} \quad Z(x) \gg x^2 / \log(x)^{7/2}$

pour ③ ça colle.

pour ① et ② la machine refuse à donner 1,25?

Derrière ces $(-t, t^3+t+1) \quad t=0$ pas un pôle, 2 complexes, 1 réel pôle, semble colle numériquement.

Cas particulière offus: $(x, y), \quad 1 \leq x, y \leq X$ tels que $(x, y) = 0$

Comme $(1, -x, -y)$ a un pt. rationnel. Soit $N(X)$ le nombre

le Th. dit que $N(X) \ll \frac{X^2}{\log(X)} \quad (\text{Lewy's problem})$

en sens inverse ordonnance semble acceptable - Voir donc la note

résultat fortel: $N(X) \gg \frac{X^2}{\log(X)^2} : \text{pour cela on prend } (x, y) \text{ premiers}$
 $\equiv 1 \pmod{4} \quad d(x, y) = 0 \text{ si } \left(\frac{x}{y}\right) = 1 -$

Naïvement: $\approx \left(\frac{X}{\log(X)}\right)^2 \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \quad ? \quad \text{pour cela il faut prouver que}$

le symbole de Legendre est distribué au hasard:

$$\sum_{\substack{x, y \text{ premiers distincts} \\ \equiv 1 \pmod{4}}} \left(\frac{x}{y}\right) \stackrel{?}{=} o\left(\frac{X^2}{\log(X)^2}\right)$$

ce fait Heilbronn montre nettement mieux $O(X^\delta) \quad \delta = 7/4?$

Quelques autres cas amusants:

$(a, b, c) \in \mathbb{Z}^3 \quad |a, b, c| < \infty$ tel que $aX^2 + bY^2 + cZ^2 = 0$ ait un

pt rationnel, combien y-en-a-t-il? pour $N \rightarrow \infty$ donne estimation?

(prends 6 symboles $(-ab, -ac)$)

(19)

même problème pour la conique générale

$$ax^2 + bxy + cy^2 + dxz + exz + fz^2 = 0$$

$$/u.c. \dots 1 \leq x \quad N(x)? \ll \frac{x^6}{\log(x)^{1/2}}$$

Beaucoup de questions ouvertes souvent sur nos cas (!)
mais 6 plus intéressent comprendre le premier exemple de Gray.
- Voir 6 exemples $(-1, t) + (5, t+1)$

(prends le symbole $(-ab, -ac)$)

(120)

même problème pour la conique générale

$$ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0$$

$$/a.e. \dots / \leq x \quad N(x)? \ll x^{6/5} / \log(x)^{1/2}$$

Beaucoup de questions ouvertes souvent très dur (!)

mais le plus intéressant comprendre le premier exemple de Grzy.

Un exemple $(-1, t) + (5, t+1)$

20-1.92 : Application de la Conjecture de Schinzel.

Hypothèse (H) de Schinzel $\Rightarrow$ Th. de densité de la Hasse-Mann

le corps de nombre $\underline{d} = (d_i)_{i \in I_{\text{fin}}}$ $d_i \in \text{Br}(k(T))$ $n d_i = 0$ n fixe $(d_i \in H^2(k(T), \mu_n^I))$

? $t \in \mathbb{P}_1(k)$ où les d_i s'annulent. (t non pôle et $d_i(t) = 0 \forall i \in I_{\text{fin}} \text{ de } \text{Br}_n(k)$)
noté $\underline{d}(t) = 0$.

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 = $\prod_v k_v$, $\mathbb{P}_1(\mathbb{A}_k) = \prod_v \mathbb{P}_1(k_v)$ topologie produit qui a fait un
espace compact. $(x_v) \in \mathbb{P}_1(k_v)$, x_v non pôle pour $\underline{d}|_{k_v}$; $\underline{d}(x_v) \in H^2(k_v, \mu_n^I)$

$N_k \subset \mathbb{P}_1(\mathbb{A}_k) \supset N_k(\#) = \{ (x_v), x_v \in \mathbb{P}_1(k_v), \underline{d}(x_v) = 0 \text{ dans } H^2(k_v, \mu_n^I) \}$

$N_k(k) \subset N_k$: principe de Hasse $\Leftrightarrow N_k(k)$ dense dans N_k .

Ensemble subordonné. k corps $\underline{d} = (d_i) \in \text{Br}_n(k(T))$
 y pt fermé de $\mathbb{P}_1/k$
 $\text{res}_y d_i \in H^2(k/y, \mathbb{Z}/n\mathbb{Z})$

" $\text{Hom}(G_{k/y}, \mathbb{Z}/n\mathbb{Z}) = \text{caractère du corps résiduel}$ "

on $\text{res}_y d_i$ p.p. $\neq 0$; $\sum_i' \text{cor}_y(\text{res}_y d_i) = 0$

$\beta \in \text{Br}_n(k(T))$ β est subordonné à $\underline{d} = (d_i)$ si

il y a pt fermé a de $\mathbb{P}_1/k$ $\text{res}_y(\beta)$ combinaison $\mathbb{Z}$ linéaire des $\text{res}_y(d_i)$

Exemples triviaux:

⊗ β constant ($\in \text{Br}_n(k)$) } - ce qui est intéressant - c'est quand
⊗ β combinaison linéaire des d_i } il y en a d'autres.

interprétation: V variété lisse irréductible et β morphisme dominant $V \xrightarrow{\beta} \mathbb{P}_1$

$k = k(V) \supset k(T)$ on a des $d_{i,k}, \beta_{i,k} \in \text{Br}_n(k)$ -

les " $d_{i,k}$ " sont non ramifiés i.e. $\in \text{Br}(V)$ et si β est subordonné à $\underline{d}$ alors

β_k est non ramifié sur V .

Revenons au cas. Soit β subordonné à α . Si $x = (x_v) \in \mathbb{A}^n(\mathbb{A}_k)$, x_v non p.s. d. regardons la quantité $e_\beta(x) = \sum_{v \in V_k} \beta(x_v)$ où $\beta(x_v) \in B_{r_n}(k_v) \hookrightarrow \mathbb{Q}_p$ en fait dans $\frac{1}{n} \mathbb{Z}/\mathbb{Z}$ - qui l'on identifie à $\mathbb{Z}/\mathbb{Z}$.

Lemme Si β subordonné à α la fonction $e_\beta : N_\alpha \rightarrow \mathbb{Z}/\mathbb{Z}$ est localement constante.

et même mieux: il existe un polynôme $S \in \mathbb{Z}[x] = S \in V_k$ tel que $x \in S \Rightarrow e_\beta(x) = 0$ implique $\beta(x_v) = 0$.

et il est clair que $e_\beta(N_\alpha(k)) = 0$. On introduit donc l'espace M_α :

$$M_\alpha = \{ x \mid x \in N_\alpha, e_\beta(x) = 0 \text{ pour tout } \beta \text{ subordonné à } \alpha \}$$

M_α évidemment est fermé dans N_α . (se ramener au cas constant ...)

Conjecture 1: H.M. $N_\alpha(k)$ est dense dans M_α .

Conséquence si $M_\alpha \neq \emptyset$ alors $N_\alpha(k) \neq \emptyset$.

Le Théorème (H) $\Rightarrow$ conj 1 ; Rappel de l'hypothèse H.

Soit (P_j) des poly. irréductibles sur $\mathbb{Q}$, à coeff. entiers, en nombre fini σ termes dominant > 0 et tels que $\forall p$ premier, il existe $x \in \mathbb{Z}/p\mathbb{Z}$ tel que toutes les $P_j(x)$ sont $\neq 0$ ds $\mathbb{Z}/p\mathbb{Z}$ alors il existe une infinité d'entiers $n > 0$ tels que $P_j(n)$ soit premier quel que soit j .

Cas particuliers: Coll. Théorème Sanson $k = \mathbb{Q}$; $n = 2$ $\alpha_i = (a_i, P_i(T))$ $a_i \in \mathbb{Q}$.

P_i irréductibles (les β subordonnés sont triviaux) alors $M_\alpha = N_\alpha$ au $\mathbb{Q}$.

existence de solutions rationnelles dans les adéliques. c'est donc Harre.

cas particuliers les P_i sont unitaires: $M_\alpha \neq \emptyset$ si l'oc. t grand > 0 est non

p premier $t = \frac{1}{p^{2n}}$ pour N grand donc casé.

Donc, sous (H), on peut rechercher $(Q_j, P_j(t)) = 0$ ex $Q_j = T-1$, $P_j(t) = T+1$

ex P_j $t, t+1, \dots, t+5$ sous (H) existe en rationnels deux dans $\mathbb{Q}^+$

t_j $t, t+1, \dots, t+5$ sont $\square + \square$ ds $\mathbb{Q}$

pour $t, t+1, t+2$ Coll. Th. suit facile

Comment faire sous H? p premier $\equiv 1 \pmod{4} \Rightarrow p = 4A+1$

façon de faire $t, t+A^2, \dots, t+5A^2$

essais $t = 1+4x$ on veut rendre premier $1+4x, 1+4x+A^2, \dots, 1+4x+5A^2$

On veut montrer que si $(x_v) \in \prod_v \mathbb{A}_k \subset \prod_v \mathbb{P}_1(k_v)$ on veut prouver que dans tout voisinage il existe un rationnel. Soit 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 $x \in \mathbb{P}_1(k)$ de ce voisinage.

Notons $\mathcal{V}(x) = \prod_v U_v$ $U_v = \mathbb{P}_1(k_v)$ pour $p \nmid v$

on voit les pôles comme des sections

$\xrightarrow{S} \text{Spec}(O_k)$

l'hypothèse de Schurzel permet de lier les x qui reviennent exactement une fois chaque variété polaire. On retrouve déjà ce genre d'obstruction dans le lemme du principe de Hasse (remarque de Albert Theilme).

Démonstration dans un cas particulier. $k = \mathbb{Q}$, un seul α , n quelconque.

- On se donne $(x_v) \in \prod_v \mathbb{A}_k$ et un voisinage. On peut agrandir à volonté S et diminuer U_v .
- On peut supposer α constant sur U_v $\alpha = 0$

- on peut supposer $S \supset$ places archimédiennes, et U_v ouvert pour ces places

il existe point rationnel de $\mathbb{P}_1$ qui $t \in \text{archimédien} \in U_v$. Par un automorphisme qui point est α ; en particulier α n'est pas un pôle. Les conditions archimédiennes :

$x \in k$ doivent être arbitrairement grand en les places archimédiennes.
- les pôles sont des entiers

Soit $\mathcal{Y}$ l'ensemble : $\mathcal{Y}$ = réunion des pôles de α , no. schéma fermé de $\mathbb{P}_1$

Soit y pt fermé de $\mathcal{Y}$. $k(y)$ corps résiduel $d_y = [k(y) : k]$, $\alpha \notin \mathcal{Y}$ Tenir $\rightarrow$

$t_y \in k(y)$ $r_y(\alpha) \in H^1(k(y), \mathbb{Z}/n\mathbb{Z})$

Soit $t \in k$, t non pôle de α $d(t) = d(\alpha) + \sum_y \omega_y(t - t_y) \cdot r_y(\alpha)$
 $\omega_y \in H^1(k, \mu_n)$ $r_y \in H^1(k, \mathbb{Z}/n\mathbb{Z})$

on peut aussi écrire $d(\alpha) + \sum_y \omega_y(1 - \frac{t_y}{t}) r_y(\alpha)$

Conditions sur S , $S = S(k, N)$ $N \geq 1$

= places archimédiennes $\cup$ places ultram. de caract. $\neq p$ et $\leq N$

avec propriétés suivantes :

(a) $N \geq n$ (n de B_n)

(b) $N \geq [k : \mathbb{Q}] + \sum_{y \in \mathcal{Y}} d_y$

(c) si $v \notin S$, dis du pôle avec $\mathbb{P}_1$ et t_y est inversible en v

- on veut aussi que les racines de Δ d'entiers soient distinctes

① les inv. de $\Delta(x)$ en les places $v \notin S$ sont 0.

② les caractères $\text{res}_y(\Delta)$ sont non ramifiés en toute place de $k(y)$ de caract. unit.

③ S' $\mathcal{O}_k$ principal

Enfin, que si $v \notin S$ et si $x_v \in \mathbb{P}^1(k_v)$ non pôle on a

$\Delta(x_v) = 0$ dans $B_n(k_v)$ si $\tilde{x}_v$ (réduct mod v de x_v) distinct des racines mod v de pôles.

Si $\tilde{x}_v$ est le réduc mod v d'un pôle : $\Delta(\tilde{x}_v) = -v(x_v, y_v) \cdot \text{inv}_{\tilde{x}_v} r_y(x)$
 $k_v(y_v) = k_v$ le plus proche
 $k_v \rightarrow \mathbb{Z}/n\mathbb{Z}$

Ceci montre clairement que le β s'annule sur un genre g . On introduit les invariants $\varepsilon(y)$, $y \in Y$ (plutôt $\varepsilon(y, (x_v))$) - de fait, par

$$\varepsilon(y) = \sum_{v \in S} \text{inv}_{\tilde{x}_v} (t - t_y) \cdot r_y(x) \in \mathbb{Z}/n\mathbb{Z}$$

(on aurait pu en introduire $\pm$ pour chaque x_i ou plusieurs x_i .)

Lemme : Soient m_y , $y \in Y$ des entiers tels que

$$\sum_y m_y \text{cor}_y r_y(x) = 0 \quad \text{dans } H^1(k, \mathbb{Z}/n\mathbb{Z}).$$

On en déduit (Cebotarev)

$\exists w \notin S$ telle que pour $H_y \in Y$, $\text{inv}_w(\text{cor}_y r_y(x))$ est égal à $-\varepsilon(y)$

On peut choisir $q \in \mathcal{O}_k$ tel que $w(q) = 1$, $v(q) = 0$ $v \notin S$ $v \neq w$.

$A = \prod_{p \in N} p$, choisissons $x \in k$ (liant Δ)

$$x = \frac{a}{qA^n} \quad \text{avec } a \in \mathcal{O}_k \quad (\text{un seul pôle en } q, \text{ en dehors de } S)$$

condition sur a :

1) $a \equiv a_0$ (à fixer) mod (A^{n+m}) de telle sorte que $x \in U_v$ $\forall v \in S - S_n$

2) $\forall v \in S_n$ $|a|_v \gg 0$

3) $P_y(\frac{a}{qA^n})$ a une valeur nulle $\forall y \notin S$ à l'exception d'une valeur y_0

avec n arbitrairement grande ou cette valeur est égale à 1.

③ est possible pour H

il faut connaître $\text{inv}_v \Delta(x) = \dots$ $v \in S$ $\text{inv}_v(\Delta(x)) = 0$ par ①

$v \notin S$ (c'est $(x - t_y) \cdot r_y(x)$)

x entier sauf pour w
 $\tilde{x}_w = \infty$

$$\text{inv}_w \Delta(x) = 0$$

~~Affirmation~~ : $\text{Cor}_y(x - t_y) \cdot r_y(x) \in B_n(k)$

(124)

~~il y a une relation de dépendance entre ces r_y .~~

- calculons la somme des coeff. = 0
 (2) termes dans S $\varepsilon(y)$

(3) en w : $-\varepsilon(y)$ grâce au choix de w

(4) en $v_y = -\text{inv}(r_y(x))$ en v_y

D'où l'on déduit $\text{inv}(r_y(x))$ en $v_y = 0$.

On revient à x . $\text{Cor}_y(x - t_y) \cdot r_y(x)$ est nul en v_y .

Indication sur la façon d'aborder (H) ~~sur~~ dans les corps de nombres.

Si P irréductible sur k , il suffit de prendre la norme.

k/k_0 . P irréductible sur k $\exists$ Norme finie d'hyperplan k_0 -affine de k
 tels que H a $\neq \emptyset$ hyperplan $N_{k/k_0}(P(H, a))$ est k_0 -irréductible.

On peut donc généraliser à un Nbre fin de P_j .

$k(y)$
 remplace y par $y-a$ pour avoir un polynôme sur k_0 .

k
 k_0

Conséquence de H pour les corps de nombres

$S(k, k)$ P_j poly k -irréductible de d_j° d_j

$N \geq [k: k_0] \sum d_j$

Soit $N \geq N$, alors pour (H) il existe $x \in C_k$

$|x|_p > N$ (le plus archi).

$x \notin j \quad \exists v_j \notin S \quad t_y \quad v(P_j(x)) = 0, v \notin S \quad v \neq v_j$

$\forall v_j \quad (P_j(x)) = 1$

Caract rest $v_j \geq N$.