

COURS DE JEAN-PIERRE SERRE

JEAN-PIERRE SERRE

ANNE QUÉGUINER (réd.)

Quelques exemples d'invariants cohomologiques

Cours de Jean-Pierre Serre, tome 15 (1993-1994)

http://www.numdam.org/item?id=CJPS_1994__15_

© 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

COLLÈGE DE FRANCE

J-P. SERRE

chaire d'Algèbre et Géométrie

Cours 1993-1994

Quelques exemples d'invariants cohomologiques

Notes de Anne Quéguiner

N° Cote : PB 929 9ap
Institut Henri Poincaré BIBLIOTHÈQUE 11, rue P.-et-M.-Curie 75231 PARIS CEDEX 05
N° Inventaire : 28 545 B

- 4 FEV. 2000

Algèbre et géométrie

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

Le cours a continué ceux de 1962/1963, 1990/1991 et 1991/1992, consacrés à la *cohomologie galoisienne*. Il a comporté trois parties :

1. Cohomologie négligeable

1.1. *Notations*. Si k est un corps commutatif, on note k_s une clôture séparable de k , et Γ_k le groupe de Galois de k_s sur k . Si M est un Γ_k -module (discret), on note indifféremment $H^q(\Gamma_k, M)$ et $H^q(k, M)$ ses groupes de cohomologie.

1.2. *Définition de la cohomologie négligeable*. Soient G un groupe fini et M un G -module. Un élément x de $H^q(G, M)$ est dit *négligeable* si, pour tout corps k et tout homomorphisme continu $\varphi : \Gamma_k \rightarrow G$, on a $\varphi^*(x) = 0$ dans $H^q(k, M)$, cf. *Résumé de cours* 1990/1991, §7.

Cette définition fait intervenir, en apparence, tous les corps k , et tous les homomorphismes φ . En fait, on peut construire, pour chaque groupe fini G , une extension galoisienne « verselle » L_G/K_G , de groupe de Galois G , telle que $x \in H^q(G, M)$ soit négligeable si et seulement si $\varphi^*(x) = 0$ pour l'homomorphisme $\varphi : \Gamma_{K_G} \rightarrow G$ associé à L_G . (Si l'on choisit un plongement de G dans un groupe symétrique S_N , on peut prendre pour L_G le corps de fonctions rationnelles $\mathbb{Q}(T_1, \dots, T_N)$, sur lequel G opère de façon évidente.)

On déduit de là :

1.3. *Il existe un entier $q(G)$ tel que, si $q > q(G)$, les deux propriétés suivantes d'un élément x de $H^q(G, M)$ soient équivalentes :*

- (i) x est négligeable ;
- (ii) la restriction de x aux sous-groupes d'ordre 2 de G est nulle.

(Noter que l'implication (i) \Rightarrow (ii) est vraie sans supposer $q > q(G)$.)

En particulier, tout élément d'ordre impair de $H^q(G, M)$ est négligeable si $q > q(G)$.

1.4. L'énoncé ci-dessus donne une caractérisation simple des classes de cohomologie négligeables lorsque la dimension q est grande. Dans la direction opposée, on a :

(a) Si $q \leq 1$, ou si $q = 2$ et G opère trivialement sur M , aucun élément non nul de $H^q(G, M)$ n'est négligeable.

D'autre part (cf. B.B. Lure, *Trudy Math. Inst. Steklov* 183, 1990) :

b) Si l'ordre de G est > 2 , il existe un G -module fini M tel que $H^2(G, M)$ contienne un élément négligeable $\neq 0$.

1.5. Détermination des classes de cohomologie négligeables lorsque G est cyclique d'ordre premier.

Supposons G cyclique d'ordre premier p , et soit s un générateur de G . Le cas $p = 2$ est peu intéressant : il n'y a pas de classe de cohomologie négligeable, à part 0, comme on le voit en prenant $k = \mathbf{R}$.

Supposons donc $p > 2$. Soit \hat{G} le pro- p -groupe défini par deux générateurs u, v liés par la relation $uvu^{-1} = v^{1+p}$, et soit $\varphi : \hat{G} \rightarrow G$ l'unique homomorphisme continu tel que $\varphi(u) = 1$ et $\varphi(v) = s$. On démontre :

(a) Pour que $x \in H^q(G, M)$ soit négligeable, il faut et il suffit que $\varphi^*(x) = 0$ dans $H^q(\hat{G}, M)$.

Comme \hat{G} est un groupe de dimension cohomologique stricte égale à 2, on déduit de là :

(b) Si $q > 2$, tout élément de $H^q(G, M)$ est négligeable.

Pour $q = 2$, la situation est différente. Si l'on identifie $H^2(G, M)$ à $\text{Ker}_M(1 - s)/\text{Im}_M(1 + s + \dots + s^{p-1})$, on trouve :

(c) Pour que $x \in H^2(G, M)$ soit négligeable, il faut et il suffit que l'on puisse représenter x par un élément de $\text{Ker}_M(1 - s)$ de la forme $y - sy$, où y est un élément de M d'ordre une puissance de p .

1.6. Autres exemples. On aimerait avoir des résultats aussi précis que ceux du n° 1.5 pour d'autres groupes finis, ne serait-ce que les groupes cycliques d'ordre p^m , $m > 1$. Cela ne paraît pas facile, à moins de faire des hypothèses restrictives sur le G -module M . Ainsi, lorsque $M = \mathbf{Z}/2\mathbf{Z}$, on peut déterminer

pour tout q la partie négligeable de $H^q(G, \mathbb{Z}/2\mathbb{Z})$ lorsque G est l'un des groupes suivants :

$C_2 \times \dots \times C_2$, 2-groupe abélien élémentaire ;

C_{2^m} , groupe cyclique d'ordre 2^m ;

D_4 , groupe diédral d'ordre 8 ;

Q_8 , groupe quaternionien d'ordre 8.

Dans chacun de ces cas, on constate qu'un élément de $H^q(G, \mathbb{Z}/2\mathbb{Z})$, $q > 2$, est négligeable si et seulement si ses restrictions aux sous-groupes d'ordre 2 de G sont nulles. Par exemple, si $G = Q_8$, les éléments non nuls de $H^q(G, \mathbb{Z}/2\mathbb{Z})$, $q > 2$, sont négligeables si q n'est pas divisible par 4.

1.7. Le cas du groupe symétrique S_n

On démontre en utilisant les résultats du n° 2.2 ci-après :

(a) *Tout élément de $H^q(S_n, \mathbb{Z}/N\mathbb{Z})$, $q > 0$, N impair, est négligeable.*

(On suppose que l'action de S_n sur $\mathbb{Z}/N\mathbb{Z}$ est triviale.)

(b) *Pour qu'un élément de $H^q(S_n, \mathbb{Z}/2\mathbb{Z})$ soit négligeable, il faut et il suffit que ses restrictions aux sous-groupes d'ordre 2 de S_n soient nulles.*

2. Invariants des algèbres étales

2.1. Invariants cohomologiques de G -torseurs

Rappelons la définition (cf. *Sém. Bourbaki*, exposé 783, §6).

Les données sont :

— un groupe algébrique lisse G sur un corps k_0 ;

— un entier $i \geq 0$ et un module galoisien C sur k_0 , que l'on suppose fini d'ordre premier à la caractéristique de k_0 .

A toute extension k de k_0 sont attachés, d'une part l'ensemble pointé $H^1(k, G)$ des classes de G -torseurs sur k , et d'autre part le groupe de cohomologie $H^i(k, G)$

Un *invariant cohomologique* de type $H^i(\cdot, C)$, pour les G -torseurs, est un *morphisme a* du foncteur $H^1(k, G)$ dans le foncteur $H^i(k, C)$, défini sur la catégorie des extensions k de k_0 . Un tel invariant associe, à tout G -torseur X sur k , un élément $a(X)$ de $H^i(k, C)$; de plus, si k' est une extension de k , et si X' est le G -torseur sur k' déduit de X par extension des scalaires, l'invariant $a(X')$ est l'image de $a(X)$ par l'application $H^i(k, C) \rightarrow H^i(k', C)$.

2.2. Invariants cohomologiques des algèbres étales de rang donné

On peut appliquer ce qui précède au cas où G est le *groupe symétrique* S_n ($n \geq 1$), vu comme groupe algébrique de dimension 0. Dans ce cas, un G -torseur X sur k s'interprète comme :

- un homomorphisme continu $\varphi : \Gamma_k \rightarrow S_n$, à conjugaison près ;
- une k -algèbre étale E de rang n , à isomorphisme près.

Un invariant cohomologique de type $H^i(\cdot, C)$ pour S_n , est une fonction

$$E \mapsto a(E) \in H^i(k, C)$$

qui, à toute algèbre étale E de rang n sur une extension k de k_0 , associe un élément de $H^i(k, C)$, de façon compatible avec les extensions de scalaires. (Cette dernière propriété entraîne aussi une compatibilité avec les *spécialisations*, comme me l'a signalé M. Rost.)

Convenons de dire qu'une algèbre étale est *multiquadratique* si elle est produit d'algèbres de rang 1 ou 2. On démontre :

(i) *Supposons que $a(E) = 0$ pour toute algèbre multiquadratique. Alors $a = 0$.*

Disons que a est *normalisé* si $a(E) = 0$ lorsque E est *scindée* (i.e. isomorphe à $k \times \dots \times k$).

(ii) *Si a est normalisé, on a $2a = 0$.*

Le cas le plus intéressant est celui où $C = \mathbf{Z}/2\mathbf{Z}$ (k_0 étant de caractéristique $\neq 2$). Si E est une algèbre étale de rang n sur k , la *forme trace* q_E de E est une forme quadratique non dégénérée de rang n . Ses classes de Stiefel-Whitney $w_i(q_E) \in H^i(k, \mathbf{Z}/2\mathbf{Z})$ sont des *invariants cohomologiques* de type $H^i(\cdot, \mathbf{Z}/2\mathbf{Z})$ de l'algèbre étale E . En fait, ce sont essentiellement les seuls. On déduit en effet de (i) le résultat suivant :

(iii) *Si $C = \mathbf{Z}/2\mathbf{Z}$, tout invariant cohomologique de type $H^i(\cdot, C)$ s'écrit de façon unique sous la forme :*

$$a(E) = \sum_{j=0}^m \gamma_j w_j(q_E) \quad \text{avec } \gamma_j \in H^{i-j}(k_0, C) \text{ et } m = [n/2].$$

Lorsqu'on applique ceci aux classes de Stiefel-Whitney *galoisiennes* $w_i^{\text{gal}}(E)$, on retrouve une formule de B. Kahn (*Invent. Math.* 78, 1984) :

$$(iv) \quad w_i^{\text{gal}}(E) = \begin{cases} w_i(q_E) & \text{si } i \text{ est impair} \\ w_i(q_E) + (2) \cdot w_{i-1}(q_E) & \text{si } i \text{ est pair} \end{cases}$$

De plus :

(v) *On a $w_i^{\text{gal}}(E) = 0$ si $i > m = [n/2]$.*

2.3. Invariants à valeurs dans le groupe de Grothendieck-Witt

Supposons la caractéristique $\neq 2$. Dans la définition des invariants cohomologiques on peut remplacer le foncteur $k \mapsto H^i(k, \mathbb{C})$ par le foncteur $k \mapsto \text{GrW}(k)$, où $\text{GrW}(k)$ est l'anneau de Grothendieck-Witt des classes de formes quadratiques sur k . (On pourrait utiliser aussi l'anneau de Witt usuel $W(k)$, mais c'est moins commode, car les puissances extérieures λ^i sont définies sur $\text{GrW}(k)$ mais pas sur $W(k)$.) On obtient ainsi la notion d'invariant de type GrW des algèbres étales de rang n . Exemple : l'application

$$E \mapsto \lambda^i(q_E),$$

qui, à une k -algèbre étale E , associe la puissance extérieure i -ème de sa forme trace.

Les résultats du n° 2.2. se transposent sans difficulté. Ainsi :

(i) Si un invariant de type GrW s'annule sur les algèbres multiquadratiques, il est identiquement nul.

(ii) Tout invariant de type GrW est combinaison linéaire, à coefficients dans $\text{GrW}(k_0)$, des $\lambda^i(q_E)$, $0 \leq i \leq m = [n/2]$.

Ceci permet de prouver des identités portant sur les $\lambda^i(q_E)$ en les vérifiant lorsque E est multiquadratique. Or, dans ce cas, on peut écrire q_E sous la forme $\omega_n \oplus q'$, où q' est de rang m , et où ω_n est la forme de rang $n - m$ définie par :

$$\omega_n = \begin{cases} m\langle 2 \rangle = \langle 2, \dots, 2 \rangle & \text{si } n = 2m \\ 1 + m\langle 2 \rangle = \langle 1, 2, \dots, 2 \rangle & \text{si } n = 2m + 1. \end{cases}$$

On obtient ainsi :

(iii) Pour toute algèbre étale E de rang n , on a :

$$\lambda^n(q_E) \cdot \lambda^i(q_E - \omega_n) = \langle 2^m \rangle \cdot \lambda^{m-i}(q_E - \omega_n) \text{ pour tout } i.$$

Noter que $\lambda^n(q_E) = \langle d_E \rangle$, où d_E est le discriminant de E , de sorte que la formule ci-dessus peut s'écrire :

$$(iii') \lambda^i(q_E - \omega_n) = \langle 2^m d_E \rangle \cdot \lambda^{m-i}(q_E - \omega_n) \text{ pour tout } i.$$

En particulier :

$$(iv) \text{ On a } \lambda^i(q_E - \omega_n) = 0 \text{ pour tout } i > m.$$

3. La forme trace en rang ≤ 7

Soit k un corps de caractéristique $\neq 2$. Soit n un entier ≥ 1 . Une forme quadratique q sur k , de rang n , est appelée une forme trace s'il existe une k -algèbre étale E de rang n telle que q_E soit isomorphe à q .

Le cas où n est impair se ramène à celui où n est pair. En effet, il résulte d'une construction de Mestre (*J. Algebra* 131, 1990) que l'on a :

3.1. Une forme quadratique de rang n impair est une forme trace si et seulement si elle est isomorphe à $\langle 1 \rangle \oplus q'$, où q' est une forme trace de rang $n - 1$.

3.2. Caractérisation des formes trace de rang ≤ 7

Vu 3.1., on peut se borner à $n = 2, 4$ ou 6 . On trouve alors qu'une forme quadratique q de rang n est une forme trace si et seulement si elle satisfait aux conditions suivantes :

(pour $n = 2$) q contient $\langle 2 \rangle$;

(pour $n = 4$) q contient $\langle 1 \rangle$ et $w_3(q) = 0$;

(pour $n = 6$) q contient $\langle 1, 2 \rangle$, et contient $\langle 1, 1, 2 \rangle$ sur $k(\sqrt{2d})$, où d est le discriminant de q .

3.3. Action des automorphismes externes de S_6

Le cas $n = 6$ présente un intérêt particulier : c'est le seul où le groupe $\text{Out}(S_n) = \text{Aut}(S_n)/\text{Int}(S_n)$ soit non trivial. Si E est une algèbre étale de rang 6, correspondant à $\varphi : \Gamma_k \rightarrow S_6$, le composé φ' de φ et d'un automorphisme externe de S_6 définit une autre algèbre étale E' de rang 6 (« résolvante sextique »). D'après le n° 2.3, la forme trace de E' peut s'exprimer en termes des $\lambda^i(q_E)$. On trouve :

$$q_{E'} = \lambda^3(q_E) - \langle 1, 2 \rangle \cdot \lambda^2(q_E) + \langle 1, 1, 2 \rangle \cdot q_E - \langle 1, 2 \rangle \quad \text{dans } \text{GrW}(k).$$

Cette formule se simplifie si l'on écrit :

$$q_E = \langle 1, 2 \rangle \oplus Q \quad \text{et} \quad q_{E'} = \langle 1, 2 \rangle \oplus Q',$$

où Q et Q' sont des formes de rang 4, cf. n° 3.2 ; on obtient :

$$Q' = \lambda^3(Q) = \langle 2d \rangle \cdot Q, \quad \text{avec } d = \text{discr}(E) = \text{discr}(E').$$

Le cas particulier $d = 1$ avait été déjà obtenu dans le cours 1990/1991.

3.4. Formes trace de rang 6 ou 7 avec $w_1 = w_2 = 0$

Soit q une forme quadratique non dégénérée de rang 6 telle que $w_1(q) = w_2(q) = 0$.

On prouve en utilisant le critère du n° 3.2 :

(i) Pour que q soit une forme trace, il faut et il suffit qu'il existe $c \in k^*$ tel que :

$$(i_1) \quad q \approx \langle 1, 1, c, c, c, c \rangle.$$

(i₂) c est somme de 4 carrés dans $k(\sqrt{2})$.

(i₃) $(2)(c) = 0$ dans $H^2(k, \mathbb{Z}/2\mathbb{Z})$, i.e. c est représenté par la forme $\langle 1, -2 \rangle$.

D'après 3.1., il y a un énoncé analogue en rang 7 : dans (i₁) on remplace $\langle 1, 1, c, c, c, c \rangle$ par $\langle 1, 1, 1, c, c, c, c \rangle$.

Disons qu'un corps k a la propriété (0) si tout $c \in k^*$ satisfaisant à (i₂) et (i₃) est somme de 4 carrés dans k (ce qui équivaut à $\langle c, c, c, c \rangle$ isomorphe à $\langle 1, 1, 1, 1 \rangle$). D'après (i), cela revient à dire que toute forme trace q , de rang 6 ou 7 et telle que $w_1(q) = w_2(q) = 0$, est isomorphe à la forme unité $\langle 1, \dots, 1 \rangle$. On démontre :

(ii) Tout corps où -1 est somme de 2 carrés (par exemple tout corps de caractéristique > 0) a la propriété (0).

(iii) Toute extension transcendante pure d'un corps de nombres ou d'un corps local (à corps résiduel fini) a la propriété (0).

(iv) Il existe des corps n'ayant pas la propriété (0), par exemple le corps des fonctions sur \mathbb{Q} de la quadrique projective d'équation homogène :

$$7X_0^2 + X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2 = 0.$$

(Cela se voit en remarquant que $c = -1$ satisfait à (i₂) et (i₃), mais n'est pas somme de 4 carrés.)

L'exemple donné dans (iv) est de degré de transcendance 4 sur \mathbb{Q} . J'ignore s'il existe des exemples analogues de degré de transcendance 1, 2, ou 3.

3.5. Application au problème de Noether pour certains sous-groupes de $2.A_7$

Soit $2.A_7$ l'unique extension non triviale du groupe alterné A_7 par un groupe à 2 éléments. Une algèbre étale E de rang 7 est telle que $w_1(q_E) = w_2(q_E) = 0$ si et seulement si E est définie par un homomorphisme $\Gamma_k \rightarrow S_7$ qui se factorise en $\Gamma_k \rightarrow 2.A_7 \rightarrow A_7 \rightarrow S_7$. En utilisant les résultats du n° 3.4, on démontre :

(i) Soit G un sous-groupe d'indice impair de $2.A_7$ (par exemple $2.A_7$, $2.A_6$, $SL_2(\mathbb{F}_7)$ ou le groupe quaternionien Q_{16}). Soit L_G/K_G une G -extension galoisienne verselle en caractéristique 0. Alors K_G n'est pas une extension transcendante pure de \mathbb{Q} .

(En effet, soit $k = K_G$, et soit E la k -algèbre étale de rang 7 associée à $\Gamma_k \rightarrow \text{Gal}(L_G/k) = G \rightarrow 2.A_7 \rightarrow A_7 \rightarrow S_7$.

Si la forme trace de E était la forme unité $\langle 1, \dots, 1 \rangle$, il en serait de même (vu le caractère versel de L_G/k) pour toute algèbre étale de rang 7 provenant d'un G -torseur. Or l'exemple du n° 3.4. (iv), convenablement précisé, montre

que ce n'est pas toujours le cas. Il en résulte que k n'a pas la propriété (0). Vu le n° 3.4. (iii), ce n'est donc pas une extension transcendante pure de \mathbb{Q} .

En particulier :

(ii) Si l'on plonge G dans un groupe symétrique S_N , le corps des G -invariants de $\mathbb{Q}(T_1, \dots, T_N)$ n'est pas une extension transcendante pure de \mathbb{Q} .

En d'autres termes le problème de Noether a une solution négative pour G .

PUBLICATIONS

E. BAYER-FLUCKIGER et J.-P. SERRE, *Torsions quadratiques et bases normales autoduales*, Amer. J. of Math. 116 (1994), 1-63.

T. EKEDAHL et J.-P. SERRE, *Exemples de courbes algébriques à jacobienne complètement décomposable*, C.R. Acad. Sci. Paris 317 (1993), 509-513.

J.-P. SERRE, *Gèbres*, L'Enseignement Math. 39 (1993), 33-85.

—, *Smith, Minkowski et l'Académie des Sciences* (avec des notes de N. Schappacher), Gazette des Mathématiciens 56 (1993), 3-9 ; traduction allemande : D.M.V. Mitteilungen 2 (1993), 4-7.

—, *Sur la semi-simplicité des produits tensoriels de représentations de groupes*, Invent. math. 116 (1994), 513-530.

—, *A letter as an appendix to the square-root parameterization paper of Abhyankar*, in *Algebraic Geometry and Its Applications* (C.L. Bajaj edit.), 85-88, Springer-Verlag, 1994.

—, *Propriétés conjecturales des groupes de Galois motiviques et des représentations ℓ -adiques*, Proc. Symp. Pure Math. 55 (1994), vol. 1, 377-400.

ÉDITION

U. JANNSEN, S. KLEIMAN et J.-P. SERRE (édit.), *Motives*, A.M.S. Symposia Pure Math. 55 (1994), 2 vol., 1423 p.

MISSIONS

Exposés

- *Tensor products of semisimple representations*, Spetses, juillet 1993 ;
- *Negligible cohomology*, Spetses, juillet 1993 ;
- *Résultats préliminaires au théorème de Fermat-Wiles*, Bordeaux, septembre 1993 ;
- *Représentations linéaires sur les anneaux locaux, d'après Carayol*, Sémin. Chevalley, octobre 1993 ; Orsay, mai 1994 ;
- *Distribution asymptotique des valeurs propres d'opérateurs de Hecke*, Besançon, octobre 1993 ;
- *Asymptotic repartition of eigenvalues of Hecke operators*, Hong Kong, décembre 1993 ;
- *Exemples : $X_0(11)$ et $X_1(11)$* , Inst. H. Poincaré, janvier 1994 ;
- *Les conjectures de Duke (2 exposés)*, Inst. H. Poincaré, janvier 1994 ;
- *La stratégie de Wiles*, Inst. H. Poincaré, janvier 1994 ;
- *Cohomologie galoisienne : progrès et problèmes*, Sémin. Bourbaki, mars 1994 ;
- *Sous-groupes finis de $GL_n(\mathbf{Q}), \dots, E_8(\mathbf{Q})$* , Sémin. Chevalley, mars 1994 ;
- *Tensor products of group representations in characteristic p* , Berkeley, avril 1994 ;
- *Finite subgroups of exceptional Lie groups*, Berkeley, avril 1994 ;
- *Cohomological invariants of étale algebras*, Berkeley, mai 1994 ;
- *De S_4 dans SO_3 à $PGL_2(\mathbf{F}_{31})$ dans E_8* , Sémin. Chevalley, juin 1994 ;
- *λ -opérations et formes quadratiques*, Luminy, juin 1994 ;
- *Galois representations and Chebotarev's density theorem*, Amsterdam, juin 1994.

Table des Matières

Introduction : invariants cohomologiques	...	I-1
Cohomologie négligeable - Définitions	...	I-8
Propriétés formelles		I-10
Exemple mod 2 : $x^2y + xy^2$		I-14
Exemple mod p : $x \cdot \delta(x)$		I-15
Isomorphisme de Shapiro		II-1
La propriété de relèvement (Lur'e)		II-2
Exemples : $C_2 \times C_2, C_p, C_4$		II-4
G-torseurs versels		II-10
Critère de négligeabilité		II-16
$2x$ est négligeable, si $\dim \gg 0$		III-2
Corps de vcd $< \infty$		III-4
Reformulation du théorème		III-14
Fin de la démonstration		IV-1
Spectre de la cohomologie effective mod 2		IV-3
Exemples : C_2, C_4, S_4, D_4, Q_8		IV-4
$H^2(G, M)$ avec action triviale		IV-10
Le cas $G = C_p$		IV-12
Retour à Q_8		V-1
Invariants cohomologiques associés à des G-torseurs	...	V-3
Exemples : C_2, PGL_2, G_2		V-8
Parenthèse sur F_4		V-11
Le cas de PGL_2 : démonstration		V-12
Un procédé de construction d'invariants		V-17
Invariants à valeurs dans le groupe de Witt		VI-3
Invariants du groupe symétrique S_n	...	VI-7
Le dictionnaire : algèbres étales - toseurs		VI-7
Critères de nullité : th.1 et th.2		VI-9
Générateurs des algèbres étales		VI-15
Générateurs des algèbres étales (corps finis)		VII-1
Invariants des algèbres étales		VII-5
Généralisation : groupes de Weyl		VII-8
Calculs explicites		VII-9
" " (mod 2)		VII-11
" " (cas général)		VII-13

Invariants à valeurs dans le groupe de Witt	VII-15, VIII-6
Compléments	VIII-1
La forme trace	VIII-4
Le cas $n = 6$	VIII-8
Structure de la forme trace VIII-10
Pas de partie fixe	VIII-12
n impair, d'après Mestre	VIII-13
La caractéristique 2	IX-1
Le cas $n = 4$	IX-2
Le cas $n = 6$	IX-10
L'automorphisme externe de S_6	IX-13
Le cas $n = 6$, $w_1 = w_2 = 0$	X-2
La propriété O_6	X-7
Sous-groupes de $2.A_7$ d'indice impair : solution négative du problème de E.Noether	X-13
Fin du cours X-15

Invariants cohomologiques

On s'intéresse à des invariants cohom. attachés à des " G -torseurs", où G est un groupe algébrique (le + souvent fini).

Si G est un groupe alg. / une base S (Le + svt, $S = \text{spec } k$, k corps), un G -torseur est un espace principal homogène / à G , i.e. un schéma $P \rightarrow S$ avec une action de G tq après changement de base fidèle plat $S' \rightarrow S$ P devient isomorphe au toseur trivial, i.e. $\cong G$.

Cas particulier: $S = \text{spec}(k)$; G lisse sur k .

On peut prendre $S' = \text{spec}(k')$, et on peut imposer k' de degré fini et séparable / k . Alors P devient trivial sur $k' \iff P(k') \neq \emptyset$.

(Analogie en topologie: un fibré ppaf ayant une section devient trivial.)

Si non: On pourrait prendre k' fini, mais pas nécessairement séparable. Cf. $G = \mu_p$ en car p .

Exple: formes quadratiques ; $O(q)$.

k est un corps ; $\text{car } k \neq 2$.

q et q' sont deux f.q. non dég. de dim. n sur $\mathbb{P} =$ espace des isomorphismes entre q et q'
 X_1, \dots, X_n variables.

pts de \mathbb{P} : matrices $n \times n$ transformant q en q'
le groupe orthogonal de q $O(q)$ agit sur \mathbb{P} et en fait un espace principal homogène.

A q fixé: on a ainsi:

classes de f.q. q' de n rg q \sim classes de $O(q)$ torseurs.
(i.e. non dég. de dim. n)

Il est bien connu que c'est bijectif.

Autre exple: G gpe fini.

G peut être vu cō un gpe alg. de dim. 0 , et dt tous les pts sont rationnels.

Soit k_s une clôture sēp. de k et $\Gamma_k = \text{Gal}(k_s/k)$

Il y a bijection entre :

- ① les G -torseurs sur k
 - ② les hom. continus $\Gamma_k \rightarrow G$, à conj. près.
 - ③ les G -alg. gal. sur k .
- en prenant l'algèbre affine.

(N.B. : continus = à noyau ouvert.)

Cas particulier:

qd $G = S_n$, gpe sym. en n lettres,
① ② et ③ st en bijections avec
④ les k alg. étates de rang n sur k .
(les alg. st commutatives, à 1 et unité).

Par pouvoir classifier ces objets,
il faut avoir des invariants calculables.

les classes de
 G -torseurs $\iff H^1(\Gamma_n, G(k_s))$
(G lisse / k) $\iff H^1(k, G)$.

(si G est non lisse, il faut prendre $H^1_{\text{ét}}$)

Ici: on aura tjrs G lisse / k .

Rappel: si Γ est un Γ_n module, avec
les hyp. habituelles (stabilisateur de
tout point ouvert), on notera
 $H^q(k, \Gamma) := H^q(\Gamma_n, \Gamma)$.

C'est dans ces gpes q'on va généralement
trouver des invariants.

Inv. cobom.

Ce st de des applications
 $H^1(k, G) \longrightarrow H^q(k, \Gamma)$
 G -torseurs

$E \rightarrow g \text{ ad } E$, Γ est assez petit.
p.ex.; $\Gamma = \mathbb{Z}/n\mathbb{Z}$, ou $M_n^{\oplus i}$.

Exple: cas des f.q.; $\text{car } k \neq 2$.
 $G = O(q)$; q de rang n .

O . a : cl. de f.q. de rang n $\xrightarrow{\chi_q} H^4(k, \mathbb{Z}/2\mathbb{Z})$

autre exple: $\text{car } k \neq 2$.

$G = U_2$ (déployé).

$H^1(k, U_2) \xrightarrow{\quad} H^3(k, \mathbb{Z}/2\mathbb{Z})$
 \updownarrow
classes d'octonions/ k

On note $O_{\alpha, \beta, \gamma}$ l'alg. déf. par
 $(1, e_1, \dots, e_7)$ $e_1^2 = \alpha \in k^*$; $e_2^2 = \beta$; $e_3^2 = \gamma$;
 $e_4 = e_1 e_2 = -e_2 e_1, \dots$

Alors $O_{\alpha, \beta, \gamma} \mapsto (\alpha)(\beta)(\gamma)$
(cup produit)

où on note (α) l'élément de $H^1(k, \mathbb{Z}/2\mathbb{Z})$
correspondant à $\alpha \in k^*/k^{*2}$.

Ici: L'invariant caractérise la
classe d'octonions; l'image est
constituée des $\mathbb{Z}e_1^2$ décomposables.

(Mais ds la pratique, il est difficile
de déterminer les $\mathbb{Z}e_1^2$ décomposables).

Pb: $k = \mathbb{Q}_p(T)$. Tout élé du H^3 est-il décomposable? (pour \mathbb{R} , c'est vrai).

Cet exple sert de modèle, mais n'est pas réalisable partout.

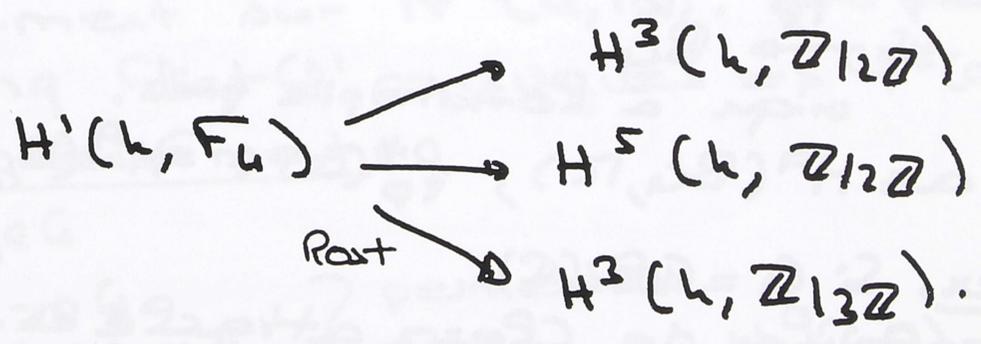
Cas des f.q.: conj. de Nielsen.

q et q' m rang; on suppose q, q' elles ont m \mathbb{N}_1 et \mathbb{N}_2 .

On peut associer au couple (q, q') un invariant dans H^3 . Si il est nul, $(q, q') \rightarrow H^4$.

Les conj. disent que si tous ces inv. relatifs st nuls, jusqu'à un rang "assez gd", alors $q \cong q'$.

(conj. de Nielsen: $gr \mathbb{N} \cong H^*(k, \mathbb{Z}/2\mathbb{Z})$.)



Il se peut que ces 3 inv. suffisent à caractériser les élém^s de $H^1(k, F_4)$. Par contre, on ne connaît vraiment pas l'image.

Cas intéressant: Si G est un gpe semi-simple, simplement connexe.

De ce cas, il semble qu'il n'y a pas d'invariants non triviaux de H^1 et H^2 .
Par contre, on en a dans $H^3(k, M_p^{\otimes 2})$
où p est un nombre premier de torsion.

P.ex. $H^1(k, E_p) \rightarrow H^3(k, M_5^{\otimes 2})$.

On ne pourra pas trop parler de ces cas généraux, mais plutôt de certains cas particuliers intéressants.

Analogie avec la topologie:

P fibré ppaf de gpe G , de base S ,
obtenu à partir d'un fibré universel:

$$\begin{array}{ccc} & E_G & \\ & \downarrow & G \\ S & \xrightarrow{f_P} & B_G \end{array}$$

unique à homotopie près.

Si $a \in H^q(B_G, \mathbb{Z})$, $f_P^*(a) \in H^q(S, \mathbb{Z})$.

P.ex. Si $G = GL_n(\mathbb{C})$

↳ classes de Chern attachées à un fibré ppaf.

Ceci permet de construire des invariants sur une base qcqz.

Rais:

- ① Par restriction au cas d'un corps, un inv. non nul peut donner un inv. nul.
- ② Il existe des inv. sur les corps qui ne proviennent pas d'inv. sur une base qcqz.

Le début du cours va être consacré à une fabrication d'inv. de type ① "théorie des classes de colon. négligeables".

Ds le cas où G est fini,
 $H^1(k, G) \rightarrow$ classes de conj. d'hom. continus $\Gamma_k \rightarrow G$.

Alors si on choisit un G -module \mathbb{Z} , un entier $q \geq 0$, et un $\mathbb{Z}G$ - $a \in H^q(G, \mathbb{Z})$,
 $\forall \varphi: \Gamma_k \rightarrow G \quad \varphi^*(a) \in H^q(k, \mathbb{Z})$.

On obtient ainsi une flèche
 $H^1(k, G) \rightarrow H^q(k, \mathbb{Z})$.

Rq: Les aut. int. de G opèrent trivialement sur $H^q(G, \mathbb{Z})$. (\rightarrow permet de mg φ et φ' conjugués $\Rightarrow \varphi^*(a) = \varphi'^*(a)$).

précisément:

$g \in G$

$G \rightarrow G$

$x \mapsto g \cdot x \cdot g^{-1}$

$\Gamma \rightarrow \Gamma$

$m \mapsto g \cdot m$

} permettent de définir

$H^q(G, \mathbb{Z}) \rightarrow H^q(G, \mathbb{Z})$



cette flèche est id.

Def: a est nég. (pour la colon. galoisienne) si $\varphi^*(a) = 0$ pour tout corp. k et $\forall \varphi: \Gamma_k \rightarrow G$.

Etude plus systématique des classes de colon. négligeables.

(p.ex., G cyclique d'ordre $g \rightarrow ???$).

Désormais, G est un gpe fini donné.

Γ est un G -module ($e + \text{aut}$, Γ fini).

$q \geq 1$; $a \in H^q(G, \Gamma)$.

k corps; $\Gamma_k = \text{Gal}(k_s/k)$.

Def.: a est k -négligeable si $\varphi^*(a) = 0$ pour $\forall \varphi: \Gamma_k \rightarrow G$ continu.

X est une catégorie de corps.

Def.: a est X -négligeable si a est k -nég. pour tout $k \in X$.

Def.: a est négligeable si il est X nég. pour $X = \text{tous les corps}$.

Ceci permettra de regarder p.ex. le cas des corps de car $\neq 0$, ou des corps $> \Gamma-1$ etc.

R.B.: Bogomolov | X cat. des corp. $> \text{un.}$
Saltman | corps alg. clos.

cf. aussi Lure (1991).

Prop.: si a est neg. a caro, alors a est neg.

Dém.: Soit k , $\text{car } k = p$.

On choisit un corps local K , de corps résiduel k , avec $\text{car } K = 0$.

Théorie des ramifications (corps locaux):

$$\Gamma_K \xrightarrow{\pi} \Gamma \rightarrow 1.$$

On sait aussi (cf. cours précédents) que cette flèche est scindée, i.e.

il y a un morphisme $\varepsilon: \Gamma \rightarrow \Gamma_K$ tq $\pi \circ \varepsilon = \text{id}$.

Donc $H^q(\Gamma, \mathbb{Z}) \hookrightarrow H^q(\Gamma_K, \mathbb{Z})$
 $\forall (q, \mathbb{Z})$.

Soit alors $a \in H^q(\Gamma, \mathbb{Z})$; $\varphi: \Gamma \rightarrow G$.

mg $\varphi^*(a) \in H^q(\Gamma, \mathbb{Z})$.

Mais $\pi^* \circ \varphi^*(a) \in H^q(\Gamma_K, \mathbb{Z})$

(car a neg. en $\text{car } 0$, et $\varphi \circ \pi: \Gamma_K \rightarrow G$).

L'injectivité de $H^q(\Gamma, \mathbb{Z}) \xrightarrow{\pi^*} H^q(\Gamma_K, \mathbb{Z})$ permet alors de conclure.

□.

N.B.: La "réciproque" est fautive:

exple de classe b } non neg. en $\text{car } 0$
"minimale" } neg. en $\text{toute car } p > 0$

On prend $G = \mathbb{Z}/2\mathbb{Z}$.

Pour ce gpe, seule $a=0$ est neg.,

car $G = \text{Gal}(\mathbb{C}/\mathbb{R}) = \Gamma_{\mathbb{R}}$.

$a \neq 0$

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

$$\varphi^*(a) \in H^2(h, \mathbb{Z}/2\mathbb{Z}) = B\Gamma_2(h).$$

$$\text{Puis } \varphi: \Gamma_h \rightarrow G = \mathbb{Z}/2\mathbb{Z}$$

$$\begin{array}{c} \updownarrow \\ \alpha \in h^0/h^2 \quad (\alpha) \in H^1(h, \mathbb{Z}/2\mathbb{Z}). \end{array}$$

$$\text{Ainsi } \varphi^*(a) = (-1)(\alpha).$$

($\Rightarrow a$ neg. en corp p qd $p \equiv 1 \pmod{4}$).

Demⁿ b est non nul dans $H^3(G, \mathbb{Z}/2\mathbb{Z})$

$$\varphi^*(b) = (-1)(\alpha)(\alpha) = \underbrace{(-1)(-1)}_{\text{quaternions usuels}}(\alpha) = 0.$$

quaternions usuels
décomposés en corp p .

N.B.: On pourra donc dorénavant
supposer $\text{car } h = 0$.

Propriétés formelles

Notat^o: $H_n^q(G, \mathbb{Z}) = \text{sgpe de } H^q(G, \mathbb{Z}) \text{ formé des } \mathbb{Z}\text{-etats négatifs}$.

$$H_n^q(G, \mathbb{Z}) = H^q(G, \mathbb{Z}) / H_n^q(G, \mathbb{Z}).$$

1) $\Gamma \rightarrow \Gamma' \quad G\text{-modules}$
$$H_n^q(G, \mathbb{Z}) \rightarrow H_n^q(G, \mathbb{Z}').$$

2) $0 \rightarrow \Gamma \rightarrow \Gamma' \rightarrow \Gamma'' \rightarrow 0$
$$\delta: H_n^q(G, \mathbb{Z}'') \rightarrow H^{q+1}(G, \mathbb{Z})$$

envoie $H_n^q(G, \mathbb{Z}'') \rightarrow H_n^{q+1}(G, \mathbb{Z})$.

ou encore, on a

$H_e^q(G, \mathbb{Z}) \rightarrow H_e^q(G, \mathbb{Z}') \rightarrow H_e^q(G, \mathbb{Z}'') \xrightarrow{\delta} H_e^{q+1}(G, \mathbb{Z})$
 Cette suite est incomplète, mais n'est pas exacte en $q=1$.

Prop.: $\boxed{\text{Si } q=0 \text{ ou } 1, H_n^q(G, \mathbb{Z})=0.}$

En effet, on sait que $\pi_1 G$ est qpe de Galois d'une extension L/K .

[ex. car $G \subset \text{Cos } \pi$
 ou par les corps de nombres].

$\varphi: \Gamma_K \rightarrow G, \varphi$ surjectif.

Alors $H^q(G, \mathbb{Z}) \rightarrow H^q(\Gamma_K, \mathbb{Z})$

\uparrow
 $\left. \begin{array}{l} \text{bij. pour } q=0 \\ \text{inj. pour } q=1. \end{array} \right\}$

Prop.: $\boxed{q=2}$ Si Γ est fini, et l'act^o de G triviale, alors $H_n^2(G, \mathbb{Z})=0$.

(La dém. sera donnée ultérieurement).

Par contre: \exists des Γ à act^o non triviale, avec $H_n^2(G, \mathbb{Z}) \neq 0$.

exple: $G = C_3$ cyclique d'ordre 3.

\mathbb{Z} -v. de dim 2 sur \mathbb{F}_3 .

Act^o d'un gén. de G donnée par $\begin{pmatrix} 1 & \\ & \omega \end{pmatrix}$.

On vérifie que $H^2(G, \mathbb{Z}) = \mathbb{Z}/3\mathbb{Z}$ est entièrement négligeable.

(cf. article de Lure).

Prop: Soit $G' \subset G$ et Γ un G module.
 Res: $H^q(G, \Gamma) \rightarrow H^q(G', \Gamma)$
 applique H^n dans H^n .

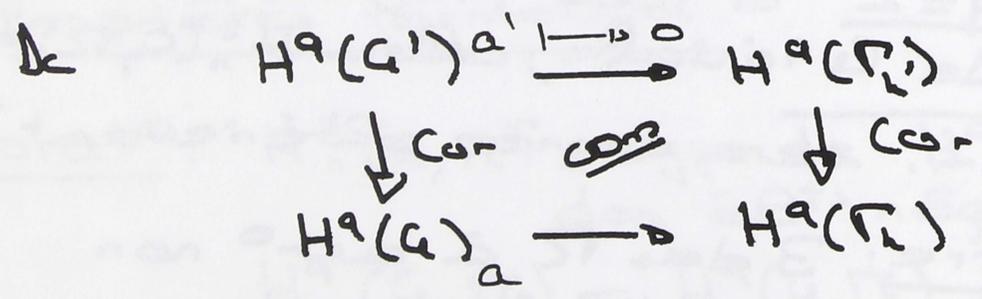
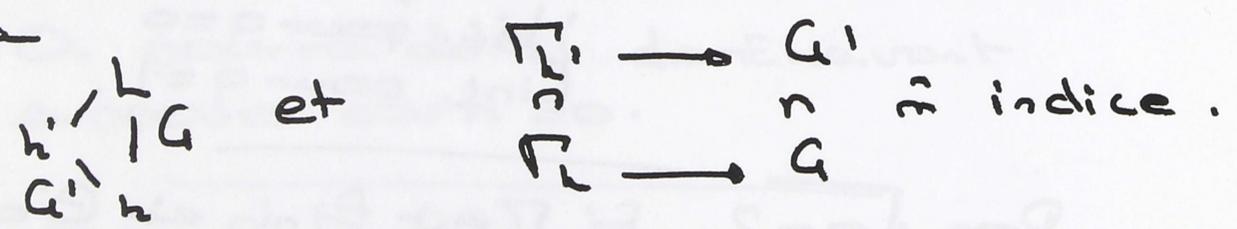
En effet: $a \in H^q(G, \Gamma)$; $a' = \text{Res } a$
 $\Gamma_h \rightarrow G' \rightarrow G$
 $\quad \quad \quad a' \quad \quad \quad a$

Prop: Cor: $H^q(G', \Gamma) \rightarrow H^q(G, \Gamma)$
 $\quad \quad \quad a' \quad \quad \quad a = \text{Cor}(a')$
 Alors a' nég. $\Rightarrow a$ nég.

Dém: c'est un peu moins évident.
 deux tps:

① Cas particulier: $\varphi: \Gamma_h \rightarrow G$ est surj.

On a



ce diagramme permet de conclure.

② Cas gale: Dx méthodes possibles.

1^{er} méthode: on utilise le lemme suivant

Lemme: Si a est tq $\varphi^*(a) = 0$ pour tout φ surjectif, alors a est nég.

2^{de} méthode: On reprend la dem. précédente.

$$\Gamma \xrightarrow{\varphi} G$$

Γ opère sur G/G' grâce à φ . ("cuisine à la Pachey").

On prend un syst. de rep. g_x des orbites de Γ dans G/G' .

Γ_{h_x} le fixateur dans Γ de g_x

$$\text{on a } \begin{matrix} \Gamma_{h_x} & \xrightarrow{\varphi_x} & G' \\ \times & \mapsto & g_x^{-1} \times g_x \in G' \end{matrix}$$

$$\varphi^* \text{Cor}_{G'}^G a' = \sum_x \text{Cor}_{\Gamma_{h_x}}^{\Gamma} \varphi_x^* a'$$

Puis a' nég. \Rightarrow les $\varphi_x^* a'$ sont nuls.

On va maintenant donner qqes ex. de classes de colon. nég.

Pour certains gpe, il y en a bcp.

On démontrera

Thm: Si $G = S_n$, et Γ un gpe ab. fini, d'ordre impair, sur lequel G opère trivialement, alors H^1 est de $H^q(G, \mathbb{Z})$, $q > 0$ est nég.

("pas d'inv. colon. d'ordre impair non triviaux pour le gpe S_n ").

On montrera aussi

Thm: $\boxed{\text{Si } |G| > 2, \exists \text{ des } q, \pi \text{ et } a \in H^q(G, \pi) a \neq 0 \text{ tq } a \text{ n'ég.}}$

Pb: peut-on prendre $q=2$?
C'est vrai si $|G|$ est impair.

Soit de G un gpe fini qcqr, et x et $y \in H^1(G, \mathbb{Z}/2\mathbb{Z})$ ($\pi = \mathbb{Z}/2\mathbb{Z}$).

On prend $q=3$ et $a = x^2y + xy^2 \in H^3(G, \mathbb{Z}/2\mathbb{Z})$.

Alors a est négligeable

Preuve: k ; $\text{car } k \neq 2$.

$$H^1(k, \mathbb{Z}/2\mathbb{Z}) \cong k^*/k^{*2}$$

$$\varphi: \Gamma_k \rightarrow G.$$

φ^*x et φ^*y s'écrivent (κ) et (ρ) .

Alors

$$\varphi^*(a) = (\kappa)(\kappa)(\rho) + (\kappa)(\rho)(\rho) = (-1)(\kappa)(\rho) + (-1)(\kappa)(\rho) = 0 \text{ (on travaille modulo 2).}$$

Exercice: Si $x \in H^1(G)$ et $y \in H^2(G)$

mq $(y+x^2)(xy) \in H^4(G)$ est négl.

(Utiliser le thm de Serre sur H^2 :

H^2 est cog. par les élts déc.,

i.e. tt élts de H^2 s'écrit $\sum (\kappa_i)(\rho_i)$.

Exemple modulo p : p premier $\neq 2$.

G gpe qcqr, $\mathbb{Z} = \mathbb{Z}/p\mathbb{Z}$.

$x \in H^1(G, \mathbb{Z}) = \text{Hom}(G, \mathbb{Z}/p\mathbb{Z})$.

$0 \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p^2\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow 0$ induit

$u \delta : H^1(G, \mathbb{Z}) \rightarrow H^2(G, \mathbb{Z})$ (Bernstein).

Alors $x \delta(x)$ est nég.

Preuve:

$G \rightarrow C_p$ gpe cyclique d'ordre p .

De ops de la dém. que G est cyclique d'ordre p .

Soit h ; car $h \neq p$.

On peut aussi supposer $h \geq 3$
racine primitive p -ième de 1.

$\left(\begin{array}{l} h(p) \\ h \end{array} \right)$ de et a div. de $p-1$,
de 1 à p .
D'où coh. \hookrightarrow coh. ...

Théorie de Kummer :

$\varphi: \Gamma_h \rightarrow G$; $\varphi^* x \in H^1(h, \mathbb{Z}/p\mathbb{Z})$

$$H^1(h, \mu_p) \cong h^* / h^{*p}$$

$(\alpha) \longleftarrow \varphi^* x$

$$\varphi^*(x) = (\alpha)$$

$$\delta x = -(\varphi)(\alpha).$$

$$\text{De } \varphi^*(x \delta x) = \underbrace{(\alpha)(\alpha)}_{=0}(\varphi) = 0$$

La donne un exple de classe nég. de H^2 d'un gpe cyclique.

En fait, on montrera que si Γ est un C_p -mod fini qcqr, $\forall \alpha \in H^q(G, \mathbb{Z})$ est nég.
 $q \geq 3$

On va commencer par exposer deux conséquences des propriétés formelles:

1) Soit G fini - \mathbb{Z} un G -module.

On suppose que $a \in H^q(G, \mathbb{Z})$ est d'ordre une puissance de p , i.e. $a \in H^q(G, \mathbb{Z})_{(p)}$ (composante p primaire).

Alors si S est un p -Sylow de G , on a :

a est nég. \iff $\text{Res}_S^G(a)$ est nég.

(preuve : on s'en a déjà été vu).

Dans l'autre, on applique la corestriction, et on utilise $\text{Cor. Res} = \text{indice}$.

Anc : Dans $H^1(G, \mathbb{Z}/2\mathbb{Z})$ on pourra regarder simplement la restriction à un 2-Sylow i.e. $H^1(G, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^1(S, \mathbb{Z}/2\mathbb{Z})$.

Si de plus S est abélien, notons N le normalisateur de S ds G et $N = N/S$. il suffit de regarder

$$H^1(G, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^1(S, \mathbb{Z}/2\mathbb{Z})^N.$$

2) LEM de Shapiro :

Soit G fini, H un sous-groupe de G , et \mathbb{Z} un H -module. $\text{Ind}_H^G \mathbb{Z} = \mathbb{Z}^*$ G -mod. induit.

(\mathbb{Z}^* est de \mathbb{Z}^* peut être vu comme $f: G \rightarrow \mathbb{Z}$ tq $f(hx) = h \cdot f(x) \forall h \in H$ et $g \cdot f(x) := f(xg) \forall g \in G$).

On a alors

Lemme de Shapiro

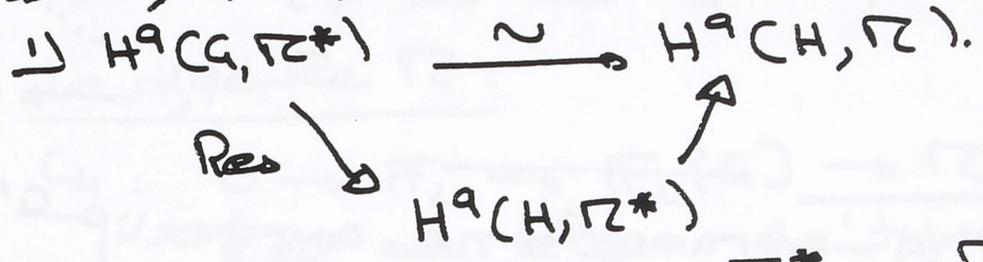
$$\boxed{\text{(Faddeu)} \quad H^q(G, \mathbb{Z}^*) \simeq H^q(H, \mathbb{Z})}$$

$$a^* \longleftarrow a.$$

Alors les classes nég. sat les \hat{m} .

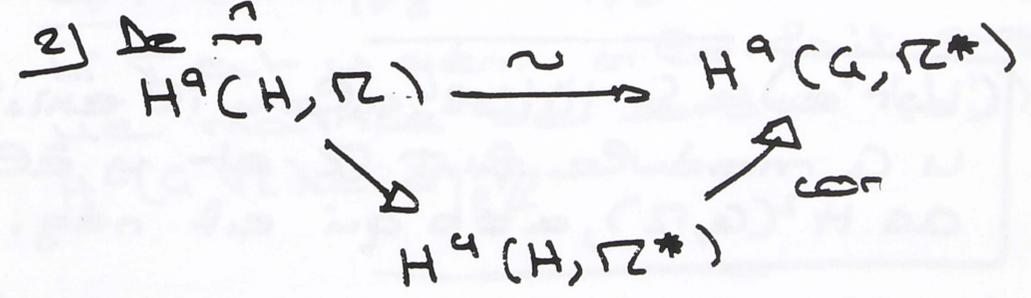
i.e. $a \text{ nég.} \iff a^* \text{ nég.}$

En effet: pour démontrer Shapiro, on fabrique des flèches dans les deux sens, qui font intervenir Res et Cor.

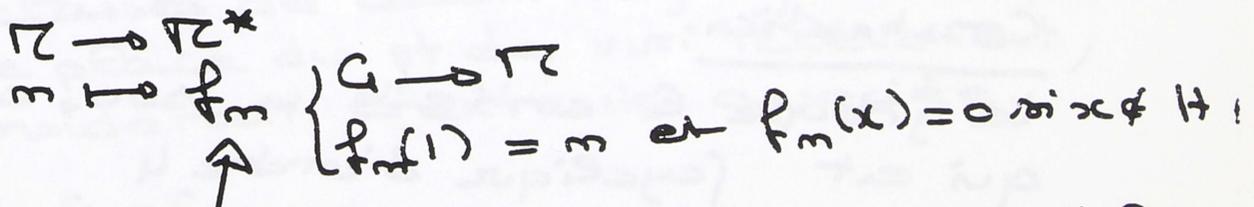


(on a un H morphisme $\begin{matrix} \mathbb{Z}^* \rightarrow \mathbb{Z} \\ f \mapsto f(1) \end{matrix}$)

Grâce aux prop. formelles vues la semaine dernière, on a alors $a^* \text{ nég.} \implies a \text{ nég.}$



(On a un G morphisme



Une telle $f_m \exists$, et !, et est compatible avec l'act° de H . capit

Paintraut, on va suivre l'article de B.B. Lurie "On universally solvable embedding problems" Proc. st. 183 (1990). Trad. ang. 199.

Soit $a \in H^2(G, \mathbb{Z})$, avec \mathbb{Z} fini.

Concrètement, qu signifie a négligeable?

a déf. une extension

$$1 \rightarrow \mathbb{Z} \rightarrow E_a \rightarrow G \rightarrow 1.$$

a nég. $\Leftrightarrow \forall h; \forall \varphi: \Gamma_h \rightarrow G$ continu,

φ se relève en $\Gamma_h \rightarrow E_a$

$$\begin{array}{ccc} & & E_a \\ & \dots & \downarrow \\ \Gamma_h & \rightarrow & G \end{array}$$

On dit qu'un morphisme surjectif $G' \rightarrow G$ a la propriété de relèvement si $\forall \varphi: \Gamma_h \rightarrow G$ se relève à G' .

Cette notion de relèvement explique bien les classes de cohomologie négligeables.

Thm (Lur'e) : Si $|G| > 2$, alors il existe un G module fini \mathbb{Z} , et un $a \in H^2(G, \mathbb{Z})$, $a \neq 0$ qui est nég.

(N.B.: on est revenu au cas commutatif).

Construction:

Le groupe G contient un sous groupe H

qui est $\begin{cases} \text{cyclique d'ordre 4} & C_4 \\ \text{ou ab. élém. de type (2,2)} & C_2 \times C_2 \\ \text{ou cyclique d'ordre } p \text{ premier } p \neq 2 & C_p \end{cases}$

Grâce aux résultats précédents, il suffira de démontrer le thm quand G est de l'un de ces 3 types.

Dans chacun de ces cas, on va trouver

$$1 \rightarrow \mathbb{Z} \xrightarrow{\text{ab}} G' \rightarrow G \rightarrow 1.$$

↑
L'ordre de G' sera
 $\begin{cases} 32 \text{ ds les 2}^{\text{es}} \text{ cas} \\ p^3 \text{ ds le } 3^{\text{eme}}. \end{cases}$

Le module \mathbb{Z} :

$$C_4: 0 \rightarrow \mathbb{F}_2 \rightarrow \mathbb{F}_2[G] \rightarrow \mathbb{Z} \rightarrow 0$$

\mathbb{Z} est ab. élen. de type $(2,2,2)$
 Act⁰ d'un gén. $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$

$C_2 \times C_2$: m^e construction.

Dans ces deux cas, $H^2(G, \mathbb{Z}) \cong H^3(G, \mathbb{Z}/2\mathbb{Z})$.

$$C_p: \mathbb{Z} = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

Si σ est un gén., on le fait agir par une matrice de Jordan $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

$$H^2(G, \mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}.$$

Plutôt que de construire directement des classes de cocycl. négligeables, on se place du pt de vue rétroactif, et considère l'extension associée.

$$\textcircled{1} \underline{G = C_2 \times C_2}$$

On se donne $\mathbb{F}_k \rightarrow G$, i.e. une G alg. gal. ops $p \neq 2$.

On introduit une k alg. com.

$$L_{\alpha, \beta} := k[x, y] / (x^2 - \alpha)(y^2 - \beta).$$

$L_{\alpha, \beta}$ est étale de $\text{rg } 4$ sur k .

un gén. agit par $\begin{cases} x \rightarrow -x \\ y \rightarrow y \end{cases}$ et l'autre $\begin{cases} x \rightarrow x \\ y \rightarrow -y \end{cases}$.

On cherche à écrire

$$\begin{matrix} L' \\ | \\ L \end{matrix} \subset G' \quad \text{i.e.} \quad L' = L_{\alpha, \beta} [Z, T, U] \quad (Z^2+1, T^2-X, U^2)$$

$$\text{rg}(L/L) = 4; \quad \text{rg}(L'/L) = 32$$

On fait de L' un alg. gal., en définissant les aut. suivant:

$$\sigma_1: \begin{cases} \sqrt[4]{x} \rightarrow i\sqrt[4]{x} \\ i \rightarrow i \\ \sqrt[4]{\beta} \rightarrow \sqrt[4]{\beta} \end{cases} \quad \text{i.e.} \quad \begin{cases} T \rightarrow ZT \\ Z \rightarrow Z \\ U \rightarrow U \end{cases}$$

On définit aussi σ_2 .

On a ainsi un $G' \xrightarrow{1} \Gamma \rightarrow G' \rightarrow G \rightarrow 1$.

Γ est de type $(2, 2, 2)$.

Il faut vérifier:

- que G' ne dépend pas de h
- Γ est un G module et bien celui qui a vu
- l'extension $G' \rightarrow G$ est non triviale.

La classe de cohomologie correspondante est la suivante: $u \in H^2(G, \Gamma)$

$$\text{tg} \quad H^2(G, \Gamma) \xrightarrow{\cong} H^3(G, \mathbb{Z}/2\mathbb{Z})$$

$$U \longmapsto U_2$$

G est ab. de type $(2, 2)$

$$H^*(G, \mathbb{Z}/2\mathbb{Z}) = \mathbb{F}_2[A, B] \quad A, B \text{ base de } H^1.$$

H^3 a comme base A^3, A^2B, AB^2, B^3 .

Alors U_2 est déf. par $U_2 = AB(A+B) = A^2B + AB^2$

↑
On a déjà vu que cet él⁺ est bien négligeable.

② $G = C_p$, p premier $p \neq 2$.

h corps ; car $h \neq \mathbb{F}_p$.

On suppose $\zeta \in h^*$ racine primitive p -ième de l'unité.

On va exhiber un gpc $G' \cong C_3$
 \downarrow
 $G \cong C_p$
 on veut mq il a la propriété de rélevement.

Rais:

① si $\text{car } h = p$, $\dim \text{cor. cd}_p(h) \leq 1$.
 de tte pièce se relève.

② si $\zeta \in h$ $h' = h(\zeta)$, do $|h'| = |h|^{p-1}$,
 $|h|$ i.e. d'o' premier à p .

Alors si la prop. de rélevement est vraie pour h' , on a $\Gamma_{h'} \subset \Gamma_h$
 indice premier à p

$u \in H^2(G, \mathbb{F}_p)$.

On sait que $\varphi^*(u)|_{\Gamma_{h'}} = 0$.

Comme indice $\lambda p = 1$, on a bien $\varphi^*(u) = 0$.

Donc on a bien le droit de faire ces deux hypothèses sur le corps h .

Soit $\varphi: \Gamma_h \rightarrow C_p$.

\downarrow

C_p alg. gal. L .

$L = h(\sqrt[p]{\alpha})$ $\alpha \in h^*$, i.e. $L = h[x] / (x^p - \alpha)$.

$\sigma: x \rightarrow \zeta x$.

On pose $L' = h(\sqrt[p]{\zeta}, \sqrt[p]{\alpha})$,

i.e. $L' = L[y, z] / (y^p - \zeta)(z^p - \alpha)$.

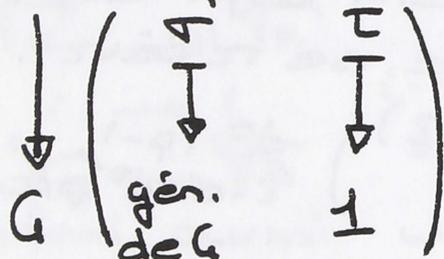
L' est de $q \mid p^3$.

Soit G' le sous-groupe de $\text{Aut}(L')$ agissant

$$\text{par } \sigma: \begin{cases} x \mapsto \zeta x \\ z \mapsto \zeta z \\ y \mapsto y \end{cases} \text{ et } \tau: \begin{cases} x \mapsto x \\ z \mapsto z \\ y \mapsto \zeta y. \end{cases}$$

On voit facilement $\sigma^p = 1, \tau^p = 1$
 et $\tau \sigma \tau^{-1} = \sigma^{1+p}$ à vérifier

De $G' = C_{p^2} \cdot C_p$ (produit semi direct)



G' est bien une extension non triviale de G .

Est négligeable correspond:
 de type (p, p) avec $\text{act}^0 (0!)$

$$H^2(G, \mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$$

Ceci donne d'autres exts négligeables.

Résultat: Soit $\mathbb{Z} \subset \mathbb{F}_p[G]$ mod., $G = C_p$,
 indécomposable, de dim i
 $1 \leq i \leq p$ (\rightarrow forme de Jordan
 de dim i).

$$H^2(G, \mathbb{Z}) = \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{si } 1 \leq i \leq p-1 \\ 0 & \text{si } i = p. \end{cases}$$

$$\text{Si } i = 1 \quad H_n^2(G, \mathbb{Z}) = 0$$

$$\text{Si } 2 \leq i \leq p-1 \quad H_n^2(G, \mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$$

Ce que l'on veut de faire démontrer
 qu pour $i=2$ $H^2(G, \mathbb{Z})$ est nég.

Or si $\text{rg}(\mathbb{Z}) > 2$, $\mathbb{Z} \supset \mathbb{Z}_2$ tq $H_2(G, \mathbb{Z}_2) \cong H_2(G, \mathbb{Z})$

On a ainsi décrit complètement
 les $\mathbb{Z} \oplus \mathbb{Z}$ nég. pour les $\mathbb{F}_p[G]$ mod.
 $d_2 H^2$.

③ $G = C_4$: ops $\text{car } h \neq 2$

Pour construire un ext. gal. de
 type C_4 :

$$h(\sqrt{a+b\sqrt{\varepsilon}})$$

$$|$$

$$h(\sqrt{\varepsilon})$$

$$|$$

$$|$$

$$h$$

$$\varepsilon \in h^*$$

$$\text{avec } a^2 - \varepsilon b^2 = \varepsilon c^2$$

$$\text{i.e. } \varepsilon = \pm 1$$

(somme de dx carrés,
 car les \mathbb{Z} forment
 un gpc).

$$x = \sqrt{a+b\sqrt{\varepsilon}} \quad \sqrt{x} = \frac{c\sqrt{\varepsilon}}{x} = x'$$

$$\text{car } \sqrt{(a+b\sqrt{\varepsilon})(a-b\sqrt{\varepsilon})} = c\sqrt{\varepsilon}$$

Si $h \neq \infty$, on peut imposer $\varepsilon, a, b, c \neq 0$.

Maintenant, on pose:

$$L = h(\sqrt{\varepsilon}, \sqrt{a+b\sqrt{\varepsilon}}) = h(x)$$

$$L' = L(i, \sqrt{x}, \sqrt{x'}) \quad \text{rg } 3/2$$

Les aut. de L' sont définies ainsi:

$$\left\{ \begin{array}{l} \sqrt{x} \rightarrow \sqrt{x'} \\ \sqrt{\varepsilon} \rightarrow -\sqrt{\varepsilon} \\ \sqrt{x'} \rightarrow ? \text{ (faire le calcul)} \end{array} \right\} \rightarrow \sigma \text{ d'ordre } 8$$

Soit un certain gpc G' aut. triviaux:

$$\left\{ \begin{array}{l} \text{id. sur } L \\ i, \sqrt{x}, \sqrt{x'} \rightarrow \pm i, \pm \sqrt{x}, \pm \sqrt{x'} \end{array} \right.$$

$$1 \rightarrow \mathbb{Z} \rightarrow G' \rightarrow G \rightarrow 1$$

\uparrow de type (2,2,2). mod. d'augmentation.

On peut vérifier que l'extension n'est pas triviale. $0 \rightarrow \mathbb{F}_2 \rightarrow \mathbb{F}_2[G] \rightarrow \mathbb{Z} \rightarrow 0$.

$$\delta : H^2(G, \mathbb{Z}) \rightarrow H^3(G, \mathbb{F}_2) \cong \mathbb{Z}/2\mathbb{Z}$$

D'où $H^3(G, \mathbb{F}_2)$ est négligeable.

Cyclique d'ordre 4.

$$H^q(C_4, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$$

$q = 0$) veut dire nég.

1) nég.

2) veut dire 0

3) nég. (cup produit...)

... $q \geq 3$ } q impair nég.
 q pair non nég. (restriction à un sous-groupe d'ordre 2).

On a:

Sait $G' \rightarrow G$ prop. de relèvement.
 \mathbb{Z} G -module.

Alors $\text{Ker}(H^q(G, \mathbb{Z}) \rightarrow H^q(G', \mathbb{Z}))$
 est un sous-groupe de $H^q(G, \mathbb{Z})$.

En effet si $\psi: \mathbb{Z} \rightarrow G$, $\begin{matrix} \psi' \nearrow G' \\ \mathbb{Z} \xrightarrow{\psi} G \\ \downarrow \end{matrix}$

ceci est trivial.

Ce qui est plus surprenant, c'est qu'on a une réciproque.

Prm: Si \mathbb{Z} est un G module, et $a \in H_n^q(G, \mathbb{Z})$, alors il existe G' ayant la
 \downarrow propriété de
 G relèvement
 et $a \in \ker(H^q(G, \mathbb{Z}) \rightarrow H^q(G', \mathbb{Z}))$.

(La dém. sera vue un peu plus tard. C'est une conséquence directe de l'existence des G -torsions universelles.)

(Qd $q > 2$ $G' \rightarrow G$ n'aura pas, en général, un noyau abélien.)

On va maintenant parler de G -torsions universelles.

(univ. = universelle - un.)

ex. : G ordre 2 en char 0

$\mathbb{Q}(T^{1/2})$

|) ext. quad.

$\mathbb{Q}(T)$

Si h est un corps quelconque, car $h = 0$, et h' une ext. quad. de h , alors on a

$h' = h(t)$, $t \in h^*$. De h'/h est obtenu

par spécialisation par rapport au cas précédent.

mais il n'y a pas utilité de t

La pas universelle.)

On prend pour G un schéma en groupe lisse sur un corps de base k_0 .

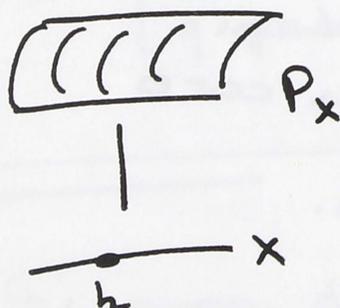
Notion de G -torseur au dessus de k_0 :

Soit K une ext. de k_0 , de t. fini, et séparable (\Rightarrow il y a un modèle lisse). Soit \underline{P} un G -torseur sur K .

On dit que \underline{P} est lisse si les propriétés suivantes sont satisfaites:

On peut trouver une k_0 -variété lisse, X , irréductible, connexe, et de corps de fct K . Quitte à la remplacer par un ouvert non vide, on peut supposer que \underline{P} provient d'un toseur P_X sur X .

Choisissons un tel P_X . (La condit^o qu'on va donner sera indép^{te} de ce choix).



La notion de spécialisation est maintenant claire: pour tout pt $x \in X(k)$, on obtient un toseur P_x . (à priori, il dépend du choix de P_X et de x).

def. \underline{P} est lisse si pour toute extension h du corps k_0 , infini, et pour tout G -torseur \underline{Q} sur h , et tout ouvert U (de Zariski) non vide de X , il existe $x \in U(h)$ tel que $\underline{Q} \cong \underline{P}_x$.

De façon équivalente,

P est versel si pour tout G torseur G sur k l'ensemble des $x \in X(k)$ tq $P_x \cong G$ est dense.

On peut définir cette notion pour des g ps ou E isses, mais ici, le cas E isse suffira.

Les versels E isses sont faciles à construire:

$\left\{ \begin{array}{l} \text{Si } G = GL_n, \text{ un torseur versel existe.} \\ \text{Si } H \subset G \text{ et si } G \text{ a un torseur versel,} \\ \text{alors } H \text{ en a un aussi.} \end{array} \right.$

N.B.: il faut supposer G g pe alg. E in.

Constructions: On se donne

$G \subset G'$ g pe E linéaire. Dans la pratique,
 $G' = GL_n$ ou SL_n ou Sp_{2n} .

On va construire un P versel pour des torseurs G' triviaux.

$P/G \quad G \rightarrow G'$ induit P/G' qui a suppose trivial.

On suppose que $G'(k)$ est dense ds G' pour tout k ∞ . On se donne $X \subset Y'$ variétés sur k_0 , et des actions de G sur Y et de G' sur Y' compatibles entre elles.

On suppose:

- Y est un G torseur, de base $X = Y/G$.
- Y est un ouvert dense de Y' .

• Pour tout corps $k \neq \infty$, $Y(k)$ est Zariski dense.

(Si k_0 est ∞ , cette dernière hyp. revient à fait à $Y(k_0)$ Zariski dense).

Alors Y est dense pour les G-torseurs qui ont G' triviaux.

Exple ① Si on prend $Y = G' = Y'$
 G et G' opérant par translation (à gauche).
 Dans ce cas, $X = G'/G$ espace homogène.

$$\begin{array}{c} \triangleleft G' \\ \downarrow \\ \text{---} X = G'/G \end{array}$$

Exple ② G gpe fini.

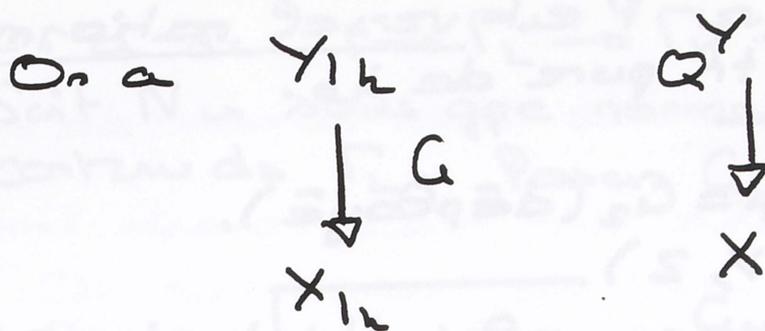
$G \subset GL_n = \text{Aut}(V)$ où V esp. de dim n sur k_0 .
 $Y' = V$. Mais l'act^o de G sur V n'est pas libre. On prend $Y = E$ ouvert de V formé des pts à fixateur trivial.

Le 1^{er} exple a l'inconvénient de donner des dimensions assez grandes.

On va maintenant expliquer le thm énoncé p. 10.

1^{er} critère:

Soit k un corps, et G un G -torseur / k .



Q est isomorphe à la fibre Y_x de Y

\Uparrow Si on tord $Y|_h$ par le G torsueur Q ,
la variété Y obtenue a un pt rationnel
au dessus de $x \in X(h)$.

(N.B.: Si F est une variété sur laquelle
 G opère, on peut définir le tordu de
 F par Q , Q^F).

$$Y \subset Y' \quad \begin{array}{c} Y \\ \downarrow Q \\ Q^Y \end{array} \subset \begin{array}{c} Y' \\ \downarrow Q' \\ Q^Y \end{array} \quad \text{ou } Q' = Q/G' \text{ (étendu à } G').$$

de les pts rationnels et de voir
qfd.

On vient donc de construire un ensemble
pour les torsueurs G' triviaux.

(Il faut vérifier que Y est G' trivial,
à revoir ...)

(En fait on suppose G' tq tout
 G' torsueur est trivial).

Exple: Si $G' = GL_n$ ou SL_n ou Sp_{2n} , on sait
que tous les G' torsueurs st triviaux.

On dit que P est verseel rationnel si K ext. tr. pure de k_0 .

(exple: $G = G_2$ (déployé),
 $K = \mathbb{Q}(x, y, z)$)

G torsours d'alg. d'octonions,
 octonion verseel : $e_1^2 = x$; $e_2^2 = y$; $e_3^2 = z$...

Quis: $G = \begin{cases} E_8 \\ F_4 \end{cases}$ est-il un torsour
 verseel rationnel ?

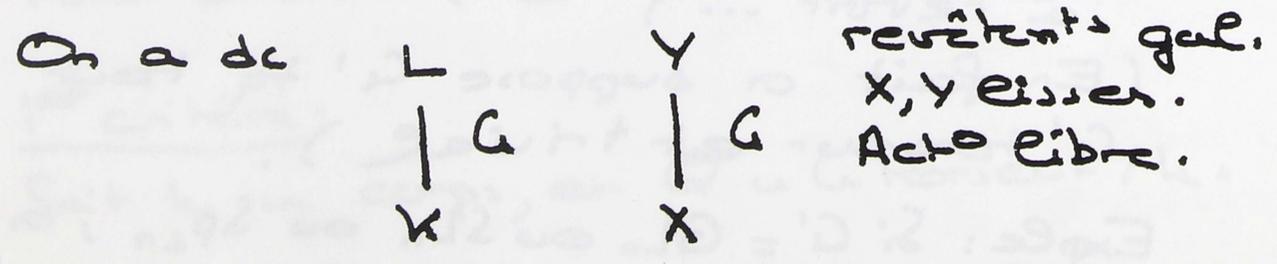
(Autre exple: $G = PU_2$; $K = \mathbb{Q}(x, y)$
 alg. de quat. $e_1^2 = x, e_2^2 = y$).

On revient maintenant au cas où
 G est un groupe alg. fini. (i.e. à un
 grpe alg. de dim. 0).

- G torsours
- \updownarrow G alg. gal.
- \updownarrow hom. continus $\Phi: \Gamma_k \rightarrow G$, à conj. près.

Partant d'un G torsour verseel pour les
 corps constants $k_0 = \begin{cases} \mathbb{Q} \\ \mathbb{F}_p \end{cases}$:

c'est un corps K , et un $\underline{\Phi}: \Gamma_K \rightarrow G$.
 verseel $\Rightarrow \underline{\Phi}$ est surjectif.



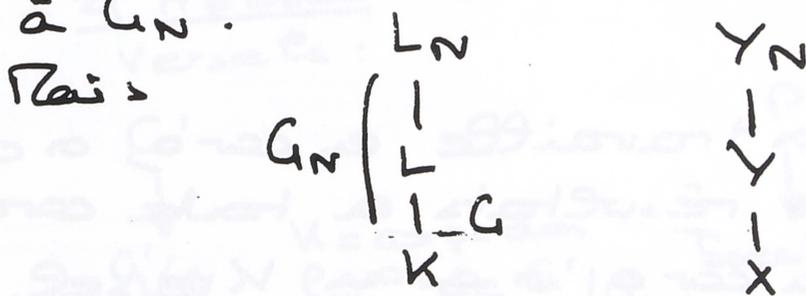
O. a de $1 \rightarrow \Gamma_L \rightarrow \Gamma_K \rightarrow G \rightarrow 1$

Soit N un sous gpe normal ouvert de Γ_K contenu dans Γ_L . Posons $G_N := \Gamma_K/N$. G_N
 \downarrow
 G

Lemme: L'extension G_N a la propriété de relèvement pour la caractéristique étudiée.

Preuve: le corps \mathbb{Q} , de la caract. donnée.

$\varphi: \Gamma_K \rightarrow G$. On veut mg φ se relève à G_N .



si X est assez petit (i.e. quitte à remplacer X par un ouvert) op Y_N relèvement étale.

versalité: φ provient d'un k pt $x \in X(k)$.

D'où \rightarrow un G_N torseur et de un $\varphi': \Gamma_K \rightarrow G_N$ relevant φ .

Soit $a \in H^q(G, \mathbb{Z})$ ou \mathbb{Z} est un G module.

- ① a est neg. pour les corps de la car. considérée.
- ② $\Phi^*(a) = 0$ ds $H^q(K, \mathbb{Z})$
- ③ Il existe un G' ayant la prop. de relèvement a ds la car. étudiée qui tue a .

Ce thm précise bien la not^o de nég.

Dém.: elle est maintenant immédiate

$$\textcircled{1} \Rightarrow \textcircled{2}$$

\parallel

$\textcircled{3}$
Reste à voir $\textcircled{2} \Rightarrow \textcircled{3}$

Puis a disparaît sur $K \Rightarrow a$ disparaît déjà sur un ext. gal. finie q'u suppose contenir L de K . Notons la L_N . On prend $G' = G_N$ le gpe correspondant.

appl.

Rqz: si on travaille en $\text{car } 0$, on obtient des résultats en toute caract.

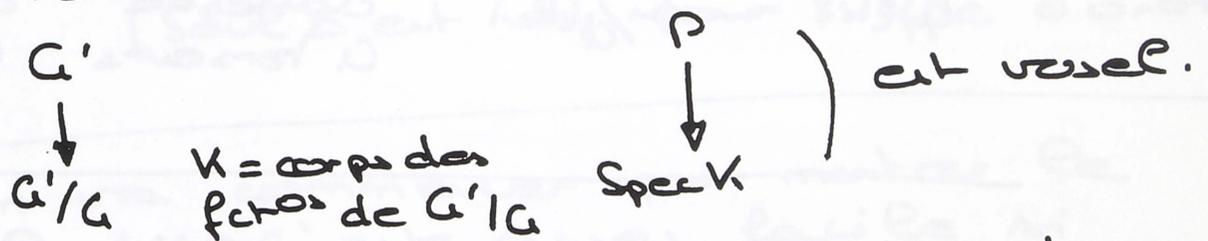
(i.e. si en $\text{car } 0$ on a un K résolu, il nous fournit des G' . Ces G' ont la prop. de relevement en toute car.)

On commence par deux remarques sur
le cours de la semaine dernière :

1) Gabber :

L'objet "vase" et on a parlé ne
l'est pas vraiment. Mais la G torsion
qui devient triviale sur G' s'obtient
bien par image réciproque à partir de
cet objet.

2) A propos de la construction d'objets
vases :



(On suppose que G' est connexe, et
 $G'(h)$ dense. Dans la pratique, $G' = GL_n$ ou SL_n .)

Preuve : Si Q est un G torsion sur h
devient triviale sur G' :

Q (G torsion / h) induit un torsion Q'
 $G \rightarrow G'$ sur G' caractérisé par
l'existence d'une flèche $Q \rightarrow G'$
compatible avec $G \rightarrow G'$.

Donc Q est une fibre de l'espace
homogène.

Les différents faisceaux d'envoyer
 $\mathcal{O} \rightarrow G'$ différent d'un pt de $G'(k)$.
 De

les G torsseurs \rightarrow $G'/G(k)$ modulo
 G' triviaux \rightarrow l'act^o de $G'(k)$.

En d'autres termes: on a la
 suite exacte de cohomologie
 galoisienne suivante :

$$\begin{array}{ccccccc}
 H^0(k, G') & \rightarrow & H^0(k, G'/G) & \rightarrow & H^1(k, G) & \rightarrow & H^1(k, G') \\
 \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\
 G'(k) & & G'/G(k) & & \text{classes de} & & \text{classes de} \\
 & & & & G \text{ torsseurs} & & G' \text{ torsseurs.}
 \end{array}$$

On va continuer à expliciter l'existence
 d'objets versels.

On va commencer par noter le
 thm suivant :

Thm 1 :
 Soit G un groupe fini. \exists un entier
 $N_1 = N_1(G)$ tq pour tout G -module
 \mathbb{Z} , pour tout $q > N_1$, et pour tout
 $x \in H^q(G, \mathbb{Z})$, $2x$ est nég.

Autrement dit, si on note

$$H_e^q(G, \mathbb{Z}) = H^q(G, \mathbb{Z}) / H_n^q(G, \mathbb{Z})$$

(effectif)

Thm 1 :
 $2 H_e^q(G, \mathbb{Z}) = 0$ si $q > N_1$.

En fait, on va même montrer mieux :

Thm 2 : \vec{n} notation et \vec{n} hyp.
 Il existe un entier N_2 tel que
 pour tout $q > N_2$ on ait équivalence
 entre
 \uparrow (i) x est négigeable
 \Downarrow (ii) la restriction de x à \mathbb{F}_q
 sous gpe d'ordre 2 de G
 est 0.

Rq : (i) \Rightarrow (ii) est clair car
 restriction d'un nég. est nég.
 { Seul 0 est nég. pour \gg gpe d'ordre 2.

On va commencer par montrer le
 Thm 1. C'est assez facile si
 on ne cherche pas une très bonne
 valeur de N_1 .

Démonstration :

Soit Q un G torsueur sur un
 corps K , ext. de type fini de \mathbb{Q} .
 Appelons d le degré de transcendance
 de K sur \mathbb{Q} . Alors $N_1 = d+3$ convient.

notons $i = \sqrt{-1}$. $K(i) = K$ ou est quadratique
 sur K . Il est connu que $\text{cd } K(i) = d+2$.
 (Grothendieck?; Tate, Lang; Colom. gal.).
 De plus $\text{scd } K(i) \leq d+3$.

Le 18.10.93

III - (4)

(Rappel): cd est relatif aux mod. de torsion.
scd qqqz

On a de

$$H^q(K(i), \mathbb{Z}) = 0 \text{ si } q > d+3 = N,$$

\Downarrow par transfert

$$2H^q(K, \mathbb{Z}) = 0 \text{ si } q > N.$$

Alors si $x \in H^q(G, \mathbb{Z})$

$$\Downarrow$$
$$x_K \in H^q(K, \mathbb{Z}). \quad 2x_K = 0.$$

\mathbb{Z} , comme le torsion est usuel,
ceci permet de conclure.

On va maintenant démontrer le 2nd
thm. On aura besoin d'un certain nombre
de résultats préliminaires.

Le premier est le suivant:

Soit K un corps.

On suppose qu'il existe une extension
finie K_1/K telle que $cd(\Gamma_{K_1}) = n < \infty$.
 $n \geq 1$.

Thm: Si \mathbb{Z} est un Γ_K module (resp. de
torsion); si $q > n+1$ (resp. $> n$);
et si $x \in H^q(\Gamma_K, \mathbb{Z})$ a une restriction
nulle à tous les sous gres
d'ordre 2 de Γ_K ,
alors $x = 0$.

Rappels (Artin-Schreier).

Si K est un corps, et si Γ_K est un \mathbb{Z} -groupe d'ordre fini $m \geq 2$, alors :

① $\text{car } K = 0$

② $m = 2$

③ s est la conjugaison complexe associée à une structure de corps ordonné sur K

ou (ce qui revient au même)

$\bar{K} \supseteq K^{(s)}$ est un corps ordonné maximal.

④ Le centralisateur de s dans Γ_K est $\{1, s\}$.

Rqra : Soit X l'espace des \mathbb{Z} -groupe d'ordre 2 de Γ_K . Γ_K opère sur X par conjugaison. Posons $\Omega = X / \Gamma_K$.

Alors

$\Omega \cong \{ \text{rel. d'ordre total sur } K \}$.

X est compact car $\{s \mid s^2 = 1\}$ est fini et 1 est un \mathbb{Z} -groupe d'ordre fini de cet espace. (cf. $K^{(i)}$).

Démonstration de ④ :

Si $t \in \Gamma_K$ commute à s , alors t définit un automorphisme du corps $R = \bar{K}^{(s)}$ qui est l'identité sur K . En fait, c'est l'identité sur R .

En effet, soit $x \in R$. Soient x_1, \dots, x_n ses K -conjugués $\in R$.

le 18.10.93

⑥

t respecte la structure d'ordre de \mathbb{R} , car les positifs et les carrés.

Mais (c'est un lemme de théorie des ensembles): un ens. fini totalement ordonné n'a pas d'aut. non triviaux.
De t fixe les x_i

D'autre part, on utilisera également le thm suivant: (Topology 1965).

Thm: Si Γ est un gpe profini, et Γ_i un ss.gpe ouvert de Γ , on a $\text{cd}_p \Gamma = \text{cd}_p \Gamma_i$, pourvu que Γ ne contienne pas d' \mathbb{Z}^t d'ordre p .

Mais si $\text{car } K \neq 0$, Artin-Schreier $\Rightarrow \Gamma_K$ est sans torsion. de $\text{cd } \Gamma_K = \text{cd } \Gamma_K$.
D'où $H^q(\Gamma_K, n) = 0$ si $q > n+1$
($q > n$ cas torsion).

Si K contient i , il n'y a pas d' \mathbb{Z}^t d'ordre 2 de Γ_K , et le même argument s'applique.

Le 18.10.93

(7)

Donc la situation intéressante est celle
d'un corps K tq $i \notin K$ et ad $\Gamma_{K(i)} = n$.
C'est cette situation qu'on étudie.

On se place dans le cas particulier
où $\Gamma = \mathbb{Z}/2\mathbb{Z}$.
cf. article Colliot-Thélène et Parigot.
(Inv. 1989).

Les arguments viennent d'Arason (1975)
cf. article Arason - Elman - Jacobson.

$\Gamma_K \supset \Gamma_{K(i)}$.

Passage de la cohomologie d'un gpe
à celle d'un ss gpe d'ordre 2.

Soit G un gpe, et G_1 un ss gpe d'indice 2.

$G \xrightarrow{\varepsilon} \{\pm 1\}$; $G_1 = \ker \varepsilon$.

Soit Γ un G -module.

Γ_ε est le bordu de Γ par ε , i.e.

$$\Gamma_\varepsilon = \Gamma \otimes_{\mathbb{Z}} \mathbb{Z}_\varepsilon,$$

où $\mathbb{Z}_\varepsilon = \mathbb{Z}$ muni de l'action de G :
c'est de signe par ε .

$H^1(\{\pm 1\}, \mathbb{Z}_\varepsilon) \cong \mathbb{Z}/2\mathbb{Z}$. Notons (ε) , l'unique
2-ét carrique d'ordre 2.

On lui associe un 2-ét de $H^1(G, \mathbb{Z}_\varepsilon)$,
qu'on note encore (ε) .

Le cocycle correspondant est défini:

$$\text{par } s \in G \rightarrow \begin{cases} 0 & \text{si } s \in G_1 \\ 1 & \text{si } s \notin G_1. \end{cases}$$

Lemme: \mathcal{O}_1 a eu suite exacte:

$$\dots \rightarrow H^q(G, \mathbb{Z}) \xrightarrow{\text{Res}} H^q(G_1, \mathbb{Z}) \xrightarrow{\text{Cor}} H^q(G, \mathbb{Z}_\varepsilon) \xrightarrow{\delta} H^{q+1}(G, \mathbb{Z}) \rightarrow \dots$$

Rqz: En fait

$$\begin{array}{ccc} H^q(G_1, \mathbb{Z}) & \longrightarrow & H^q(G, \mathbb{Z}_\varepsilon) \\ \parallel & \nearrow & \text{Cor} \\ H^q(G_1, \mathbb{Z}_\varepsilon) & & \end{array}$$

car $\mathbb{Z}_\varepsilon = \mathbb{Z} \hat{=} G_1$ module.

Par ailleurs: $\mathbb{Z}_\varepsilon \otimes \mathbb{Z}_\varepsilon \rightarrow \mathbb{Z}$.

de $d(x) = (\varepsilon)_1 \cdot x$ (cup produit).

Lemme:

Soit $x \in H^q(G, \mathbb{Z})$.

$$\text{Res}(x) = 0$$

$\Leftrightarrow x$ est div. par $(\varepsilon)_1$.

i.e. $\exists x' \in H^{q-1}(G, \mathbb{Z}_\varepsilon)$

$$\text{tq } x = (\varepsilon)_1 x'.$$

(C'est une conséquence directe du lemme précédent: exactitude).

C'est un lemme standard en cohomologie d'ordre 2.

Démonstration de ce cas :

$$\tilde{\mathbb{Z}} := \text{Ind}_{G_1}^G \mathbb{Z}.$$

$\tilde{\mathbb{Z}} = \mathbb{Z} \oplus \mathbb{Z}$ est grpe abélien, muni de l'act^o de G définie par

$$s \in G \quad s(m_1, m_2) = \begin{cases} (sm_1, sm_2) & \text{si } s \in G_1 \\ (sm_2, sm_1) & \text{si } s \notin G_1. \end{cases}$$

On a

$$0 \rightarrow \mathbb{Z} \rightarrow \tilde{\mathbb{Z}} \rightarrow \mathbb{Z}_2 \rightarrow 0 \quad \text{suite exacte de } G \text{ modules.}$$

$$(m_1, m_2) \mapsto m_1 - m_2$$

$$m \mapsto (m, m)$$

La suite exacte de cohomologie induit est celle qu'on veut.

$$H^q(G, \mathbb{Z}) \rightarrow H^q(G, \tilde{\mathbb{Z}}) \rightarrow H^q(G, \mathbb{Z}_2) \xrightarrow{\delta} H^{q+1}(G, \mathbb{Z})$$

\swarrow Shapiro \parallel \nearrow Cor
 $H^q(G, \mathbb{Z})$ (faute à vérifier)

E. fait, il reste juste à vérifier que le cobord δ est un cup produit.

Calcul: On part d'un q -cocycle de \mathbb{Z}_2 $m(g_1, \dots, g_q)$. $m \in \mathbb{Z}_2$ peut se relever à $(m, 0)$.

$$\tilde{m}(g_1, \dots, g_q) = (m(g_1, \dots, g_q), 0).$$

On veut calculer

$$\delta \tilde{m}(g_1, \dots, g_{q+1}) \stackrel{\text{déf.}}{=} g_1 \tilde{m}(g_2, \dots, g_{q+1}) - \tilde{m}(g_1 g_2, \dots, g_{q+1}) \\ \dots \pm \tilde{m}(g_1, \dots, g_q g_{q+1}).$$

On obtient donc

$$\delta^{\tilde{m}}(g_1, \dots, g_{q+1}) = \begin{cases} (g_m(g_1, \dots, g_q), 0) \\ \infty \\ (0, g, m(g_2, \dots, g_q)) \dots \pm (m(g_1, \dots, g_q), 0) \end{cases}$$

dirant que $g_i \in G_i$ ou non.

Mais m est un cocycle de \mathbb{Z}_E . De pratiquement il s'en va, et on obtient finalement $\delta^{\tilde{m}} = (\epsilon)_{,m}$.

Le pt ② d'Artin Schreier explique bien pourquoi les $\mathbb{Z}E$ de torsion ont d'ordre 2.

Si $s \in \Gamma_K$ est d'ordre $n > 2$, alors

$$\bar{K}^{s^2} = K'; \Gamma_{K'} = C_n.$$

Alors on est le seul $\mathbb{Z}E$ nég. de la cohomologie de C_n

La contradiction.

On a de $K_i = K(i)$ (initiateur du thm. p. ④).

$$K \mid \mathbb{Z}E \text{ est un } \Gamma_K \text{ module.}$$

avec $\text{cd } \Gamma_{K(i)} \leq n$.

$\Gamma_{K(i)} / \Gamma_K$ cyclique d'ordre 2

La fournit un caractère ϵ d'ordre 2.

Prop.: Si $q > n+1$, alors le cup produit par $(\epsilon)_i \in H^1(\Gamma_K, \mathbb{Z}_E)$ est un isom. de $H^q(\Gamma_K, \mathbb{Z}_E)$ dans $H^{q+1}(\Gamma_K, \mathbb{Z})$.

Preuve: $H^q(\Gamma_K, \mathbb{Z}) = 0$. D'après la suite exacte devint

$$0 \rightarrow H^q(K, \mathbb{Z}_\ell) \xrightarrow{\cong} H^{q+1}(K, \mathbb{Z}) \rightarrow 0.$$

On a une sorte de périodicité d'ordre 2.

$$\mathbb{Z}_\ell \otimes \mathbb{Z}_\ell = \mathbb{Z}$$

$$(\varepsilon)_1, (\varepsilon)_1 = (\varepsilon)_2 \in H^2(K, \mathbb{Z})$$

$$\stackrel{12}{H^1(K, \mathbb{Q}/\mathbb{Z})}.$$

$$u \in H^2(C_2, \mathbb{Z})$$

$(\varepsilon)_2$ est l'image préimage de u .

$$H^q(\Gamma_K, \mathbb{Z}) \xrightarrow{\cong} H^{q+2}(\Gamma_K, \mathbb{Z})$$

par cup produit par $(\varepsilon)_2$.

De façon générale, si $\varphi: \Gamma_K \rightarrow (\pm 1)$, on

lui associe:

$$\begin{cases} \varphi \in H^1(\Gamma_K, \mathbb{Z}/2\mathbb{Z}) \\ (\varphi)_1 \in H^2(K, \mathbb{Z}_\varphi) \\ (\varphi)_2 \in H^2(K, \mathbb{Z}). \end{cases}$$

C'est car $K=0$,

si $a \in K^*/K^{*2} \mapsto (a) \in H^1(K, \mathbb{Z}/2\mathbb{Z})$.

On notera $(a)_1 \in H^1(K, \mathbb{Z}_\varphi)$ et $(a)_2 \in H^2(K, \mathbb{Z})$ les éléments correspondants.

Lemme: Si $(a)(b) = 0$ dans $H^2(K, \mathbb{Z}/2\mathbb{Z})$, $a, b \in K^*$ on a $(a)_1, (b)_2 = 0$ dans $H^3(K, \mathbb{Z}(a))$.

le 18.10.93

En particulier, $(a), (-a)_2 = 0 \forall a \in K^*$. (12)
(On sait en effet $(a)(-a) = 0$).

Preuve: $0 \rightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$

$\delta: H^1(K, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(K, \mathbb{Z})$ le cobord.

$\delta(\varphi) = (\varphi)_2$.

Posons $(b) = \varphi$

$(a), (b)_2 = (a), \delta(\varphi)$.

Mais $0 \rightarrow \mathbb{Z}_{(a)} \xrightarrow{2} \mathbb{Z}_{(a)} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$.

$\delta_{(a)}: H^1(K, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^{q+1}(K, \mathbb{Z}_{(a)})$.

$(a), \varphi \in H^2(K, \mathbb{Z}_{(a)} \oplus \mathbb{Z}/2\mathbb{Z}) = H^2(K, \mathbb{Z}/2\mathbb{Z})$.

$\delta_{(a)}((a), \varphi) = (a), \delta(\varphi) = (a), (b)_2$.

Mais $(a), \varphi = (a)(b) = 0$.

De $\delta_{(a)}((a), \varphi) = 0$. ~~effd~~

On devrait maintenant pouvoir démontrer le thm 2. (idée d'Arason).

Soit $x \in H^q(\Gamma_K, \mathbb{Z})$ avec $q > n+1$ (resp. $> n$).

On suppose que $\text{Res}_H(x) = 0$ pour tout sous groupe H d'ordre 2. mg $x = 0$.

Supposons $x \neq 0$.

Soit S e' est. des $>>$ q'es fermés H de Γ_K tels que $\text{Res}_H(x) \neq 0$.

On l'ordonne par inclusion descendante.

Si (H_α) est une famille totalement ordonnée d'éléments de S , alors $\bigcap_\alpha H_\alpha$ est ds

$(H^q(H, \mathbb{Z}) = \varprojlim (H^q(H_\alpha, \mathbb{Z})).$)

Par Zorn, on peut de choisir un H minimal.
On va montrer que tel H est d'ordre 2,
ce qui permet de conclure.

H étant minimal, quitte à remplacer
 K par \bar{K}^H , on a que Γ_K est minimal,
i.e. que si $H \subset \Gamma_K$, fermé, $\neq \Gamma_K$
alors $\text{Res}_H x = 0$.

On sait depuis le départ que $2x=0$.
La classe de colon. x est de
d'ordre 2.

① Γ_K est un pro 2 gpe.

Si non, soit H un 2 Sylow de Γ_K .

$H \neq \Gamma_K$ et $\text{Res}_H(x) = 0$. contradictoire.

② Γ_K est cyclique.

• $H^1(\Gamma_K, \mathbb{Z}/2\mathbb{Z})$ est de dim. 1.

Il est clair que $i \notin K$. De $K(i)/K$ est
une ext. quadratique. Elle correspond
à un élément $(-1) \in H^1(K, \mathbb{Z}/2\mathbb{Z})$.

Le dim ≥ 1 .

Si $\dim H^1(K, \mathbb{Z}/2\mathbb{Z}) > 1$, il y aurait un autre
élément $a \in K^*$ tq $(a) \neq (0), (-1)$

$x \in H^1(K, \mathbb{Z})$. On restreint x au sous-
d'indice 2 défini par a . Par le
lemme, on trouve 0. De $x = (a)$, x'
avec $x' \in H^1(K, \mathbb{Z}_a)$.

[En fait, on joue sur l'ext. biquadratique $\kappa(\sqrt{a}, i)$].

De \vec{m} $x = (-a), x''$ avec $x'' \in H^{q-1}(\kappa, \pi_{-a})$.

Alors:

$$(-1)_2 x = (-1)_2(a), x' \in H^2(\kappa, \mathbb{Z}).$$

$$(-1)_2 = (a)_2 + (-a)_2.$$

$$\Delta (-1)_2 x = (a)_2(a), x' + \underbrace{(-a)_2(a), x'}.$$

$$(-1)_2 x = (a)_2(a), x' = (a)_2 x. \quad \text{"}$$

$$(-1)_2 x = \underbrace{(a)_2(-a), x''}_0 = 0. \quad \Delta \boxed{(-1)_2 x = 0}$$

Mais la multiplication par $(-1)_2$ est injective (cf. Lemme précédent).

$$\Delta \boxed{x = 0.}$$

R.B.: En fait, on va démontrer le thm avec les hyp. suivantes:

G gpe profini; G_1 ss gpe d'indice 2.

$$\varepsilon: G \rightarrow \pm 1 \quad \text{cd } G_1, z_n < \infty.$$

Pour H ss gpe fermé H de G , et

$$H \times G \in H^1(H, \mathbb{Z}/2\mathbb{Z}) \text{ on a } \kappa \cdot \kappa = \varepsilon_H \cdot \kappa$$

$$\text{ou } \varepsilon_H = \text{Res}_H \varepsilon.$$

- Γ_κ est de u pro 2 gpe tq $H^1(\kappa, \mathbb{Z}/2\mathbb{Z})$ est de dim. 1.

Mais $\varepsilon \in H^1$ d'u pro \mathcal{P} gpe détermine les générateurs de ce gpe.

$\Delta \Gamma_\kappa$ est engendré par un élém^t.

Ainsi $\Gamma_K \simeq \mathbb{Z}_2$ ou $\mathbb{Z}/2^k\mathbb{Z}$ $k \geq 1$.

Déjà $k > 1$ est imp. par Artin-Schreier.

De plus pour \mathbb{Z}_2

$$H^q(\mathbb{Z}_2, \mathbb{Z}) = 0 \text{ si } q \geq 3.$$

Or ds le thm, $q \geq 3$

↳ contradicto car $x \neq 0, x \in H^q(\dots)$.

Supplément au thm (Artin-Schreier-Jacob, Colliot-Thélène et Parimala)

Cas où $\Gamma = \mathbb{Z}/2\mathbb{Z}$

$$H^q(K, \mathbb{Z}/2\mathbb{Z}) \simeq \mathcal{C}(\Omega, \mathbb{Z}/2\mathbb{Z}) \text{ (fctos continus)}.$$

où $\Omega = \{ \text{structure d'ordre sur } K \}$
 $= \{ \text{eets d'ordre 2, à conf. près} \}.$

$$\text{d'ordre 2} \in H^1(\mathbb{C}_2, \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}.$$

Ds le cas gal :

Sur Ω , on peut mettre deux faisceaux Γ^+ et Γ^- :

Si Γ est vu cō u faisceau est sur Ω , on définit des sous-faisceaux :

$$\mathcal{Q} = \Gamma_2 / \text{conj.} \quad \Gamma_2 = \{ \text{eets de } \Gamma_K \text{ d'ordre 2} \}.$$

$$\text{On a } 1 \rightarrow \Gamma_K \rightarrow \Gamma_K \rightarrow \mathbb{C}_2 \rightarrow 1$$

↳ pas de torsion.

De Ω revient à prendre les sectos qui st des ss gpes, à conf. près.

le 18.10.93

III- (16)

On peut de trouver un secteur
confiné $\omega \in \Omega$ et $\Delta_\omega \in \Gamma_2$.

Du coup, on peut définir

$$\text{Ker}(1-\Delta_\omega)\Gamma_2 / \text{Im}(1+\Delta_\omega)\Gamma_2 = \Gamma_+(\omega) = H^{\text{pair}}(\mathbb{C}_2, \Gamma_2)$$

et

$$\text{Ker}(1+\Delta_\omega)\Gamma_2 / \text{Im}(1-\Delta_\omega)\Gamma_2 = \Gamma_-(\omega) = H^{\text{impair}}(\mathbb{C}_2, \Gamma_2)$$

Il paraît naturel que

$$H^q(K, \Gamma) \cong H^0(\Omega, \Gamma_\pm)$$

} + si q pair
- si q impair.

(Mais ce n'est pas encore démontré.)

(Hyp: K est un corps, car $K=0$
tq dim. conf. de $K(i) = n < \infty$.

Ceci serait vrai pour

$$\begin{cases} q > n & \text{si } \Gamma \text{ est de torsion} \\ n+1 & \text{si non.} \end{cases}$$

J.P. Serre IV
Cours au collège
de France.

Le 25 octobre 93

IV ①

La démonstration du thm 2 n'est pas
tout à fait terminée:

Thm 2: \exists une N_2 (dpt de G) telle que
si \mathbb{Z} est un G module, $q \geq N_2$ et
 $x \in H^q(G, \mathbb{Z})$, et si x a une restriction
nulle à ts les ss gpes d'ordre 2
de G , alors x est négligeable.

On sait qu'il suffit de vérifier sur
les ss gpes d'ordre 2 dans un cas
verse, où on a K ext. de t.p. de \mathbb{Q}
et ext. gal L/K de gpe G .

L/K correspond à $\varphi: \Gamma_K \rightarrow G$.

x négl. $\Leftrightarrow \varphi^* x = 0$ ds $H^q(\Gamma_K, \mathbb{Z})$

On prend $N_2 = \deg \text{tr } K + 3$.

On regarde $K(i)$ cd $\Gamma_{K(i)} = \deg \text{tr } K + 2$.

Alors si $K = K(i)$ pas de pb: $H^q(\Gamma_K, \mathbb{Z}) = 0$.

Si $\Gamma_{K(i)} \subset \Gamma_K$ et on applique le thm

démontre la dernière fois, qui dit
que la cohom. est déterminée par les

ss gpes d'ordre 2. Si $\{1, c\} \subset \Gamma_K$ est un

tel ss gpe $\{1, c\} \subset \Gamma_K \xrightarrow{\varphi} G$

$\varphi(c)$ est d'ordre 1 ou 2 ds G .

ce qui permet de conclure

②

Application: $\Gamma = \mathbb{Z}/2\mathbb{Z}$ $H^q(G, \mathbb{Z}) = H^q(G)$.

$H^*(G) = \bigoplus H^q(G)$ est une algèbre commutative-lire, graduée, sur \mathbb{F}_2 , de t. finie.

$$H^*(G)_e := H^*(G) / H^*(G)_n$$

on s'efforce à décrire ceci.

Quillen: a donné une description de $\text{Spec } H^*(G)$ (encore valable en car. mod. p en négligeant les élts nilpotents).

Pour car. mod. p:

$I \subset G$ élémentaire abélien (p, \dots, p) .
 $I \subset I^{\text{vect}} \quad I^{\text{vect}} = \text{Spec } \text{Sym}_{\mathbb{F}_p}(I^*)$.

À si p.ex. I est cyclique d'ordre p ,
 $I^{\text{vect}} = G_a = \text{Spec } \mathbb{F}_p[T]$ (ditz affine).

Il est facile de voir que

$\text{Spec } H^*(I) = I^{\text{vect}}$. On a de plus des flèches $I^{\text{vect}} \rightarrow \text{Spec } H^*(G)$.

Thm de Quillen:

- 1) $\text{Spec } H^*(G) = \bigcup$ des images des I^{vect}
- 2) donne la rel. d'équiv. (induite par conj.).

2): si I_1, I_2 et $g \in G$ $g I_1 g^{-1} \subset I_2$ on obtient des flèches entre les cohomologies, qui donnent l'idéalité au niveau de $\text{Spec } H^*(G)$.

le 25.10.93

IV-③

Ds le cas où on a un p -Sylow
élémentaire (p, \dots, p) , on a
 $\text{Spec } H^*(G) = \text{Sylow}^{\text{vect}} / \text{Norm.}$

En particulier,

$\dim \text{Spec } H^*(G) = \text{rg maximale des ss gres}$
élémentaires de type
 (p, \dots, p) .

Regardons maintenant $H_e^*(G)$ ds le
cas $p=2$.

$\text{Proj.}(H_e^*(G))$ est de dimension 0. Il
est formé des classes de conjugaison
des involutions de G . C'est de n
els. fini Ω . (C'est des pts rationels
sur \mathbb{F}_2).

$\text{Spec } H_e^*(G) = \text{cone sur } \Omega$.

En particulier, si $2 \mid |G|$, on voit
que $\dim \text{Spec } H_e^*(G) = 1$.

i.e. $\dim H_e^q(G)$ est bornée qd q varie.

En fait, il y a même périodicité
de la cohomologie en grands degrés.

Quatre espaces: (sans démonstration).

C_2 : $H^0 = H^2 = \mathbb{F}_2[t]$ t de degré 1.

C_4 : $\dim H^q = 1 \forall q$. Notons x_1 et x_2 les éléments non nuls de degré 1, 2, ils engendrent la cob. avec la relation $x_1^2 = 0$.

$(1, x_1, x_2, x_1 x_2, x_2^2, \dots)$.

On mq x_1, x_2 est nég., et engendre l'idéal des nég.

De $H^0_C: 1, x_1, x_2, 0, x_2^2, 0, x_3^2$.

Ceci dit, $H^3(C_4, \mathbb{Z}/4\mathbb{Z}) = \mathbb{Z}/4\mathbb{Z}$
Si on note β_3 un gén., $2\beta_3$ est nég.
(mod. 2, c'est nég.), mais a part
mq β_3 n'est pas nég.

S_4 : type symétrique d'ordre 4.

De façon générale, $H^0(S_n) \simeq \mathbb{N}$
 \mathbb{N} = classes de Steifel Whitney.

$(S_n \rightarrow D_n$
 $B_{S_n} \rightarrow B_{D_n} \leftarrow$ classes naturelles.

$H^0(B_{S_n}) = H^0(S_n)$.

donnent des éléments de \mathbb{N} .

Ainsi \mathbb{N}_1 correspond à $\text{sgn}: S_n \rightarrow \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$

$H^0(S_4)$ est engendré par w_1, w_2 et w_3 avec la relation $w_1 w_3 = 0$.

$$\begin{array}{cccc} 1 & w_1^2 & w_1^3 & w_1^4 & \dots \\ & w_2 & w_1 w_2 & w_1^2 w_2 & \\ & & w_3 & w_3^2 & \end{array}$$

$\Delta_c \text{ Spec}$ est de dim 2, formé de deux composantes irréductibles.

($\uparrow \downarrow$) S_4 a deux types de ss qpas (2,2):

1 carteru dans $\Omega_4 \rightarrow w_1 = 0$

et $\{1; (1,2); (3,4); (1,2)(3,4)\}$.

Qd on passe à $H_e^0(S_4)$ on introduit

les rel. $\begin{cases} w_3 = 0 \\ \text{et} \\ w_1 w_2 = 0. \end{cases}$

i.e. $H_e^0(S_4)$ engendré par w_1, w_2 avec la relation $w_1 w_2 = 0$.

Groupe diédral d'ordre 8: Δ_4

H' a une base $\{t_1, t_2\}$

$$\begin{array}{l} t_1, t_2: \Delta_4 \rightarrow \mathbb{Z}/2\mathbb{Z} \\ \uparrow \end{array}$$

à noyau de type (2,2)

La relation $t_1 t_2 = 0$.

H^2 a comme base (t_1^2, t_2^2, e)
 e est l'unique élément de H^2 restrict^o
 aux \gg qps d'ordre 2 et $\neq 0$.

$H^0(\Delta_4)$ est engendré par (t_1, t_2, e) avec
 l'unique relat^o $t_1 t_2 = 0$.

On constate $t_1^3 + e t_1$ et $t_2^3 + e t_2$ st
 négligeables, et engendrent l'idéal
 des négligeables.

De $H^0_e(\Delta_4)$: $1 ; t_1 ; t_2 ; t_1^2 ; t_2^2 ; e ; t_1^3 = e t_1 ; t_2^3 = e t_2 ; t_1^4 = e t_1^2 ; t_2^4 = e t_2^2$

Pour mq $t_i + e t_i$ st négligeables,
 on peut regarder les dx placements
 de Δ_4 dans S_4 . W_3 de S_4 est négl., et
 ces dx élém^{ts} st ceux de Δ_4 qui
 donnent W_3 .

Q_8 qpe des quaternions d'ordre 8:

C'est un qpe à col. périodique:

$H(Q_8)$: $1 ; t_1 ; t_2 ; t_1^2 ; t_2^2 ; t_1^3 ; t_2^3 ; e_4 ; e t_1 ; e t_2$
 base de H^1 ; classe de périodicité.

$$t_1^2 + t_1 t_2 + t_2^2 = 0$$

d'où (Bockstein) $t_1^2 t_2 + t_1 t_2^2 = 0$
 et $t_1^3 = t_2^3 = 0$

On montre que $t_1^2 t_2 = t_2 t_1^2$ est nég.ig.
 e n'est pas nég. ; et t_1 et t_2 est.

De

$$H_e^*(Q_8): 1; \begin{matrix} t_1 \\ t_2 \end{matrix}; \begin{matrix} t_1^2 \\ t_2^2 \end{matrix}; 0; e; 0; 0; 0; e^2; \dots$$

\uparrow \uparrow
 $\dim L_1$ $\dim 8$

Rqn. $H^3(Q_8, \mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/8\mathbb{Z}$ (cartan Eilenberg).

Soit u un gène-rateur.

On peut mq $\begin{cases} 2u \text{ nég.} \\ u \text{ non nég.} \end{cases}$

Soit si $\begin{matrix} L \\ | \\ Q_8 \\ | \\ k \end{matrix} \iff \varphi: \Gamma_k \rightarrow Q_8$

$\varphi^*(u) \in H^3(k, \mathbb{Z}/8\mathbb{Z})$ avec $2\varphi^*(u) = 0$.

Prm. Les applications naturelles car $\neq 2$
 $H^3(k, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^3(k, \mathbb{Z}/4\mathbb{Z}) \rightarrow H^3(k, \mathbb{Z}/8\mathbb{Z})$
 et injectives.

(conséquence d'un lem de Serre)

Preuve: pour $H^3(k, \mathbb{Z}/4\mathbb{Z}) \rightarrow H^3(k, \mathbb{Z}/8\mathbb{Z})$.

On a $0 \rightarrow \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$.

Il faut de dénoter

$H^2(k, \mathbb{Z}/8\mathbb{Z}) \rightarrow H^2(k, \mathbb{Z}/2\mathbb{Z})$ est surj.

Mais (Serre) $H^2(k, \mathbb{Z}/2\mathbb{Z})$ est engendré par des cup produits $(x)(y)$ $x, y \in L^*$.

Donc: ? $\rightarrow (x)(y)$.

$$H^2(k, \mathbb{M}_8^{\otimes 2}) \quad x \mapsto \begin{cases} (x) \in H^1(k, \mathbb{M}_2) \\ (x)_8 \in H^1(k, \mathbb{M}_8). \end{cases}$$

$(x)_8 (y)_8$?

Mais $\mathbb{M}_8^{\otimes 2} \cong \mathbb{Z}/8\mathbb{Z}$. Si u racine primitive 8ème de ± 1 ,
 $u \otimes u \in \mathbb{M}_8^{\otimes 2} \mapsto \pm 1 \in \mathbb{Z}/8\mathbb{Z}$.

De tout ça, il résulte qu'en si on a
 L on peut lui attacher un
 \downarrow
 \mathbb{Q}_8 inv. cyclom. dans $H^3(k, \mathbb{Z}/2\mathbb{Z})$.

$$H^3(k, \mathbb{Z}/2\mathbb{Z}) \rightarrow H^3(k, \mathbb{Z}/8\mathbb{Z})$$

et $2\varphi^*(u) = 0$ implique qu'
 $\varphi^*(u) = a(L/k) \in H^3(k, \mathbb{Z}/2\mathbb{Z})$.

cf article E. Bayer - Bases normales autoduales.

O. peut définir un autre invariant
 $b(L/k)$:

P.ex., on regarde q_L forme trace de L
 c'est une f.g. de $\text{rg } 8$, du type suivant:

$$q_L = \langle 1, 1, 1, 1 \rangle \oplus \langle x, x, x, x \rangle \quad x \in K^*$$

(On peut regarder $C = \{1, -1\}$ car \mathbb{Z} de Q_8 .

$$\begin{array}{l} L \\ | 2 \\ L^c \\ | \\ h \end{array} \quad L = L^c \oplus L^-$$

\uparrow
 forme trace
 = forme nitée.

On peut aussi dire qu'il a une
 3-forme de Pfister $\langle \langle 1, 1, x \rangle \rangle$.

On regarde l'invariant d'Arason
 de q_L $(-1)(-1)(-x) \in H^3(h, \mathbb{Z}/2\mathbb{Z})$.

On pose $b(L/h) = (-1)(-1)(x) \in H^3(h, \mathbb{Z}/2\mathbb{Z})$

$(b(L/h) = (-1)(-1)(-1) + \text{Arason})$.

$b(L/h) = 0$ si et seulement si $q_L \simeq \langle 1, \dots, 1 \rangle$
 si et seulement si L/h a une base
 normale autoduale.

$b = a ?$

le 25.10.93

IV-10

G gpe fini.

On va maintenant montrer deux thms:

Thm: Si $a \in H^2(G, \mathbb{Z})$ et si l'act^o de G sur \mathbb{Z} est triviale, alors

$a \text{ n'ég.} \iff a = 0$

(\mathbb{Z} de type fini.).

On peut se ramener à $\mathbb{Z} = \mathbb{Z}$; $\mathbb{Z} = \mathbb{Z}/p^k \mathbb{Z}$ pprem $k \geq 1$

$$H^2(G, \mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z}) = \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$$

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

$$G \rightarrow G \quad n \geq 1.$$

À $\mathbb{Z} = \mathbb{Z}$ et \mathbb{Z} est un cas très simple.

$$\mathbb{Z} = \mathbb{Z}/p^k \mathbb{Z} \cdot \begin{matrix} x \in H^2(G, \mathbb{Z}/p^k \mathbb{Z}) \\ \neq 0 \end{matrix}$$

mg x n'est pas n'ég. Il faut de exhiber un corps...

pt essentielle de la dem.: soit k_0 le corps des racines p^{k_0} ième de 1 (sur \mathbb{Q}).

Alors k_0 ne contient pas de racines primitives p^{k_0+1} ième de 1.

(Irréductibilité du pol. cyclotomique).

$$\mathbb{C}_{p^k} \subset k^*$$

Lemme: Soit F un corps de nbre et μ_F le sgpe des racines de l'unité de F .

Alors $F^* \cong \mu_F \times L$ L ab. libre.

Preuve: E unités de F .

Directement: $E = \mu_F \times L_1$

Mais $F^*/E \cong$ id. ppx C qpe des idéaux.

On qpe des id. est fibre, de base C en id. premiers. De (lt ss qpe d'un fibre et fibre) $F^*/E \cong L_2$

et $F^* = \mu_F \times L_1 \times L_2$.

Ainsi C_{p^α} est facteur direct dans h_0^* .

$\mu_{h_0^*} = C_{p^\alpha} \times \text{reste}$.

De $\boxed{H^2(G, C_{p^\alpha}) \hookrightarrow H^2(G, \mu_{h_0^*})}$

On va maintenant faire le calcul sur un corps réel.

On choisit p.ex. un p -agent de G ds S_n , et on fait opérer G sur $L = h_0(T_1, \dots, T_n)$.

$K = L^G$ invariants.

On va mg la classe $x_K \in H^2(K, \mathbb{Z}/p^\alpha\mathbb{Z})$ est non nulle.

$\mathbb{Z}/p^\alpha\mathbb{Z} \cong \mu_{p^\alpha}$.

De $H^2(K, \mathbb{Z}/p^\alpha\mathbb{Z}) = H^2(K, \mu_{p^\alpha}) \cong B\Gamma_{p^\alpha}(K)$.

On a

$$1 \rightarrow h_0^* \rightarrow L^* \rightarrow \text{Div} \rightarrow 1.$$

(G opère).

Div a pour base l'ensemble Dirr des diviseurs irréductibles, et G permute Dirr . Donc Div est somme directe de modules de permutation.

$$\text{Div} = \bigoplus_{\alpha} \text{Ind}_{G_{\alpha}}^G \mathbb{Z} \quad G_{\alpha} \subset G$$

$$\text{Dirr} = \bigsqcup_{\alpha} G/G_{\alpha}.$$

$$H^1(G, \text{Div}) = \bigoplus_{\alpha} H^1(G_{\alpha}, \mathbb{Z}) = 0.$$

(un gpe fini n'a pas d'hom. non triviaux de \mathbb{Z})

$$\text{Dc} \quad H^2(G, \mathbb{C}_p) \hookrightarrow H^2(G, h_0^*)$$

$$0 \rightarrow H^2(G, h_0^*) \rightarrow H^2(G, L^*)$$

$$\qquad \qquad \qquad \text{Br}^n(K).$$

$$\begin{matrix} \omega \\ x \end{matrix} \mapsto u \in \mathbb{Z}^+ \neq 0.$$

Un cas où on détermine complètement ce qui est négligeable et ce qui ne l'est pas: $G = C_p$, gpe cyclique d'ordre p .

Rat u G module qcqr.

Soit Γ le gpe profini produit semi direct $\Gamma = \mathbb{Z}_p \cdot U_p'$.

$$(U_p = \mathbb{Z}_p^* ; U_p' = 1 + p\mathbb{Z}_p \hookrightarrow U_p)$$

Γ est défini par gén. et relations
cô pro p gpe :

$$\begin{cases} \forall \text{ gén. de } \mathbb{Z}_p ; \sim (\text{corresp. } 1+p \in U_p') \\ \text{relat° } \tau \sigma \tau^{-1} = \sigma(1+p) \end{cases}$$

$$\varepsilon : \Gamma \rightarrow \mathbb{C}_p$$

$$\begin{cases} \forall \mapsto \sigma_p \in \mathbb{C}_p \\ \tau \mapsto 1 \in \mathbb{C}_p \text{ (1 est neutre).} \end{cases}$$

Thm.

① La projection $\varepsilon : \Gamma \rightarrow \mathbb{C}_p$ a la propriété de relèvement.
(i.e. tout hom. continu $\Gamma_h \rightarrow \mathbb{C}_p$ se relève à $\Gamma \rightarrow \mathbb{C}_p$).

② Il existe un corps k , de car 0, avec $\Gamma_k = \Gamma$.

Cor 1 : Une classe $x \in H^q(\mathbb{C}_p, \mathbb{Z})$ est nég. si $\varepsilon^* x = 0$ dans $H^q(\Gamma, \mathbb{Z})$.

Cor 2 : Si $q \geq 3$, x est nég.

Cor 2:

IV- (14)

Γ est un type de Lie de dim 2 p-adique
réalisé par $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \left\{ \begin{array}{l} a \in U \\ b \in \mathbb{Z}_p \end{array} \right.$.

de $\text{scd } \Gamma = 2$

et $H^q(\Gamma, \mathbb{Z}) = 0 \quad \forall q \geq 3$,

Cor 1:

\Rightarrow évident.

\Leftarrow vient du relèvement.

$H^2(\mathbb{C}_p, \mathbb{Z})$, \mathbb{Z} \mathbb{C}_p module.

c'est $\mathbb{Z} \mathbb{C}_p / (1 + \sigma_p + \dots + \sigma_p^{p-1}) \mathbb{Z}$ σ_p générateur de \mathbb{C}_p .

Cor 3:

Soit de $x \in \mathbb{Z} \mathbb{C}_p$.

x classe négligeable

$\Leftrightarrow x = (1 + \sigma_p + \dots + \sigma_p^{p-1})(y) + (1 - \sigma_p)(z)$

où $y \in \mathbb{Z}$ et $z \in \mathbb{Z}$, z p-primaire.

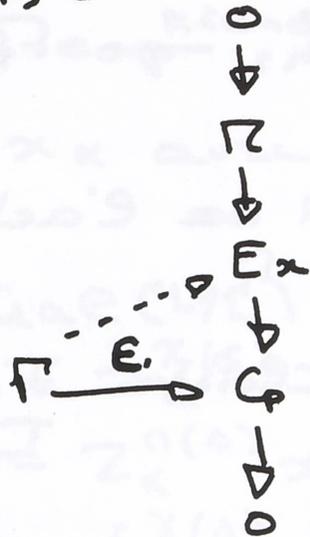
(i.e. $p^\nu z = 0$ pour ν assez grand).

Dc: si e act⁰ est triviale, rien n'est négligeable à part 0.

Par contre \mathbb{Z} de type (p, p) , σ_p agissant par $\begin{pmatrix} 1 & \\ 0 & 1 \end{pmatrix} \rightarrow H^2(\mathbb{C}_p, \mathbb{Z}) \neq 0$ mais nég.

Principe de la dém. du cor 3 :

$$x \in H^2(\mathbb{C}_p, \mathbb{Z})$$



E doit se relever. le relèvement est dét. par les images de σ et τ . la relation imposée à σ et τ donne γ et δ .

Dém. du thm :

② On veut de construire un corps k , avec $\Gamma_k \cong \Gamma$.

Soit k_1 un sous corps de $\overline{\mathbb{Q}}$ contenant

\mathbb{F}_p tel $\chi_p : \Gamma_{k_1} \rightarrow \mathcal{U}_p$ soit un isom.

$$\Gamma_{k_1} \xrightarrow{\sim} \mathcal{U}_p'$$

Un tel corps existe :

$$\chi_p : \Gamma_{k_1} \rightarrow \mathcal{U}_p$$

$$\begin{array}{ccc}
 S & \rightarrow & \mathcal{U}_p' \\
 (pS \in \mathbb{N}) & & pS \in \mathbb{N} \\
 & & \mathbb{Z}
 \end{array}$$

$$\mathbb{Z}_p \subset S \rightarrow \mathbb{Z}_p \text{ fibres}$$

\mathbb{Z}_p correspond de à un sous corps de $\overline{\mathbb{Q}}$. C'est celui qu'on veut.

Posons $h_2 = h_1((T))$.

Γ_{h_2} .

$$1 \rightarrow \varprojlim_n M_n \rightarrow \Gamma_{h_2} \rightarrow \Gamma_{h_1} \rightarrow 1$$

$$\cong \prod_e \mathbb{Z}_e(1)$$

) muni de l'action naturelle de Γ_{h_1} .

$$h = \bigcup_{(m,p)=1} h_2(T^{1/m}) \quad (\text{choisir } T = T_m^3, T_m = T_{m^2}).$$

$$D_0: 1 \rightarrow \mathbb{Z}_p \rightarrow \Gamma_h \rightarrow \mathbb{Z}_p' \rightarrow 1. \quad \text{cfd.}$$

Reste à montrer que Γ a la propriété de relèvement. Il suffit de le faire en cas.

On suppose $h \ni \sqrt{1}$.

L cyclique de $d^o p$.

z , racine primitive p -ième de 1.

$$L = h(\sqrt{x}), x \in h^*$$

$$\text{Act}^o: \sqrt{x} \mapsto z, \sqrt{x}.$$

Relèvement $\Gamma_h \rightarrow \Gamma$ revient à trouver un ext. gae. de h de type de gae. se plonge dans h .

(17)

On adjoit à k toutes les racines p^x ièmes de 1 et de x .

z_α racine p^{α} ième de 1 tq $z_\alpha^p = z_{\alpha-1}$.

De n x_α avec $\begin{cases} x_1^p = x \text{ donné} \\ x_\alpha^p = x_{\alpha-1} \end{cases}$

Si $\sigma \in \text{Gal}(L/k)$:

$$\sigma(z_\alpha) = z_\alpha^{\chi(\sigma)} \quad \chi(\sigma) \in \mathbb{Z}_p^\times$$

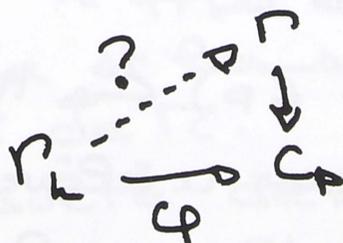
$$\sigma(x_\alpha) = z_\alpha^{n(\sigma)} x_\alpha$$

$$\text{Si } \sigma \mapsto \begin{pmatrix} \chi(\sigma) & n(\sigma) \\ 0 & 1 \end{pmatrix}$$

On obtient un plongement $\text{Gal} \hookrightarrow \Gamma$

Qd $L \not\cong \mathbb{F}_p^\Gamma$ (cas général)

Si $k' = L(\mathbb{F}_p^\Gamma) \cong \mathbb{F}_p^\Gamma$ $[\mathbb{F}_p^\Gamma : \mathbb{F}_p]$ est d'ordre premier à p .

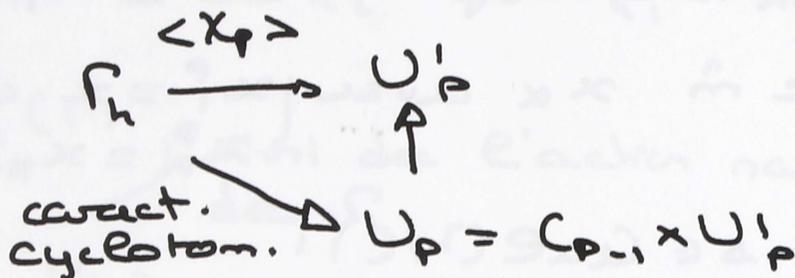


En fait, grâce à la dén. précédente, si on regarde

$$\begin{array}{ccccccc} 1 & \rightarrow & \mathbb{F}_p^\Gamma & \rightarrow & \mathbb{F}_p \times \mathbb{Z}_p^\times & \rightarrow & 1 \\ & & (x, y) & \mapsto & (x \bmod p, y) & & \end{array}$$

l'extension est décrite par un élém^t de $H^2_{\text{cont}}(C_p \times U_p', p\mathbb{Z}_p)$.

De plus



$$\Gamma_h \longrightarrow C_p \times \mathcal{U}_p'$$

$$\psi = (\varphi, \langle X_p \rangle).$$

On a démontré $\psi^{-1}(C_p \times \mathcal{U}_p')$ est une extension scindée si $h \ni \sqrt{p}$.

La $u \in H^2_{\text{cont}}(C_p \times U_p', p\mathbb{Z}_p)$.

$\psi^* u = 0$ ds $H^2_{\text{cont}}(\Gamma_h, p\mathbb{Z}_p)$ si $h \ni \sqrt{p}$.

On invoque cores $(\Gamma_h: \Gamma_{h'})$ premier à p

$$\Rightarrow H^2_{\text{cont}}(\Gamma_h, \mathbb{Z}_p) \hookrightarrow H^2_{\text{cont}}(\Gamma_{h'}, \mathbb{Z}_p).$$

(vrai; démontré par un élém^t de Leuzra).

Ceci permet de conclure.

Pb: C_{p^2} ??

On n'a pas de $\Gamma \rightarrow C_{p^2}$ qui soit

- } relèvement
- } gpe de gal. ab. d'un corp.

V. ①

Quelques commentaires sur le cours précédent:

① U Janssen:

Soit h un c. de nombres totalement imag.,
et K une ext. de h de deg. de tr. d .

$\Gamma_K = \text{Gal}(K/h)$. Alors $\text{scd}(K) \leq d+2$.

($\text{cd}(K) \leq d+2$ était déjà connu.

Il y a égalité si K/h de t. fini).

(Cela revient à dire que $H^{d+2}(K, \mathbb{Q}/\mathbb{Z}) = 0$.)

② On a montré que (G fini)

si \mathbb{Z} est un G module, à action triviale,
et si \mathbb{Z} est de t. fini sur \mathbb{Z} ,
alors 0 est le seul zét nég. de
 $H^2(G, \mathbb{Z})$.

En fait l'hypothèse " \mathbb{Z} de t. fini"

est inutile.

En effet $H^i(G, \mathbb{Z}) = \varinjlim H^i(G, \mathbb{Z}_n)$,

où les \mathbb{Z}_n sont les sous $\mathbb{Z}[G]$ modules
de t. fini de \mathbb{Z} .

(Cela résulte de l'existence
d'objets usuels. $\Gamma_K \rightarrow G$).

③ Colom. de $G = Q_8$ gr. des quat.
d'ordre 8.

en fait, ce n'est
pas (encore) démontré

$H^i(G) \text{ mod. } 2$ a été mal décrit

$i =$	0	1	2	3
dim	1	2	2	1
base	1	x, y	x^2, y^2	$x^2y = xy^2$ $x^3 = y^3 = 0$

à effet: $x^2 + xy + y^2 = 0$ (1)

$$x^3 + x^2y + xy^2 = 0$$

$$x^2y + xy^2 + y^3 = 0.$$

On applique à (1) $x^2y + xy^2 = 0$.

$$\text{Dc } x^3 = y^3 = 0.$$

On va mg x^2y et xy^2 .

$$h: \Gamma_h \rightarrow G$$

x et y donnent $x_h \in H^1(L)$.

$$\text{Puis } x_h^2 = (-1)x_h.$$

$$\text{Dc } (-1)x_h + x_h y_h^2 (-1)y_h = 0.$$

$$\text{Dc } \underbrace{(-1)(-1)x_h}_{x_h^3} + \underbrace{(-1)x_h y_h^2}_{x_h^2 y_h} + \underbrace{(-1)(-1)y_h}_{y_h^3} = 0.$$

$$\text{Puis } = x_h^3 = x_h^2 y_h = y_h^3.$$

$$\text{Dc } (x_h^3 = y_h^3 = 0) \quad x_h^2 y_h = 0$$

et x^2y est bien mg .

Invariants cohomologiques attachés à des G torsseurs.

On a un corps de base k_0 .
(e.g. $k_0 = \mathbb{Q}$).

G est un gpe alg. lin. sur k_0 .

(e.g. $G = G_2$; $G = E_8$?; G fini.

En part., on va étudier le cas $G = S_n$).

k est une extension de k_0 . G définit

un gpe sur k . On s'intéresse aux

G torsseurs sur k . On notera

$P(G, k) =$ classes d'isom. de tels torsseurs.

||

$H^1(k, G)$.

Cas particuliers intéressants:

si $G = G_2$ $P(G, k) =$ classes d'algèbres
d'octonions sur k .

si $G = F_4$ $P(G, k) =$ classes d'algèbres
de Jordan excep. de dim 27.

si $G = E_8$? $P(G, k) =$ classes de
 k formes de E_8 .
e car. o : classes d'alg.
de Lie de type E_8 .

Si $G = S_n$ $P(G, k) =$ classes d'isom.
d'algèbres étalées sur k de
rang n .

Invariants cohomologiques :

On fixe un Γ_{h_0} -module C .

On suppose que C est fini, et
d'ordre premier à la caract.

(i.e. C est un q -gpe abélien fini
sur lequel Γ_{h_0} opère continuellement).

Exple: $\mu_n^{\otimes i}$, n premier à la caract.

$$C/h = C. \quad H^i(h, C).$$

Un invariant cohom. pour G de
type (i, C) est une règle qui
associe à tout torsion T sur G ,
déf/h un $\tilde{a}(T) \in H^i(h, C)$,
avec axiomes (1) et (2).

C'est de la donnée pour tout h/h_0
d'une app $a: P(G, h) \rightarrow H^i(h, C)$
avec (1) et (2).

(1) dit que si on a un homomorphisme
 $h \rightarrow h'$

$$\begin{array}{ccc} P(G, h) & \longrightarrow & P(G, h') \\ \downarrow a & \hookrightarrow & \downarrow a \\ H^i(h, C) & \longrightarrow & H^i(h', C) \end{array}$$

En g^{al}, cette axiome (1) suffit.
 Pour pouvoir spécialiser, on impose
 aussi :

(2) On se donne K ext. de k_0 muni
 d'une val. discrète v triviale sur k_0 .
 $R =$ anneau de valuation, $k_0 \subset R$.
 k corps résiduel.
 $k_0 \rightarrow R \rightarrow k$. k est une k_0 algèbre.
 On suppose K est complet.

Soit T un G torsueur sur $\text{Spec } R$.

$R \rightarrow k$ $\hookrightarrow K$ De sorte T_h G torsueurs sur k
 $\rightarrow K$ T_K

(Situation de "bonne réduction").

$$a(T_h) \in H^i(k, C).$$

$$a(T_K) \in H^i(K, C).$$

Axiome (2) $H^i(k, C) \xrightarrow{\varepsilon} H^i(K, C)$
 envoie $a(T_h)$ sur $a(T_K)$

Il vient de l'existence d'une
flèche $\Gamma_K \rightarrow \Gamma_h$. E est inj.

Rappel: $\Gamma_K \rightarrow \Gamma_h$ est surjective.
 E est également scindée.

(L'image de $H^i(h, C)$ est
facteur direct de $H^i(K, C)$).

Un cas où (2) résulte de (1).

On sait (Bourbaki AC IX) que
l'on peut relever h de R :

il existe $h \rightarrow R$ tq $h \rightarrow R \rightarrow h$ est
l'identité.

(Vrai pour t anneau noeth. complet
en égale caract.).

$$\begin{array}{ccc} R_{\text{cis}} & h_0 & \rightarrow R \\ & \searrow & \downarrow \\ & & h \end{array}$$

(*) | Supposons que le relèvement de
h prolonge celui de h_0

(*) est vérifiée e car 0 (Bourbaki).

En corp, si h est un ext. sép.
de t. finie de h_0 , alors (*) est
vérifiée.

[mod. EGA O_{1v} ? k_0 parfait
suffit].

Avec ces hyp., (2) résulte de (1).

En effet:

T torseur sur R .

Soit T' le torseur sur R déduit
de T_h par le plongement $\varphi: h \rightarrow R$.

En fait $T' \cong T$, car ce sont deux torseurs
sur R qui ont même réduction mod. e id.
max.

[et G -lisse-Hensel:

Torseurs sur $R \leftrightarrow$ torseurs sur k].

De $T/h \quad T/R \cong T, \quad T_k$.

$a(T_h) = a(T_k)$ résulte maintenant
du critère de base pour $h \rightarrow k$.

De sur un corps parfait, et a car,
axiome (2) ne sert à rien.

Notation pour les inv. cohom.
d'un type donné: $A(G, k_0, i, c)$.

Pb: calculer explicitement ?
 $A(G, h_0, i, C)$

Invariant est:

On se donne $\kappa \in H^i(h_0, C)$.

$\forall h$, on en déduit $\kappa_h \in H^i(h, C)$.

$a(T) = \kappa_h$ qq soit $T \in P(G, h)$.

On note $A_{\text{cst}}(G, h_0, i, C)$ {inv. csts}.

$H^i(h_0, C)$.

Inv. normalisé: $a(T) = 0$ si T est trivial.

A_0 ss qpe des inv. norm.

On a $A = A_{\text{cst}} \oplus A_0$.

Un expe: (dpdt de $j = 1, 2, 3$).

- (1) $G = C_2$ qpe cycle d'ordre 2
- (2) $G = PGL_2$ quotient de GL_2 /centre
- (3) $G = G_2$ déployé.

$C = \mathbb{Z}/2\mathbb{Z}$. On note $H^i(h) = H^i(h, \mathbb{Z}/2\mathbb{Z})$.

car $h_0 \neq 2$. i qcqr.

De chacun de ces cas, il existe un $a_i \in A(G, h_0, i, c)$ canonique.

(1) C_2 torseur \rightarrow ext. quad. de k
 \leftrightarrow Rom. continus Γ_k de $\mathbb{Z}/2\mathbb{Z}$
 \parallel
 $H^1(k).$

$$k[x] / x^2 - \alpha \longmapsto (\alpha) \in H^1(k).$$

Donne un a_1 à val. de H^1 .

(2) PU_2 torseur \rightarrow alg. de quat. / k

$$\begin{cases} i^2 = \alpha \\ j^2 = \beta \\ ij = -ji \end{cases}$$

alg. de quat $(\alpha, \beta) \mapsto (\alpha)(\beta) \in H^2(k).$

a_2 à val. de $H^2(k).$

(3) G_2 torseur \rightarrow octonions.

inv. de à Arason

$(\alpha, \beta, \gamma) \mapsto (\alpha)(\beta)(\gamma) \in H^3(k).$

a_3 à val. de $H^3(k).$

Thm: De ces 3 cas, et inv. cohom.
 $\in A(G, h_0, i, \mathbb{Z}/2\mathbb{Z})$ s'écrit de façon !
 $a = x_0 + (x_1, x_{a_i})$
 $x_0 \in H^i(h_0); x_1 \in H^{i-1}(h_0).$

Et d'autres termes :

$$A(G, h_0) := \bigoplus_{i=0}^{\infty} A(G, h_0, i, \mathbb{Z}/2\mathbb{Z}).$$

$A(G, h_0)$ est un $H^*(h_0)$ module libre, de base $(1, a_i)$.

Cor. Et inv. normalisé est un multiple de l'invariant fondamental a_i (a_i val. de H^i).

Rqrs

1) En part., on a $a_i^2 = x_0 + x_1 a_i$.

Cela donne

$$a_i^2 = \varepsilon^i a_i \quad \varepsilon^i = (-1)^i \in H^1(h_0).$$

2) Oct $\xrightarrow{\sim}$ 3-f. de Pfister C_0 est de $H^3(h)$
 \uparrow
 Rehurjer sur lin.

$H^1(h, G_2) =$ ss. ens. de $H^3(h)$ formé des états décomposables (au sens strict).

3) On pourrait étudier des inv. corom. associés aux r formes de Pfister. La dén. qui suit s'applique.

4) Cas de F_4 (déployé).

inv. cor. mod. 2

On trouve dx inv. $\begin{cases} a_3 \in H^3(k) \\ a_5 \in H^5(k) \end{cases}$

qui a fait a_5 $\left\{ \begin{matrix} 3 \\ 5 \end{matrix} \right.$ formes de Pfister.

On peut mg inv. cor. de F_4 mod. 2
former un mod. fibre de base
 $1, a_3, a_5$.

inv. cor. mod. 3

" $M_3^{\otimes 2}$ N.B.

inv (Rost) $\in H^3(k, \mathbb{Z}/3\mathbb{Z})$.

\vec{n} genre de résultat.

(N.B.: Conjecturalement

$H^i(k, M_n^{\otimes(i-1)}) \xrightarrow{\text{inj?}} H^i(k, M_{nm}^{\otimes(i-1)})$).

Pb. Un torsion sous F_4 est-il
déterminé par ses deux inv. mod. 2
et son inv. mod. 3?

5] Pb. Y a-t-il un inv. cor. pour E_8
norm., non identiquement nul, et
valeurs de $H^3(k, \mathbb{Z}/2\mathbb{Z})$? (Oui, Rost?).

On va maintenant démontrer le thm.

On se place (p.ex.) ds le cas $i=2$.

$PGL_2 \rightarrow \text{alg. de quaternions}$.

h_0 est fixé.

$h = h_0(x, Y)$ x et Y indéterminées.

Alg. de quat. $i^2 = X; j^2 = Y; ij = -ji$.

$a(T) \in H^0(h) = H^0(h_0(x, Y), \mathbb{Z}/2\mathbb{Z})$.

1^{er} étape Soit $a \in A$.

mq $a(T) = x_0 + x_1(x) + x_2(Y) + x_3(X)(Y)$

avec $x_i \in H^0(h_0)$;

écriture unique.

$(x) = \bar{e}$ et de $H^1(h)$ déf. par $X \dots$.

Raison: cette classe de cohom. n'a pas de pôles sur l'esp. affine A^2 et de lors de $X=0$ et $Y=0$.

2^{de} étape:

En fait $x_1 = 0; x_2 = 0$.

3^{eme} étape: Si $a(T) = 0$, alors $a = 0$.

Alors le thm est évident:

$a' := x_0 + x_3 \cdot a_2$

$a - a'(T) = 0$ par construction.

De $a = a'$.

Détails1^{ere} étape:

k corps; v valuation discrète, égale car.
 $x \in H^0(k)$.

On dit que x est hol. en v si :

\hat{h}_v complète; \tilde{h}_v corps résiduel.

$x_v \in H^0(\tilde{h}_v) \subset H^0(\hat{h}_v)$.

On définit alors le résidu de x en v :

$x \in H^i(\hat{h}_v) \xrightarrow{\text{res}_v} H^{i-1}(\tilde{h}_v)$.

Axiome (2) \Rightarrow si X est un div. irred.

de \mathbb{A}^2 distinct de $X=0$ et $Y=0$,

$a(T)$ est hol. en la v.d. associée à X .

Autre méthode (qui n'utilise pas axiome (2)).

$k_0 \infty$.

$\mathbb{A}^2 \quad X, Y \xrightarrow{\sigma_{d,\mu}} d^2 X, \mu^2 Y \quad d, \mu \in k_0^*$.

Le torseur est inv. par $\sigma_{d,\mu}$.

De $a(T)$ _____ :

{Pôles de $a(T)$ } _____ :

Comme il n'y a qu'un nbre

fini de pôles, on obtient

$X=0$ et $Y=0$ st les seuls.

Il manque la page V-14 dans le document original.

2^{de} étape

$$a(\tau) = x_0 + x_1(x) + x_2(y) + x_3(x)(y).$$

$$\text{mg } x_1 = x_2 = 0.$$

On peut supposer $a_0 = 0$, i.e.
a normalisé.

$$\begin{array}{ccc} h(x^{1/2}, y) & 0 & \text{(Ajouter } \Gamma \text{ sur} \\ & \uparrow & \text{l'alg. de} \\ & & \text{quaternions).} \\ h(x, y) & a(\tau) & \end{array}$$

Mais l'image de $a(\tau)$ est $x_2(y)$.

De $x_2(y) = 0$ ds $h(x^{1/2}, y)$.

Par le résidu, on a déduit $x_2 = 0$.

3^{eme} étape: $a(\tau) = 0 \Rightarrow a = 0$.

(spécialisation).

Soit $T_{\alpha, \beta}$ alg. de quat. sur un corps
 $k \supset k_0$ déf. par $\alpha, \beta \in k^*$.

$$a(T_{\alpha, \beta}) \stackrel{?}{=} 0.$$

$$k_1 = k(x, y) \quad T_{x, y} \text{ sur } k_1.$$

$$a(T_{x, y}) = 0 \text{ car } a(\tau) = 0.$$

Lemme: Soit R un alg. locale régulière sur k_0 , de corps résiduel k .
 Soit U un \mathcal{O} -torseur sur $\text{Spec}(R)$.
 $K = \text{Fr}(R)$. U_k, U_K les toseurs correspondants.
 Si $a(U_K) = 0$, alors $a(U_k) = 0$.

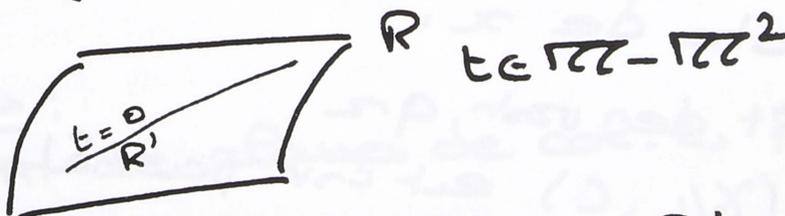
Ceci résulte de l'axiome (2).

Si $\dim R = 0$, $k = K$ clair.

Si $\dim R = 1$, R ord. o.p.s. R complets, et axiome (1) s'applique. et K

$$a(U_k) = a(U_K) = 0.$$

Cas g \in : récurrence.



$K' = \text{corp. des fct. sur } R' = R/tR$.

$a(U_{R'}) = 0$ par spécialisation $K \rightarrow K'$.

Puis (hyp. de réc.): id. sur k .

N.B.: En fait, on pourrait faire cela sans l'axiome (2).

Un procédé de construction d'inv.

com. pour G qcz:

$G \subset H = SL_N$ N convenable

$X = H/G$ esp. hom.

$x \in H_{\text{ét}}^i(X, \mathbb{C})$ \mathbb{C} coef.

T torsueur sous G déf. / k .

IE est obtenu à partir d'un pt h rat.

$x \in X$, défini à conj. près par l'action de $SL_N(k)$.

$\varphi_x: \text{Spec } k \rightarrow X$.

$\alpha_x(T) = \varphi_x^*(U)$.

Thm: cette classe de cohom. est indépendante de x .

(IE suffit de voir qz

$U_h \in H_{\text{ét}}^i(X/h, \mathbb{C})$ est inv. par $SL_N(k)$.)

Preuve: Quitte à lui ajouter un ind. ops $h \rightarrow \infty$.
hs clôtures sêp. $H^0(X/h_s, \mathbb{C})$.

Γ_h opér:

$H^0(\Gamma_h, \underbrace{H^0(X/h_s, \mathbb{C})}_{\text{gpes finis}}) \Rightarrow H_{\text{ét}}^i(X, \mathbb{C})$.

gpes finis.

L'action de $SL_N(k)$ dessus
est triviale.

Lemme: Soit $0 = A_0 \subset A_1 \dots \subset A_n = A$
une filtration d'un gpe ab. A .

Les aut. de A qui respectent la
filtration, et agissent trivialement
sur $g = A = \bigoplus A_i/A_{i-1}$ est un gpe
nilpotent.

↳ L'image de $SL_N(k)$ ds $\text{Aut}(H_{\text{ét}}^i(X, \mathbb{C}))$
est un gpe nilpotent.

⇒ cette $SL_N(k)$ triviale.

Les axiomes st faciles à vérifier.

ARou:

Partir de classes de col. ds $H_{\text{ét}}^0(X, \mathbb{C})$.

↳ expe

$u \in H_{\text{ét}}^2(X, \mathbb{M}_5^{\otimes 2})$. $G = E_8 \hookrightarrow SL_{248}$

→ cl. fondamentale de $H^3(SL_N)$.

déf. op. colon. à val. dans

$H^3(k, \mathbb{M}_5^{\otimes 2})$.

(?) $a \neq 0$.

J.P. Serre VI
 Cours au collège
 de France.
 Le 15 novembre 93

VI-①

Retour sur le dernier cours.

Exemple concret de construction d'invariant.

$$G = G_2 \subset SL_7 = S$$

$$G = E_8 \subset SL_{248} = S$$

On se place sur le corps \mathbb{C}

$$X = S/G.$$

$$\pi_1 = \pi_2 = 0; \begin{cases} \pi_3(G) \cong \mathbb{Z} \\ \pi_3(S) \cong \mathbb{Z}. \end{cases}$$

$$d \begin{cases} \mathbb{Z} \rightarrow \mathbb{Z} \rightarrow \pi_3(X) \rightarrow 0 \\ \pi_1(X) = \pi_2(X) = 0. \end{cases}$$

$$\pi_3(X) = \mathbb{Z}/d\mathbb{Z} \quad (\text{on peut montrer facilement } d \neq 0).$$

1^{er} cas: $d = 2$.

2nd cas: sauf erreur, $d = 60 = 2^2 \cdot 3 \cdot 5$
 ↑
 nbre de Coxeter de E_8 .

De pour G_2 on calcule mod. 2

$$H^3(X, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}.$$

pour E_8 $60 = 4 \times 3 \times 5$ $H^3(X, \mathbb{Z}/4\mathbb{Z})$ cycl. d'ordre

$$- (\quad, \mathbb{Z}/3\mathbb{Z})$$

$$- (\quad, \mathbb{Z}/5\mathbb{Z})$$

le 15.11.93

(2)

Preons pour $k = k(V)$, V variété complexe
Quitte à restreindre V , on a un G torsion sur k et un G fibré principal sur V
qui devient trivial sur S .

Ce fibré provient d'une pléiade $V \xrightarrow{f} X$ S/G
 $u \in H^3(X, \mathbb{Z}/d\mathbb{Z})$

On attache au fibré

$$f^* u \in H^3(V, \mathbb{Z}/d\mathbb{Z}) \rightarrow H^3(k, \mathbb{Z}/d\mathbb{Z}).$$

Cas G_2 : On retrouve l'invariant
d'Arason défini la dernière fois.

(Comment le prouver ??)

[En prenant $V = \text{Aff}^3$ - plans coord.
i.e. $\{(x_1, x_2, x_3) \mid x_i \neq 0\}$.

Torsion versée par G_2

\Leftrightarrow octonions avec $e_i^2 = x_i \quad i=1,2,3$.

$$V = G_m^3 \xrightarrow{f} X$$

(f obtenu à partir de

$$G_m^3 \rightarrow S$$

$$\downarrow^2$$

$$G_m^3 \rightarrow X$$

)

$$S_1 \times S_1 \times S_1 \rightarrow X.$$

Il faudrait que la classe de
coker. de X donne bien la classe
fond. dans $S_1 \times S_1 \times S_1$.]

Autre complément:

On a déf. des inv. colom.

G-torseur \mapsto coh. $H^i(h, C)$.

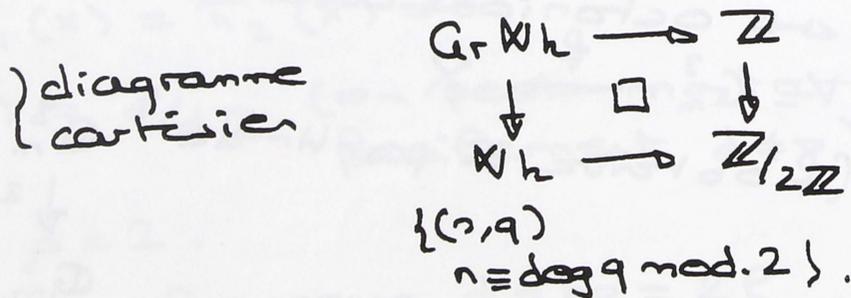
On peut aussi regarder des invariants

G-torseur \mapsto | gpe de Witt de k
 $| K_i(h) / m K_i(h)$.

Pour gpe de Witt : on suppose $\text{car } k \neq 2$.

W_k anneau de Witt
 = classes de p.q. (p. hyp. $\rightarrow 0$
 i.e. $\langle 1, -1 \rangle = 0$ ds W_k).

Parfois, on travaille sur le groupe
 de Witt-Grothendieck $Gr W_k$



Plus tard, nous regarderons les opérations
 Or elles ne st pas définies sur W_k .
 Par contre, elles le st sur $Gr W_k$.

"Bonne réduction" : si k complet, val. dis.,
 corps résiduel \tilde{k} de $\text{car} \neq 2$,

On a

$$0 \rightarrow Gr W_{\tilde{k}} \rightarrow Gr W_k \xrightarrow{\partial \pi} W_{\tilde{k}} \rightarrow 0.$$

$\langle x_1, \dots, x_n \rangle \mapsto \langle \bar{x}_1, \dots, \bar{x}_n \rangle$.
 $\bar{x}_i \in$ anneau de val., associé à x_i .
 vu co gpe
 additif.

On peut choisir n'importe quel représentant $x_i \rightarrow \bar{x}_i$.

Par contre, ∂_π dpd du choix de e uniformisante :

$$q = \langle \alpha_1, \dots, \alpha_n, \pi \beta_1, \dots, \pi \beta_m \rangle \quad \pi \text{ u.i.p.}$$

$x_i, \beta_j \text{ u.i.v.}$

$$\downarrow$$

$$\langle \tilde{\alpha}_1, \dots, \tilde{\alpha}_n \rangle = \partial_\pi q.$$

[EEEE est bien à valeurs ds \mathbb{N}_h^2 , car

$$q = \langle \pi x, -\pi x \rangle \quad \partial_\pi q = \langle \tilde{x}, -\tilde{x} \rangle.$$

Or $q \approx \langle 1, -1 \rangle$. De il faut que $\langle \tilde{x}, -\tilde{x} \rangle$ soit nul.]

On peut définir un résidu qui ne dpde pas du choix d'une u.i.p. :

$$V = m/m^2 \cdot v^* \text{ est un } \mathbb{N}_h^* \text{-tenseur.}$$

Or \mathbb{N}_h^* opère sur \mathbb{N}_h^2 . De on peut border

\mathbb{N}_h^2 par le tenseur en question.

La fournit un opérateur à val. ds \mathbb{N}_h^2 .

Opération à val. ds $\mathbb{A}r\mathbb{N}$

C'est la donnée pour tout G tenseur T sur $h \rightarrow h_0$ d'un $\tilde{e} \in \mathbb{E}^+$ $a(T) \in \mathbb{A}r\mathbb{N}(h)$ avec les axiomes (1) et (2)

- (1) $h \rightarrow h'$
- (2) val. discrète d'égalité car.

{ Travailler ds $\mathbb{A}r\mathbb{N}$ est plus précis que coh. mod. 2 et permet d'utiliser les ep. d.

Exemple: $G = G_2$ déployé.

G_2 torseur \Leftrightarrow alg. d'octonions.

↓
f. trace 3 forme de Pfister q

De à H torseur T on peut associer $q_T := a(T)$

PRM. Toute GrW opération sur les G_2 torseurs s'écrit de façon unique

$$T \mapsto q_0 + q_1 \otimes a(T)$$

avec $q_0, q_1 \in \text{GrW h.o.}$

Exple (cf. cours précédents)

$T \mapsto$ forme de G_2 : G_2^T

Killing $q(G_2^T) = b(T)$ de $\mathfrak{g} \mathfrak{h}$.

On a

$$Killing q(G_2^T) = \langle -1, -3 \rangle \otimes (a(T) - \langle 1 \rangle).$$

ie. $q_0 = -\langle -1, -3 \rangle$ et $q_1 = \langle -1, -3 \rangle$.

sur \mathbb{R} f compacte $a(T) = \langle 1, \dots, 1 \rangle = 8$.

la démonstration est essentiellement la même que celle de la dernière fois:

On choisit $h = h_0(x, y, z)$ } T^{ver} / h .
Octonion $e_1^2 = x, \dots, e_3^2 = z$

$a(T^{\text{ver}}) \in \text{GrW } h$.

le 15.11.93

⑥

Cet \mathbb{Z}^3 a bonne réduction sur l'esp. affine à 3 dim. privé de $\begin{cases} x=0 \\ y=0 \\ z=0. \end{cases}$

(bonne réduction pour les val. d. attachées aux div. irréd.)

Puis, avec des suites exactes de Néron :

Les \mathbb{Z}^3 de $\text{Gr}(\mathcal{O}_h)$ ayant bonne réduction ont co base

$\langle 1 \rangle, \langle x \rangle, \langle y \rangle, \langle z \rangle, \langle xy \rangle, \dots, \langle xyz \rangle$.

$$D_{\mathbb{Z}^3} a(T^{(v)}) = d_0 + d_1 \langle x \rangle + d_2 \langle y \rangle + d_3 \langle z \rangle + d_4 \langle xy \rangle + d_5 \langle xz \rangle + d_6 \langle yz \rangle + d_7 \langle xyz \rangle$$

Ici, $a_0 = \langle 1, x, xy, \dots, xyz \rangle$.

On veut mg ts les d_i st égaux (sf d_0).

En fait :

si l'on remplace x par -1 , alors $a(T)$ devient hyperbolique, et ne dépend pas de y et z .

$$D_{\mathbb{Z}^3} a(T) = d_0 + d_1 \langle -1 \rangle + d_2 \langle y \rangle + d_3 \langle z \rangle + d_4 \langle -y \rangle + d_5 \langle -z \rangle + d_6 \langle yz \rangle + d_7 \langle -yz \rangle$$

donne :

En fait on travaille de \mathbb{Z}^3

$$\begin{aligned} \hookrightarrow d_2 &= d_4 \\ d_3 &= d_5 \\ d_6 &= d_7 \dots \end{aligned}$$

Une fois qu'on a le cas vu, on spécialise.

le 15.11.93

VI-7

Opérations sur
les n.f. de Pfister

$\rightarrow \mathbb{N}, \mathbb{Q}, \mathbb{N}$

p.ex.: si q est une n forme de Pfister

$$d^i q = a \oplus b q \quad | a, b \in \mathbb{Z} \\ | a, b \text{ dpt de } i \text{ et de } n$$

Invariants { corom. du groupe S_n
Nitt

Dictionnaire:

Torseurs sous $S_n \iff$ algèbres étales de deg. n

si S est un schéma

$X \rightarrow S$ fini, étale,
partout de d^n .

$\iff S_n$ torseurs
sur S .

$\downarrow \pi$
 S

($\pi_* \mathcal{O}_X$ est loc. libre)
de \mathbb{Z}^n

\implies :

si $X \rightarrow S$, on forme le produit

$$X_S^n = X \times_S \dots \times_S X \quad (n \text{ fois}).$$

"fat diagonale"

Δ_n formé des pts ayant au moins
deux coordonnées égales, $\Delta_n = \cup \Delta_{i,j}$

$$T_X = X^n - \Delta_n.$$

S_n agit librement sur T_X .

T_X est bien un torsueur: on le vérifie qd $X = S \cup S \cup \dots \cup S$ (n fois).

\Leftarrow : si T est un S_n torsueur,

on lui associe $X = T/S_{n-1}$, qui a

les vertus voulues.

\uparrow
 S_{n-1} = fixateur
 de $n \in [1, n]$.

Si I fini à $n \in \mathbb{Z}^+$; $S_I = \text{Sym}(I)$

$X \mapsto$ torsueur sous S_I $X^I - \Delta$.

\triangleleft regarde $S \times I$
 \downarrow
 S

Cas des corps: si $S = \text{Spec } k$

S_n torsueur sur $k \iff k$ algèbre étale L de $\text{rg } n$.

$L = \prod k_i$ k_i/k sép.
 et $\sum [k_i:k] = n$.

k_0 corps de base.

$C \Gamma_{k_0}$ module fini, d'ordre premier à la caract.

i.

S_n torsion sur $h \supset h_0 \mapsto H^i(h, C)$.

i.e. $L \mapsto a(L) \in H^i(h, C)$.

Théorème 1: Supposons que $a(L) = 0$ pour tout L/h tq $L \cong \prod L_i$ avec $[L_i: h] = 1$ ou 2 . Alors $a = 0$.

Théorème 2: Supposons a normalisé. (i.e. $a(L) = 0$ si $L = h \times \dots \times h$). Alors $2a = 0$.

Thm 1 \Rightarrow Thm 2:

Preuve: Soit a normalisé.

On veut mq $2a(L) = 0 \forall L$.

Grâce au thm 1, il suffit de le voir qd $L = L_1 \times \dots \times L_m$ avec $\deg L_i = 1, 2$.

Récurrence sur le nbre r de fact. de deg. 2.

$r=0$ $L \cong h \times \dots \times h$ $\left. \begin{array}{l} \\ a \text{ normalisé} \end{array} \right\} \Rightarrow a(L) = 0$.

On peut supposer $\left. \begin{array}{l} L_1, \dots, L_r \text{ de deg. 2} \\ L_i = h \quad i > r. \end{array} \right\}$

15.11.93

VI- (10)

On peut aussi supposer

que L est un corps. Sinon
Hyp. de réc. marche.

Soit h' ce corps. $[h':h] = 2$.

Soit

$$L' = L_1 \times \dots \times L_{r-1} \times \underbrace{h \times h}_h \times h \times \dots \times h$$

$2a(L') = 0$, par Hyp. de réc.

De plus L et L' deviennent isom.
après ext. des scalaires à h' . De
leurs invariants sur h' suit $2a(L) = 0$.

i.e.

$a(L) - a(L')$ est triviale par l'ext. h'/h .

Mais h'/h de degré 2.

De (argument de Coroll. Habituel:

$$\text{Cor } (a(L)/h' - a(L')/h') = 0)$$

$$2(a(L) - a(L')) = 0.$$

$$\text{A } 2a(L) = 2a(L') = 0.$$

Q.F.D.

La dém. du Thm 1 utilise l'algèbre
verselle. Récurrence sur n .

Cas versel: n degré fixé

$$h = k_0(A_1, \dots, A_n) \quad A_i \text{ indéterminées.}$$

$$L^{\text{ver}} = k[x] / P_n(x), \quad P_n = x^n + A_1 x^{n-1} + \dots + A_n$$

L^{vo} est étale de $\text{rg } n$.
(C'est \hat{n} un corps).

Regardons $a \in (L^{\text{vo}}) \in H^i(k, \mathbb{C})$.

Assertion: la classe a n'a pas de pôles sur APP^n .

\mathcal{W} div. irred. de APP^n .



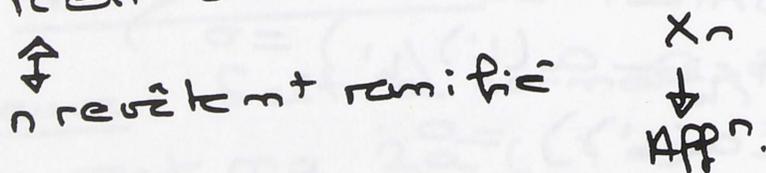
On veut montrer que $a \in (L^{\text{vo}})$ n'a pas de pôles sur \mathcal{W} .

Mais P_n définit une algèbre

$$\Gamma = k_0[A_1, \dots, A_n, X] / (P_n).$$

Si $S = k_0[A_1, \dots, A_n] = \text{alg. affine de } \text{APP}^n$.

Γ est une S -alg. libre de base $1, X, \dots, X^{n-1}$.



Si Δ est le pol. discriminant, $\Delta(A_1, \dots, A_n)$.

X_n est non ramifié en dehors de $\Delta=0$.

- } Δ est irred. en $\text{car} \neq 2$
- { Δ est le carré d'un pol. irred. en $\text{car } 2$.

La classe $a \in (L^{\text{vo}})$ n'a pas de pôles sur \mathcal{W} se décompose en

- { (1) pas de pôles si $\mathcal{W} \neq (\Delta=0)$.
- { (2) _____ $\mathcal{W} = (\Delta=0)$.

(1) est une conséquence de l'axiome
(2) des invariants cohomologiques.

Pour montrer (2), on va utiliser
l'exp. $a(L) = 0$ si L est produit
d'alg. de dim. ≤ 2 .

Le o.p.s. thm 1 vrai a deg. $< n$.

Prop.: Soit $k \supset k_0$ muni d'une val. disc.
triviale sur k_0 , et complet.
(corp. résiduel \bar{k}).

Soit $\varphi: \Gamma_n \rightarrow S_n$ un hom.
Soit $I \subset \Gamma_n$ le gpe d'inertie.
Supposons que $\varphi(I)$ soit un gpe
de S_n d'ordre 2 engendré par
une transposition.
Soit L_φ l'alg. correspondant à φ .
Alors $a(L_\varphi) = 0$.

On utilisera seulement que le
résidu de $a(L_\varphi)$ est nul.

Preuve: Faisons opérer Γ_n sur $[1, \dots, n]$
grâce à φ . L'image de I opère
et fixe $n-2$ pts de $[1, n]$ et en
permutant les deux autres. (disons 1, 2).
 I est normal ds Γ_n . De cette desc.
de $[1, n] = [1, 2] \cup [3, n]$ est stable par Γ_n .
D'où $L_\varphi = L_2 \times L_{n-2}$ avec $\text{res } L_i = i$.
Le $a(L_\varphi) = 0$, par le lemme qui suit.

Lemme: Soit L une algèbre étale de rang n sur k de la forme $L = L' \times L''$ avec $\deg. L' = 1$ ou 2 . Alors $a(L) = 0$.

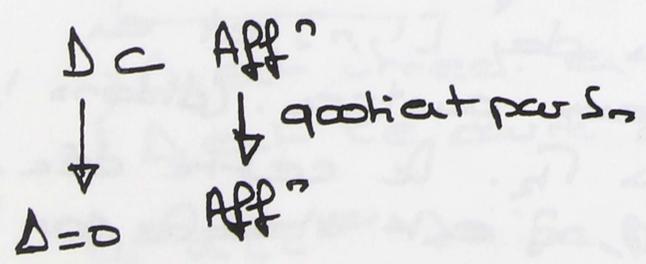
Démonstration: Soit $n'' = \deg. (L'')$.
 Définissons un opérateur a sur les algèbres étales sur les ext. de k de degré n'' par:
 Si \mathcal{R} est une telle algèbre, sur $k' \supset k$
 $b(\mathcal{R}) = a(L'/k' \times \mathcal{R})$.
 b a la propriété de s'annuler sur les algèbres décomposables en alg. de d° .
 Par hyp. de réc., ceci $\Rightarrow b = 0$.
 D'où le lemme avec $\mathcal{R} = L''$.

Regardons Aff^n . S_n opère en permutant les coordonnées.

$\forall (1 \leq i < j \leq n) \quad D_{ij} \text{ diag. } x_i = x_j$

$I = \cup D_{ij}$

S_n opère librement sur $\text{Aff}^n - I$.



x_i variables "a fait".
 A_i "a bas".
 $x_i + A_i x^{n-1} \dots = \prod (x - x_i)$
 i.e. $-A_i = \sum x_i$

$\Delta = \prod_{i < j} (x_i - x_j)^2$.

$\Delta = 0$ est clairement irred.

Par qpe d'inertie:

On relève Δ en $\Delta_{1,2}$

Qpe d'inertie = ss qpe de S_n fixant $\Delta_{1,2}$
 $= \{1, (1,2)\}$.

Le résultat précédent s'applique:
 a n'a pas de pôle en $\Delta = 0$.

(Le lemme précédent s'applique
 au complété de $h_0(A_1, \dots, A_n)$ pour
 la val. définie par Δ).

On a donc démontré que
 $a(L^{\text{res}}) \in H^i(h_0(A_1, \dots, A_n), \mathbb{C})$ n'a
 pas de pôles. De il \in au ss qpe
 "est" $H^i(h_0, \mathbb{C})$. Notons α cet él
 de $H^i(h_0, \mathbb{C})$.

Reste à mq $\begin{cases} x=0 \\ \forall L \ a(L) = 0. \end{cases}$

Prop.: Soit $P(x) = x^n + a_1 x^{n-1} + \dots + a_n$
 avec $a_i \in k$ et $\Delta(a_1, \dots, a_n) \neq 0$.

Soit L_P l'algèbre étale correspondante
 $L[x]/(P(x))$. Alors $a(L_P) = \alpha$.

(k désigne maintenant n'importe quelle
 extension de k_0).

On regarde $a - \kappa$.
 Arguments de spécialisation...
 (Déjà fait).

Prenons $h = h_0$.

Supposons tt d'abord $|h| \geq n$.

Prenons $h = h_0$ et $P = \prod_{i=1}^n (x - d_i)$
 $d_i \neq h_0, d_i \neq$

$L_P = h \times h \times \dots \times h$.

$a(L_P) = 0 = \kappa$. De $\kappa = 0$.

Sinon, \tilde{m} argument appliqué à
 $h_0(U)$ (U indéterminée), en utilisant
 cohom. C_0 cohom.

Ainsi a s'annule sur toutes les
 alg. étates qui possèdent un gén.

("Générateur d'une alg. étate L :
 c'est un scg L tq $1, x, \dots, x^n$ base de L)

{ Si $h = \infty$: H alg. étate a un gén.
Si $|h| \geq n$: _____ de $\text{rg } n$ _____

Si $h = \infty$, tte alg. étate $\simeq L_P$. OK.

Sinon, on remplace h par $h(U)$.

Explication: de $h \times$
 h est alg. ét. a un gén.

L étale de \mathbb{A}^n/k .
 \exists un nbre fini de h sev de L , de
 $\text{codim} \geq 1$ $\forall i$ tels que h est
 $x \in L - \cup V_i$ soit un générateur.

base (e_1, \dots, e_n) de L .

$x = x_1 e_1 + \dots + x_n e_n$ $x_i \in k$.

x^h comb. des e_i à coeff. pol. (x_1, \dots, x_n) .

$x^i = \sum_j a_{ij}(x) e_j$ $a_{ij}(x_1, \dots, x_n)$ pol.

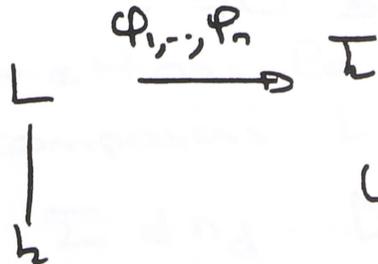
$\det(a_{ij}(x)) = R(x)$

R n'est pas identiquement nul.

(critère de base: il suffit de le vérifier
pour $L = k[x_1, \dots, x_n]$, et $e_i = (0, \dots, 0, 1, 0, \dots, 0)$).

Dans ce cas $x^i = (x_1^i, \dots, x_n^i)$ et

$R(x) = \prod_{i > j} (x_i - x_j)$ (= $V \Delta$).



$UV = \{ x \text{ tq } \exists i \neq j$
avec $\varphi_j(x) = \varphi_i(x) \}$.

le 15.11.93

VI-17

Cas des corps fini:

k fini à q elt.

Si $n \geq q$ e.a. alg. déc. $k[x_1 \dots x_n]$ de rg
n'a pas de générateurs.

($x = (x_1, \dots, x_n)$ avec $x_i \neq x_j$ imp.).

Par contre $n < q$, on a des gén.

F corps de nbre.

\mathbb{Q}

\mathcal{O}_F anneau des entiers

Pour définir différent, ...)

il est commode de supposer $\mathcal{O}_F = \mathbb{Z}[x]$.

Ce n'est pas tjrs vrai.

En fait, ce n'est pas vrai n'a plus

localement, à cause de ce qui précède
(La fact. excep. de disc.).

\Rightarrow Il faut localiser a lant,
sur les idéaux de \mathcal{O}_F .

J. P. Serre VII
Cours au collège
de France.
Le 22 novembre 93

VII- (1)

Générateurs des algèbres étales.

k ; L/k étale de $\text{rg } n$.

$x \in L$ tq $L = k[x]$. x est un générateur.

On a vu que les générateurs forment
un ouvert de L .

Si $|k| = q$ fini

Thm: Si $q \geq n$, L a un générateur.
(Si $q < n$, l'algèbre déployée
 $k[x] \cdots k[x]$ de $\text{rg } n$ n'a pas de
générateurs).

Preuve du thm:

Notons $m(q, d) =$ nombre de polynômes
unitaires irréductibles de degré d sur
 $k = \mathbb{F}_q$.

Lemme: $m(q, d) \geq q/d$

Admettons le lemme pour l'instant.

Décomposons $L = \prod (\mathbb{F}_{q^{d_i}})^{n_i}$.

$n = \sum d_i n_i$. Donc $n_i \leq n/d_i \leq q/d_i$.

Grâce au lemme, il existe donc
des polynômes $P_{d,1}, \dots, P_{d,n_d}$ irred.
unitaires distincts de degré d .

le 22.11.93

VII-②

Posons $P = \prod_{d,i} P_{d,i}$. $\mathbb{I}\mathbb{E}$ est unitaire, sans facteurs carrés, et $L \cong k[x]/(P(x))$.

Preuve du lemme:

$$k_d = \mathbb{F}_{q^d} \quad [k_d : k] = d.$$

$\mathbb{I}\mathbb{E}$ existe un générateur $x \in k_d$.

$k_d = k[x] \rightarrow$ fournit un polynôme P irréductible de degré d . (polynôme minimal (x))

Alors $\forall d \in k \quad P_d := P(x+d)$.

P_d est aussi irréductible unitaire de degré d .

d fixé. le nombre de v tq $P_d = P_v \leq d$.

[$x+d$ et $x+v$ sont conjugués si $P_d = P_v$].

Ceci fournit un nombre de polynômes $\geq q/d$.

Revenons aux nombres $m(q,d)$

$$(1) \quad q^n = \sum_{d|n} d m(q,d).$$

$x \in k_{q^n} \mapsto$ pol. min. de x . $\mathbb{I}\mathbb{E}$ est irréductible de degré $d|n$.

$$(2) \quad \frac{1}{1-qt} = \prod_{d=1}^{\infty} \frac{1}{(1-t^d)^{m(q,d)}} = \prod_{\substack{\text{P. unit.} \\ \text{irréduct.}}} \frac{1}{1-t^{\text{degr}}}$$

C'est l'écriture habituelle de la fonction zêta de la droite affine.

\prod = produit eulérien.

$$X = \text{APP}' / \mathbb{F}_q ; Z_X(t) = \zeta_X \text{ de } X.$$

(3) Rœbius :

$$m(q, n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}$$

$$m(q, 1) = q$$

$$m(q, 2) = \frac{1}{2} (q^2 - q)$$

$$m(q, 3) = \frac{1}{3} (q^3 - q)$$

La formule (2) intervient dans la théorie des alg. de Lie libres :

$(Q; q \geq 1)$.

On peut définir l'algèbre de Lie libre en X_1, \dots, X_q . C'est une alg. graduée

Notons $\text{Lie} = \text{Lie}(X_1, \dots, X_q)$.

Appelons $\mathcal{R}(q, d)$ la dim. de $\text{Lie}(X_1, \dots, X_q)^d$.

$$\left[\begin{array}{l} d=1 \quad X_1, \dots, X_q \quad \mathcal{R} = q \\ d=2 \quad [X_i, X_j] \quad i < j \quad \mathcal{R} = \frac{q^2 - q}{2} \end{array} \right].$$

$$\forall \mathcal{P}_m : \boxed{\mathcal{R}(q, d) = m(q, d)}.$$

Dém: On regarde l'algèbre enveloppante de Lie : $U\text{Lie} = \text{alg. associative libre en } X_1, \dots, X_q$. Sa série de Poincaré est $\frac{1}{1-qt}$.

Puis gr $U\text{Lie} = \text{Sym Lie}$ et sous cette forme, la série de Poincaré

$$\text{est } \prod \frac{1}{(1-t^d)^{\mathcal{R}(q, d)}}.$$

ce qui démontre le \mathcal{P}_m .

Ceci permet également de redémontrer
 $m(q, d) \geq q/d$:

$[x_1, [x_1, [\dots [x_1, x_2] \dots]]$ permet de prouver
 l'existence d'au moins un polynôme
 irréductible de degré d .

En fait, leur nombre est $\geq q-1$.
 (Remplace x_2 par x_3, \dots, x_q).

La formule (2) intervient aussi
 en topologie :

r impair ≥ 3

$X = S_r \vee \dots \vee S_r$ (q copies)

(bouquet de sphères ).

ΩX espace des lacets de X .

La série de Poincaré de ΩX est $\frac{1}{1-qt^r}$.

$H^*(\Omega X, \mathbb{Q})$ algèbre de polynômes en
 des variables de degré $(r-1)d$, en
 nombre $N(q, d)$.

Thm : $N(q, d) = m(q, d) = \sum_{d'|d} \mu(d') q^{d/d'}$.

En effet la série de Poincaré
 s'écrit

$$\prod_d \frac{1}{(1-t^{d(r-1)})^{N(q, d)}}$$

On obtient ainsi la formule

$$\text{Rang } \pi_{d(r-1)+1}(X) = m(q, d)$$

$$\text{Rang } \pi_i = 0 \text{ si } i \not\equiv 1 \pmod{(r-1)}.$$

Invariants cohom. des alg. étates.

k_0 corps de base.

C module fini sur Γ_{k_0} ; $(|C|, \text{car } k_0) = 1$.

$n \geq 1$ seq des alg. étates.

$$\begin{array}{c} L/k \\ k > k_0 \end{array} \quad L \mapsto a(L) \in H^{\bullet}(k, C).$$

On a montré q' un invariant cohom. qui est nul sur les alg. $L = \prod L_i$ avec $\text{rg } L_i \leq 2$ est nul.

On commence par s'intéresser au cas où $C = \mathbb{Z}/2\mathbb{Z}$ ($\text{car } k_0 \neq 2$).

On notera $H^{\bullet}(k)$ au lieu de $H^{\bullet}(k, \mathbb{Z}/2\mathbb{Z})$.

1er exple d'invariants.

On choisit une classe de cohom.

$$x \in H^{\bullet}(S_n, \mathbb{Z}/2\mathbb{Z}) = H^{\bullet}(S_n).$$

L correspond à un $\phi_L: \Gamma_k \rightarrow S_n$
 déf. à conj. près.

De on peut définir $a_x(L) = \phi_L^*(x)$.

C'est un inv. cohom.

De et $x \in H^{\bullet}(S_n) \mapsto$ inv. cohom. a_x .

Classes de Stiefel-Whitney:

ce nt des $w_i \in H^i(S_n)$ définis de

la façon suivante:

$S_n \hookrightarrow O_n$ grpe orthogonal.

$\hookrightarrow B S_n \rightarrow B O_n$

et $H^*(B O_n) \xrightarrow{\cong} H^*(B S_n) = H^*(S_n)$

$H^2[\omega_1, \dots, \omega_n] \xrightarrow{\cong} \omega_1, \dots, \omega_n \in H^*(S_n)$.

$\omega_1 \in H^1(S_n) = \text{Hom}(S_n, \mathbb{Z}/2\mathbb{Z})$: signature.

$\omega_2 \in H^2(S_n)$ correspond à une extension \tilde{S}_n de S_n par $\mathbb{Z}/2\mathbb{Z}$.

On notea l'invariant correspondant $\alpha_{\omega_i}(L) = \omega_i(L)^{\text{gae}}$

2nd expe d'invariants.

$L \mapsto q_L$ f.g. de \mathbb{F}_q^n

$x \mapsto T_{2/K}(x^2)$.

Mais $q \mapsto \omega_i(q) \in H^i(k)$

Si $q = \langle \alpha_1, \dots, \alpha_n \rangle$ $\omega_i(q) = \sum_{i_1 < \dots < i_i} (\alpha_{i_1}) \dots (\alpha_{i_i})$.

$\omega_i(x)$ est l'élément de $H^i(k)$ correspondant à $x \in K^*$.

On notea l'invariant correspondant $\omega_i(L) = \omega_i(q_L)$.

Prm 1 : $\omega_i(L)^{\text{gae}} = 0$ si $i > \lfloor \frac{n}{2} \rfloor$

Prm 2 : $B. Katz$ Inv. 12 1984
 $\omega_i(L)^{\text{gae}} = \omega_i(L)$ si i impair
 $\omega_i(L)^{\text{gae}} = \omega_i(L) + (2)\omega_{i-1}(L)$ si i pair.

(2) $\in H^1(k)$

$L = 0$ si et seulement si L est un carré de k .

Grâce au thm qui précède, o.p.s.

$L = \prod L_i$ avec $\text{rg } L_i \leq 2$.

$\varphi_L : \Gamma_k \rightarrow S_n$.

Appelons H_n le ss gpe de S_n de type $(2, \dots, 2)$ formé des permutations qui laissent stables $\{1, 2\}; \{3, 4\}; \dots$

$L = \prod L_i$
 $\text{rg } L_i \leq 2 \iff \varphi_L : \Gamma_k \rightarrow S_n$
 \searrow
 H_n

Mais

$S_n \hookrightarrow D_n \quad m = \lfloor \frac{n}{2} \rfloor$

$H_n \hookrightarrow D_m \quad (A \in D_m \mapsto \begin{pmatrix} A & 0 \\ 0 & I_{m-1} \end{pmatrix})$.

Mais D_m n'a plus de classes de Skjelvel Whitney au delà de la dim. m .

De $\chi_i(L)^{\text{gal}} = 0$ si $i > \lfloor \frac{n}{2} \rfloor$.

Pour le 2nd thm :

① le thm est vrai si $n=2$: ($n=1$ évident)

$L = k[x]/(x^2 - \alpha) \quad \alpha \in k$

$\chi_1^{\text{gal}} = (\alpha) ; \chi_2^{\text{gal}} = 0$.

Forme trace : ds la base $(1, \sqrt{\alpha})$, on obtient $q_L = \langle 2, 2\alpha \rangle$

De $\chi_1(L) = (4\alpha) = (\alpha) = \chi_1^{\text{gal}}(L)$

$\chi_2(L) = (2)(2\alpha) = (2)(2) + (2)(\alpha)$

Mais $(2)(2) = (-1)(2) = 0$.

et $\chi_2^{\text{gae}}(L) = 0 = \chi_2(L) + (2)(K)$
 car $(2)(K) + (2)(K) = 0$.

Le thm est vrai pour $n=2$.

② Pour conclure, on va montrer que si le thm est vrai pour deux algèbres L et L' , alors il est vrai pour leur produit.

Puis, on sait multiplier les séries de Witt
 forme trace = \oplus forme traces.

↳ on va m.q. les deux membres sont multiplicatifs.

$$\chi = \sum \chi_i \in H^*(k) = \bigoplus H^i(k),$$

$$= \chi_{\text{pair}} + \chi_{\text{impair}} (= \chi_+ + \chi_-).$$

On veut montrer que $\chi^{\text{gae}} = \chi + (2)\chi_-$

Puis :

$$1) \chi^{\text{gae}}(L \times L') = \chi^{\text{gae}}(L) \cdot \chi^{\text{gae}}(L')$$

(car : multiplicativité).

$$2) \chi(q_1 \oplus q_2) = \chi(q_1) \chi(q_2)$$

$$\chi(\chi(L \times L') + (2)\chi_-(L \times L'))$$

$$= \chi\chi' + (2)(\chi_+\chi'_- + \chi_-\chi'_+)$$

$$= \chi\chi' + (2)(\chi\chi'_- + \chi'\chi_-)$$

$$= (\chi + (2)\chi_-)(\chi' + (2)\chi'_-)$$

$$\text{car } (2)\chi_-(2)\chi'_- = 0 \text{ vu que } (2)(2) = 0.$$

capit

Rem: On peut refaire tout ça en remplaçant S_n par un groupe de Weyl

d'un système de racines. (Du moins si h_0 est de car 0).

Notons $E \in \mathcal{N}$. $n = \text{rg } \mathcal{N}$.

Repr. naturelle sur \mathbb{Q}^n engendré par des réflexions.

H_n est remplacé par des sous groupes de type $(2, \dots, 2)$ obtenus ainsi:

On considère des hyperplans radicaux 2 à 2 orthogonaux.

Le ss gpe de Weyl engendré par les symétries par rapport à un hyperplan.

Les inv. coh. seront détectés par ces sous groupes de type $(2, \dots, 2)$.

$$[\text{APP}^n / \mathcal{N} \cong \text{APP}^n]$$

↑
Est-ce encore vrai en car p ?

Détermination explicite des inv.

coh. des alg. étates de $\text{rg } n = \binom{2n}{2m+1}$

Phm: Les inv. coh. pour S_n et S_{n+1} sont les mêmes si n est pair.

(Vrai pour la coh. de \mathbb{C} , pas uniquement modulo 2).

Plus précisément: $H \subset G$

Res: inv. coh. de $G \rightarrow$ inv. coh. de H
Cor: $\text{---} H \rightarrow \text{---} G$

Res \circ Cor = indice de H ds G

($\varphi: \Gamma_n \rightarrow G \mapsto a(\varphi) \in H^0(h, c)$
 Mais $\varphi: \Gamma_n \rightarrow H \subset G \dots$).

Thm: Res : inv. coh. de $S_{n+1} \rightarrow$ inv. coh. de S_n
 est un isomorphisme si n est pair.

Dém: Il suffit de le voir pour les
 invariants normalisés. $2 \cdot \text{inv.} = 0$.
 $\text{Or } [S_{n+1} : S_n] = n+1 \equiv 1 \pmod{2}$.
 $\Delta \text{ Res} \circ \text{Cor}$ est l'identité sur les
 inv. normalisés
 $\hookrightarrow \text{Res}$ est surjectif.

Res est aussi injectif. En effet
 si a inv. coh. de S_{n+1} tq $\text{Res } a = 0$,
 on a $a(L) = 0$ pour $L = L_n \times h$ $\text{rg } L_n =$
 Mais $\text{co } n+1$ est impair, si $L = \prod L_i$ avec
 $\text{rg } L_i \leq 2$, on peut forcément écrire $L = L_n \times h$.
 Ceci suffit à prouver que a est nul.

[Lien avec thm de Noether:

Si on a une alg. étale de rg impair
 $n+1$, il existe une alg. étale de rg
 n qui a la même forme trace].

Désormais, on se place à nouveau
 dans le cas où $C = \mathbb{Z}/2\mathbb{Z}$.

Thm: Les inv. colon. des algèbres étales de rang n sur des extensions de k_0 forment un $H^0(k_0)$ module libre de base $1, \kappa_1^{gal}, \dots, \kappa_m^{gal}$ $m = \lfloor \frac{n}{2} \rfloor$.

Preuve: car $\neq 2$.

Les invariants cohomologiques sont détectés par le sous-groupe

$$H_n = \underbrace{C_2 \times \dots \times C_2}_{n \text{ fois}} \subset S_n$$

On va déterminer les inv. colon. de H_n

Pour C_2 : Les inv. colon. forment un mod. libre de rang 2, de base $1, "(x)"$.

(Algèbre étale donnée par $x \in k^0/k^0_2$

$$L_0(x) \in H^1(k).$$

On a montré que tout invariant est de la forme $L \mapsto d_0 + d_1(x) \cdot d_1 \in H^0(k_0)$

$$\varphi: \Gamma_k \rightarrow H_n.$$

Une alg. galoisienne à groupe

$H_n = C_2 \times \dots \times C_2$ est définie par

$$m \text{ éléments } \kappa_1, \dots, \kappa_m \in k^0/k^0_2.$$

$$L_0(\kappa_i) \in H^1(k) \quad \chi_i(\varphi) \quad (i=1, \dots, m).$$

Thm: Les inv. colon. mod. 2 des H_n torsseurs ont pour base les cup produits $x_{j_1} \dots x_{j_c}(\varphi)$ avec $j_1 < \dots < j_c$

($m=2 : 1, x_1, x_2, x_1 x_2$).

Preuve (n dem. qz précédemment).

$$h = h_0(x_1, \dots, x_m)$$

φ^{vr} correspondant à $x_i = X_i$

$$a(\varphi^{vr}) \in H^0(h).$$

Pas de pôles a dehors des $X_i = 0$.

D'où l'écriture voulue.

Par spécialisation, on démontre le thm.

$$I \subset [1, \dots, m] \quad I = \{i_1, \dots, i_r\} \quad i_1 < \dots < i_r$$

$$x_I(\varphi) = \prod_{k=1}^r x_{i_k}(\varphi).$$

Les x_I forment une base des inv. colom.

Si a est un inv. col. de S_n

$$a|_{H_n} = \sum d_I x_I \quad d_I \in H^0(h_0).$$

Le gpe sym. S_m opère sur H_n ,

$$\text{i.e. on a } H_n \subset N \subset S_n$$

$$N|_{H_n} \cong S_m$$

(on permute les paires)

La restriction de a à H_n est invariante par l'action de S_n .

$$\text{D } d_I = d_J \text{ si } |I| = |J|.$$

D'où

$$a|_{H_n} = \sum_{i=0}^m d_i \left(\sum_{|I|=i} x_I \right).$$

$$\text{Mais } \sum_{|I|=i} x_I = \omega_i g a e.$$

$$\text{D } a|_{H_n} = \sum_{i=0}^m d_i \omega_i g a e.$$

□

Cas g n ral (C quelconque).

Thm : Tout invariant cohomologique normalis  s' crit de fa on unique sous la forme $\sum_{i=1}^m d_i \kappa_i$ $d_i \in H^0(h_0, C(-i))_2$

Explicat  :

$d_i \in H^0(h_0, C(-i))_2$

signifie que $d_i \in H^0(h_0, C(-i))$ et $2d_i = 0$.

Si $nC = 0$ $n \wedge \text{car } h_0 = 1, n \geq 1$.

$C(-i) \stackrel{\text{d f.}}{=} \text{Hom}(H_n^{\otimes i}, C)$. (torsion   la Tate).

$\left. \begin{array}{l} \kappa_i \in H^i(h, \mathbb{Z}/2\mathbb{Z}) \\ d_i \in H^i(h, C(-i)), 2d_i = 0 \end{array} \right\} \xrightarrow{?} d_i \kappa_i \in H^i(h, C)$
"cup produit".

On peut supposer $n = 2^k$

Si $x \in H^i(h, \mu_n^{\otimes i})$, alors $d_i x$ (cup prod.)

a un sens dans $H^i(h, C)$.

Mais $C(-i) \otimes \mu_n^{\otimes i} \rightarrow C$.

Lemme (triviale) : κ_i est relevable dans $H^i(h, \mu_{2^k}^{\otimes i})$ pour tout k .

car :

\hookrightarrow On  et de degr  1 est toujours relevable $x \in H^1(h, \mathbb{Z}/2\mathbb{Z}) = H^1(h, \mu_2)$ $x = (\zeta)$ $\zeta \in h^*$.

th orie de Kummer : le \tilde{n} ζ d finit

un  et de $H^i(h, \mu_{2^k}^{\otimes i})$.

On est ramené à déterminer
 les car. géom. de C de $h_0(X, \dots, X_n)$
 non ramifiée à dehors de $X_i = 0$.

↑

Écriture ! sous la forme $\sum_{I \in \mathbb{C}(1, n)} d_I \chi_I$
 $d_I \in H^0(h_0, C(-|I|))$.

$\chi_I = \text{cup produit des } \chi_j \in H^1(h, M_n)$
 $\quad \quad \quad \uparrow \in I$.

$$2d_I = 0$$

$$d_I = d_J \text{ si } |I| = |J| \dots$$

(n d'ém.).

Invar. des alg. de Witt :

$$L \rightarrow a(L) \in \begin{cases} \text{Gr } W_h \\ W_h \end{cases}$$

Cas évident : la forme trace
 $L \rightarrow q_L$.

et aussi : $\Lambda^i q_L \quad \forall i \quad (0 \leq i \leq n)$.

Thm : Il n'existe à val. de W_h
 des alg. étates de rang
 s'écrit de façon unique
 $L \rightarrow \sum_{i=0}^n \lambda_i \Lambda^i q_L \quad \lambda_i \in W_h$.

i.e. les $\Lambda^i q_L$ forment une base
 des invariants.

Cor : On a des formules pour
 $\Lambda^{n+1} q_L, \dots$

Quelques compléments sur les invariants
 cohomologiques usuels.

Thm: Soit $x \in H^i(S_n, \mathbb{Z})$.
 On suppose $\begin{cases} i \geq 1 \\ \text{Act}^0 \text{ de } S_n \text{ sur } \mathbb{Z} \text{ triviale.} \end{cases}$
 Alors $2x$ est négligeable.

Preuve:

o.p.s. \mathbb{Z} est de type fini, i.e. $\mathbb{Z} = \mathbb{Z}$ ou $\mathbb{Z}/m\mathbb{Z}$
 De plus le cas \mathbb{Z} se ramène à $\mathbb{Z}/m\mathbb{Z}$ car

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

$$\begin{cases} H^i(G, \mathbb{Z}) \cong H^{i-1}(G, \mathbb{Q}/\mathbb{Z}) \\ H^1(G, \mathbb{Z}) = 0 \end{cases} \quad \begin{matrix} \uparrow \\ \text{de torsion} \end{matrix}$$

En car 0

$$h; \varphi: \Gamma \rightarrow S_n \quad \varphi^*(2x) \stackrel{?}{=} 0$$

La classe de $2x$ définit une opération
 cohomologique sur les algèbres étales
 de rang n sur $h \supset h_0 = \mathbb{Q}: \varphi \mapsto \varphi^*(x)$.

Elle est normalisée, car $\varphi=1 \Rightarrow \varphi^*(x) = 0$
 (vu que $i \geq 1$).

$$\text{Dc } 2\varphi^*(x) = 0.$$

Plus précisément :

$$H = \underbrace{C_2 \times \dots \times C_2}_{\lfloor \frac{n}{2} \rfloor \text{ termes}} \subset S_n$$

H engendré par $(1,2); (3,4); \dots$

LEM : $x \in H^i(S_n, \mathbb{R})$ est négligeable
ssi sa restriction à H est nég.

Cas particulier : $\mathbb{R} = \mathbb{Z}/2\mathbb{Z}$.

LEM : $x \in H^i(S_n, \mathbb{Z}/2\mathbb{Z})$ est négligeable
ssi sa restriction aux sous-espaces
d'ordre 2 de S_n est 0.

\Rightarrow est clair

\Leftarrow Considérons $x|_H \in H^i(H, \mathbb{Z}/2\mathbb{Z})$
H de type $(2,2, \dots, 2)$.

On sait $H^*(H) = \mathbb{F}_2[x_1, \dots, x_N]$ $N = \lfloor \frac{n}{2} \rfloor$

$\Delta_c x$ est un polynôme en les x_i , qui
est nul c'est-à-dire sur \mathbb{F}_2^N .

On peut vérifier :

Les polynômes homogènes sur \mathbb{F}_q qui
s'annulent comme fonction sont dans
l'idéal engendré par $x_i^q - x_i$.

En particulier, x est dans l'idéal

engendré par les $\underbrace{x_i^2 x_j + x_i x_j^2}_{\text{nég.}}$ $i \neq j$

A_6 - Inv. cohom. mod. 3 et mod. 5

$$H^2(A_6, \mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z}$$

$C_3 \times C_3$ u op. cohom. correspondant.

Prm: Les inv. cohom. de A_6 torseurs à coeff. mod. 3 sur h_0 forment u $H^*(h_0, \mathbb{Z}/3\mathbb{Z})$ module libre de base $\{1, \psi\}$.

Tout inv. cohom. de A_6 mod. 5 normalisé est 0.

Sylow $C_3 \times C_3$ ~~à 0~~
 $C_5 \subset D_5$
 normalisateur.

Rais: Inv. cohom. mod. 3 de A_6 ?
 (le Sylow est plus compliqué).

On a vu que les inv. cohom. mod. 2 pour S_n ont pour base les classes $\kappa_i(q_L) = \kappa_i$ ($0 \leq i \leq m$; $m = \lfloor \frac{n}{2} \rfloor$)
 ou bien $\kappa_i q^a$.

On a vu aussi $\kappa_i q^a = 0$ si $i > m$.

$$\begin{cases} \kappa_i q = \kappa_i + (2) \kappa_{i-1} & \text{si } i \text{ pair} \\ \kappa_i q = \kappa_i & \text{si } i \text{ impair.} \end{cases}$$

On peut énoncer ce résultat autrement:

Si n est pair: $\boxed{w_i^2 = w_i(2q_L)}$.

Rqre: Forme trace (du pt de vue torsion).

Forme standard $\langle 1, \dots, 1 \rangle$ $x_1^2 + \dots + x_n^2$.

$\varphi: \Gamma_h \rightarrow S_n$.

L'act^o de S_n tord $\langle 1, \dots, 1 \rangle$ par φ et donne la forme trace.

Qd n est pair, on a de intérêt à prendre $2x_1^2 + \dots + 2x_n^2$.

Autre écriture:

$$w_i^2 = \sum_i w_i^2 ; w = \sum_i w_i. \quad w_i = (d).$$

On a $\boxed{w_i^2 = w(1 + (2)(d))}$.

Pour le démontrer, on a besoin d'identités entre les classes de Stiefel-Whitney (S. Milnor; Inv 10).

Ces identités st valables pour les w_i de f.q. qu'elles:

On écrit i sous forme dyadique

$$i = \sum_{d \in I} 2^d \quad I \subset \mathbb{N}.$$

$$\boxed{w_i = \prod_{d \in I} w_{2^d}}$$

exple: $w_7 = w_1 w_2 w_4$.

Alors si $i = \sum_{d \in I} 2^d$ $j = \sum_{d \in J} 2^d$

$\boxed{w_i w_j = u^r w_e}$ où $\begin{cases} u = (-1)^{e-i} \\ e = \sum_{v \in I \cup J} 2^v = i + j - r \end{cases}$

Exple : $w_7 = w_1 w_2 w_4$
 $w_{10} = w_2 w_8$

$\hookrightarrow w_7 w_{10} = w_1 w_2^2 w_4 w_8 = u^2 w_1 w_2 w_4 w_8 = u^2 w_{15}$

(Si $x \in H^i(k, \mathbb{Z}/2\mathbb{Z})$ est décomposable, alors $x^2 = u^i x$).

Généralisation aux $\text{Tr}(KX^2)$

$n \binom{L}{h}$ $K \in L^*$
 $q_{L,K}$ forme de rang n .
 $w_i(q_{L,K})$.

Mais on peut aussi associer des w_i^q , car la donnée de (L, K) équivaut à la donnée d'un torseur sous $S'_n = 2^n S_n$ (permutat° et chgt de signe de n lettres)
 $S'_n \subset O_n(\mathbb{R}) \rightarrow w_i \in H^i(S'_n)$.

Formule

$\boxed{(B. Karan)}$
 $w_i^q = w_i(1 + (2)(d))$ où $d = \text{disc}(L)$

Mais, on peut en fait se ramener au cas précédent par :

$$2n \left(\begin{array}{c} L[x] / (x^2 - \alpha) \\ | \\ L \\ | \\ h \end{array} \right)$$

La formule se déduit du cas $\alpha = 1$ appliqué à L et à " $L(\sqrt{\alpha})$ ".

Invariants Witt :

On revient au tr_m sur les invariants à valeurs dans K^h .

TRM : Ces invariants forment un K^h -module libre de base les $d^i(q)$, $0 \leq i \leq m$, où q est la forme trace.

$$m = \lfloor n/2 \rfloor.$$

Dém : Elle est presque identique à celle pour les invariants coform .

1^{ère} étape :

Soit a un K^h -invariant.

TRM : Si a est 0 pour les alg. $L = \prod L_i$ avec $\text{rg}(L_i) \leq 2$, alors a est 0.

$$h = h_0(A_1, \dots, A_n)$$

L^{vo} déf. par $X^n + A_1 X^{n-1} + \dots + A_n$.

$$a(L^{v_0}) \in \mathcal{N}h = \mathcal{N}h_0(A_1, \dots, A_n)$$

corps des fct^{os} sur $\mathbb{A}P^n$.

On montre que a est non ramifié :

\mathcal{N} irred. \neq disc = 0 : c'est axiome (2)

\mathcal{N} = disc : L se décompose en $L_2 \times L_{n-2}$ sur le complété.

Un raisonnement par récurrence permet de conclure.

Et $a(L^{v_0}) \in \mathcal{N}h_0$.

Par spécialisation, on a déduit $a=0$.

2^{de} étape :

Supposons p.ex. $n=2m$.

L_1, \dots, L_m $L_i = h[x] / (x^2 - x_i)$ x_i inv.

Cas versé : $h = h_0(x_1, \dots, x_m)$ x_i ind.

$a(L^{v_0}) \in \mathcal{N}h$ sans pôles à dehors des hyperplans $x_i = 0$.

Prop. :

Les \mathbb{Z}^+ de $\mathcal{N}h$ n'ayant pas de pôles à dehors des hyperplans $x_i = 0$ forment un $\mathcal{N}h_0$ module libre de base $1, \langle x_1 \rangle, \dots, \langle x_m \rangle, \langle x_{i_1} \rangle \dots \langle x_{i_m} \rangle, \dots$
 $i_1 < \dots < i_m$.

$I \subset [1, m]$ $x_I = \prod_{i \in I} x_i$ base : $\langle x_I \rangle$
 $I \subset [1, m]$.

$$\text{De } a(L^{\vee}) = \sum c_I \langle x_I \rangle \quad c_I \in \mathbb{N}_0.$$

C'est invariant par l'action de S_n (qui permute les facteurs) : de c_I ne dépend que de $|I|$.

$$a(L^{\vee}) = \sum_{i=0}^n c_i \left(\sum_{|I|=i} \langle x_I \rangle \right).$$

$$L^{\vee} = \prod L_i \quad L_i = k(\sqrt{x_i}).$$

$$q_{L^{\vee}} = \bigoplus \langle 2, 2x_i \rangle.$$

$$2q_{L^{\vee}} = \bigoplus \langle 1, x_i \rangle = \underbrace{\langle 1, \dots, 1 \rangle}_m \oplus q'$$

$$\text{c'est } q' = \langle x_1, \dots, x_m \rangle.$$

$$\text{i.e. } 2q = m + q'.$$

Les $d^i q'$ ($0 \leq i \leq m$) forment une base.

Mais on a une matrice triangulaire inversible qui fait passer aux $d^i q$:

$$q = \langle 2 \rangle m + \langle 2 \rangle q'$$

$$d^i q = \sum_{a+b=i} \lambda^a \underbrace{(\langle 2 \rangle m)}_{\text{etc}} \cdot \lambda^b (\langle 2 \rangle q')$$

□

Exemple: $n=6$.

S_6 a un automorphisme externe:

$$1 \rightarrow S_6 \rightarrow \text{Aut}(S_6) \rightarrow C_2 \rightarrow 1$$

En effet

$S_5 \rightarrow S_6$) En permutant les 6
 ss qpe transitif) S -sylloux de S_5 .

$X = S_6/S_5$ a 6 \mathbb{Z} ets.

S_6 opère sur X .

D'où $S_6 \rightarrow \text{Aut}(X) \cong S_6$.

Soit dc $\sigma \in \text{Aut}(S_6)$, $\sigma \notin S_6$.

Soit L ue alg. étale de rg 6 sur k .

$\varphi: \Gamma_k \rightarrow S_6$

$\sigma\varphi: \Gamma_k \rightarrow S_6 \mapsto L_\sigma$ (à isom. près).

(cf, en termes de polynômes, la
 réécriture sextique).

$$q(L_\sigma) = ?$$

Grâce au thm précédent, on sait
 que $q(L_\sigma)$ s'écrit comme C.L. et
 coeff. dans \mathbb{N} (corps premier) de
 $1, d^3q_L, d^2q_L, d^3q_L$.

$$q_{L_\sigma} = d^3q_L - \langle 1, 2 \rangle \otimes d^2q_L \\ + \langle 1, 1, 2 \rangle \otimes q_L - \langle 1, 2 \rangle.$$

Forme Trace :

Dans la dernière partie du cours, on s'intéresse à la forme trace.

En part., on regarde les cas $\left\{ \begin{array}{l} n=3,4,5 \\ n=6,7. \end{array} \right.$

Question :

Soit k un corps ; car $k \neq 2$
 n entier ≥ 1 .

"Quelles st" les f. quad.

q à n variables / k qui
 st égales à q_E pour E
 alg. étale de $\text{rg } n$ / k ?

Condition triviale :

$n = \sum_{i \in I} 2^{i_i}$ écriture dyadique de n :
 $I = \{i_1, \dots, i_r\}$ $i_1 < \dots < i_r$.

Prop. : q_E contient la forme quadratique
 $\langle 2^{i_1}, \dots, 2^{i_r} \rangle$, de $\text{rg } k = |I|$.

Exple : $n=7$ $\langle 1, 2, 4 \rangle \cong \langle 1, 1, 2 \rangle$.

[contient signifie $q_E \cong \langle 2^{i_1}, \dots, 2^{i_r} \rangle \oplus q'_E$
 avec $\text{rg } q'_E = n - r$].

Preuve:

Springer: h'/h de deg. impair.

Si q_1 et q_2 st des p.q. sur h telles que q_1 contient q_2 après extension à h' , alors q_1 contient q_2 .

En d'autres termes "Les extensions de degré impair ne comptent pas".

$\varphi: \Gamma_h \rightarrow S_n$.

Après ext. de deg. impair, l'image de φ est contenue dans un 2 Sylow de S_n .

$$\text{Si } n = 2^{i_1} + \dots + 2^{i_r} \quad \Omega = \bigsqcup_{j=1}^r \Omega_j \quad [\Gamma, \Omega] = \prod_{j=1}^r \Omega_j \quad |\Omega_j| = 2^{i_j}$$

$$\begin{aligned} 2 \text{ Sylow de } S_n &= S_\Omega \\ &= \prod 2 \text{ Sylows de } S_{\Omega_j}. \end{aligned}$$

Le $\Omega = \bigsqcup \Omega_j$ est la décomposition de Ω en orbites d'un 2 Sylow de S_n .

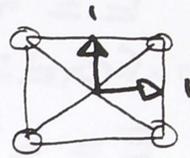
Γ_h préserve cette décomposition de Ω
 $\Leftrightarrow E = \prod E_j$ avec $\text{rg } E_j = 2^{i_j}$.

Or la forme trace représente n (si $n \neq 0$ ds h) car $\text{Tr}(1^2) = n$.

La q_{E_j} représente 2^{i_j} et $q = \langle 2^{i_j} \rangle \oplus q'_{E_j}$.

D'où $q_E = \bigoplus q_{E_j} = \dots$

$$\text{Mais } \begin{cases} \langle 4 \rangle \cong \langle 1 \rangle \\ \langle 2, 2 \rangle \cong \langle 1, 1 \rangle \end{cases}$$



On peut réduire la partie triviale à $\langle 1, \dots, 1 \rangle$ ou $\langle 1, \dots, 1, 2 \rangle$.

Exercice:

Démontrer que q' n'a pas de "partie fixe".

Précisément : $\begin{cases} k \text{ corps car } k \neq 2 \\ n \text{ entier } \geq 1. \end{cases}$

mg: $\exists K/k$ et \exists une alg. étale E sur K de rang n de la forme $q'E$ ne représentable avec $\hat{e}t$ de k .

Indications: construire une ext. multiqua-dratique, à Galois de type $(2, \dots, 2)$ avec des indéterminées.

exple: $n = 7 = 1 + 2 + 4$.

$$k; E = K \times K(\sqrt{x}) \times \underbrace{K(\sqrt{y}, \sqrt{z})}_{K(\sqrt{y}) \otimes K(\sqrt{z})}$$

x, y, z indéterminées / k .

Rm: Si $n \leq 3$, la cadito triviale suffit pour qu'une forme donnée soit forme trace.

Dem: $n=1$

$$E = k; \quad q_E = \langle 1 \rangle.$$

Condition triviale: contenu $\langle 1 \rangle$. $n=2$

$$E = k[x] / (x^2 - d) \quad q_E \cong \langle 2, 2d \rangle.$$

Condition triviale: contenu $\langle 2 \rangle$. $n=3=1+2$

$$q_E = \langle 1, 2, x \rangle$$

$$\text{si } q = \langle 1 \rangle \oplus \langle 2, x \rangle$$

$$E = k \times E_2 \text{ avec } q_{E_2} = \langle 2, x \rangle.$$

Prop(Reste) k ; $\text{car } k \neq 2$ Si n est impair ≥ 1 , et E étale de rang n , $\exists E'$ de rang $n-1$ telle que $q_E \cong \langle 1 \rangle \oplus q_{E'}$,i.e. E et $k \times E'$ ont \tilde{n} forme traceEx.: $n=3$ E ; $d = \text{disc. de } E$ $E' = k[x] / (x^2 - d)$ E et $k \times E'$ ont \tilde{n} forme trace.Cor:Si q est de rang impair ≥ 1 ,

vérifie la condition triviale,

on peut écrire $q = \langle 1 \rangle \oplus q_0$.Alors q forme trace a rang n $\Leftrightarrow q_0$ rang $n-1$

Dém. du thm de Rost:

On peut supposer $h \infty$.
 (Corps fini: il faut faire une vérification directe).

"déformations équitracées".

$$P_t = P - tQ \quad \left. \begin{array}{l} P \text{ unitaire de deg. } n \\ Q \text{ de degré } \leq n. \end{array} \right\}$$

P_t est unitaire de deg. n . $\text{Res}(P, Q) = 1$.

On suppose P séparable. $\text{disc}(P) \neq 0$.

Alors $\text{disc}(P_t) \neq 0$ pour tout $t \in \text{corps fini}$.

$$E_t = k[x]/(P_t) ; \mathcal{Q}_{E_t}$$

On dit que c'est une déformation "isotraccée" si on a

(*) ① $\mathcal{Q}_{E_t} \cong \mathcal{Q}_E + \text{générique} / h(t) \text{ ind.}$
 ou

② $\mathcal{Q}_{E_x} \cong \mathcal{Q}_E \quad \forall x \in h'$
 $h' \text{ ext. de } h / \text{disc}(P_x) \neq 0$

① \Leftrightarrow ②

(\Leftarrow clair ; \Rightarrow par spécialisation).

Thm: Si n est impair, pour tout E ,
 $\exists P \text{ et } Q \text{ tq}$
 1) Les E_t vérifient (*)
 2) $E \cong E_0 = k[x]/(P)$.

Admettons ce résultat pour l'instant.
 Choisissons $x \text{ tq } P - xQ$ ait une racine dans h .

p.ex. $x = \frac{P(\zeta)}{Q(\zeta)}$ pour $\zeta \in k$ tq $Q(\zeta) \neq 0$,
 et x tq $\text{disc}(P - xQ) \neq 0$.

$P - xQ = (x - \zeta) P_{n-1}$ où P_{n-1} est de deg. $n-1$.

Donc $E_x = k[x] E_{n-1}$.

N.B. : Pour cette dém., $Q \neq 0$ suffit.

[Mestre - J. of algebra - 131 (1990)]

"Presque tout polynôme P " signifie
 ts ceux dt les coeff. ne vérifient pas
 une eq. $F(a_1, \dots, a_n) = 0$ où F est un
 polynôme non identiquement nul.

Il faut démontrer que si P est général,
 il existe des polynômes Q et R avec
 $\deg Q, \deg R < n$

$$\begin{cases} \textcircled{1} PQ' - QP' = R^2 & (n \text{ impair}). \\ \textcircled{2} (P, Q) = 1 ; (P, R) = 1 \end{cases}$$

Construction :

$$P(x) = \prod (x - x_i)$$

$$\frac{Q}{P} = \sum \frac{q_i}{x - x_i} ; \quad \frac{R}{P} = \sum \frac{r_i}{x - x_i}$$

$$\left(\frac{Q}{P}\right)' = \frac{R^2}{P^2}$$

$$\text{i.e.} \quad \sum \frac{-q_i}{(x - x_i)^2} = \sum_{i \neq j} \frac{r_i r_j}{(x - x_i)(x - x_j)}$$

$$= \sum \frac{r_i^2}{(x - x_i)^2} + \sum_{i \neq j} \frac{r_i r_j}{x_i - x_j} \frac{1}{x - x_i}$$

Ceci donne $q_i = -r_i^2$.

On trouve que ça marche si les r_i est sol. du syst. $\sum_{i \neq j} x_{ij} r_i = 0$

avec $x_{ij} = \frac{1}{x_i - x_j}$.

Or (x_{ij}) est alternée (de de n pair) de type $n \times n$ avec n impair.

De \exists une soluto non triviale $(r_i) \neq (0, \dots, 0)$

En fait, on veut que les r_i soient tous $\neq 0$. C'est vrai pour le polynôme générique.

Puis c'est évident :

① + ② \Rightarrow (*) (isotrace).

(En cas : la dérivée a une valeur paire (\mathbb{R}^2))

$\begin{matrix} x \\ \downarrow^n \\ \mathbb{P}_1 \end{matrix}$ différentiable et u carré.)

Exple : $P = X^3 + pX + q$:

On peut écrire Q et $R \dots$

J. P. Serre

Cours au collège de France.

Le 06.12.93 IX-①

Formes traces en rang 4, 5, 6 et 7

On va voir :

- ① Caractérisation: quelles sont les p.q. à 4, 5, 6 et 7 variables qui sont des formes traces ?
- ② Applications aux propriétés de certains groupes: $2A_6, 2A_7, SL_2(\mathbb{F}_7), Q_{16}$

k est un corps de $\text{car} \neq 2$.

Dans ce dém., k sera le plus souvent supposé infini.

Rq: $\text{car } 2$

On a un analogue de la forme trace:

E/k de rang n .

$$\begin{array}{l}
 x \in E \quad E \rightarrow \bar{E} \\
 \quad \quad \quad x \mapsto \sigma(x)
 \end{array}$$

On remplace $\sum \nabla(x)^2$ par
 $f(x) = \sum_{\nabla \neq \bar{\nabla}} \nabla(x) \bar{\nabla}(x)$ (2nd coeff. du pol. car. de x).

f est une f.q., et si n est pair, elle est non dégénérée. Cela nous donne un invariant des algèbres étales.

Mais A.-P. Bergé et J. Martinet ont montré que f est déterminée par n et le disc. additif de E .

(disc. additif : $\Gamma_n \xrightarrow{\varphi} S_n \xrightarrow{\text{sgn}} \mathbb{Z}/2\mathbb{Z}$
 $\text{Hom}(\Gamma_n, \mathbb{Z}/2\mathbb{Z}) \cong k/\mathfrak{p}_k \quad \mathfrak{p}x = x^2 + x$).

Précisément :

$\frac{n}{2} - 1$ fois forme hyperbolique $\oplus x^2 + xy + by^2$.

Exercice : nq il y a pas d'invariant des alg. étales en car. 2 normalisés, à valeurs dans le qpe de Brauer non nul.

Le rang 4

E alg. étale / k de rang $n=4$.

\mathcal{Q}_E contient $\langle 1 \rangle$.

$\mathcal{Q}_E = \langle 1 \rangle \oplus \mathcal{Q}_E \quad \text{rg } \mathcal{Q}_E = 3$.

On désire caractériser les formes \mathcal{Q}_E de rang 3 qui interviennent.

Prop.: Soit Q une forme de rang 3, de discriminant d . Il y a équivalence entre:

- (1) $\kappa_3(Q) = 0$ dans $H^3(k, \mathbb{Z}/2\mathbb{Z})$.
- (2) d est représenté par la 2-forme de Pfister $\langle 1 \rangle \oplus \langle d \rangle \oplus Q$.
- (3) 1 est représenté par $\langle d \rangle \oplus Q$.
- (4) $d_1 Q = 0$ dans κ_h (ou $\text{Gr} \kappa_h$).
i.e. $\underset{1}{d^0} Q - \underset{Q}{d^1} Q + d^2 Q - d^3 Q = 0$
- (5) Il existe $a \in k^*$ représenté par Q tel que $(a)(d) = 0$ dans $H^2(k)$.
- (6) Il existe $A, B \in k^*$ $A^2 - B \neq 0$ t.q. $Q \simeq \langle A, A^2 - B, AB(A^2 - B) \rangle$.

Requis:

- Notat° : $d_k q = \sum_{i=0}^{\infty} t^i d^i q$ (q forme quad.)
- Si $d(Q) = 1$, $\langle 1 \rangle \oplus Q$ est une 2-forme de Pfister. ($Q = \langle a, b, ab \rangle \rightarrow \langle 1 \rangle \oplus Q = \langle 1, a, b, ab \rangle$).

On a alors:

Thm: Pour qu'il existe une alg. étale E de rang 4 avec $Q_E = \langle 1 \rangle \oplus Q$, il faut et il suffit que Q satisfasse aux propriétés (1) à (6).

Dém. du thm. :

1) Il faut voir que si E est une alg. étale, \mathcal{Q}_E satisfait aux conditions (1), ..., (6).

p.expe.: (1) est vraie. (thm gal sur les K_i ; on est en rang 1).

2) Réciproquement, on a:

Lemme: Soient $A, B \in K^*$, $A^2 - B \neq 0$.
 Soit $F(x) = x^4 - 2Ax^2 + B$.
 $E_{A,B} = K[x]/(F)$. Alors
 $\mathcal{Q}_{E_{A,B}} = \langle 1 \rangle \oplus \langle A, A^2 - B, AB(A^2 - B) \rangle$

Preuve:

$$d(E_{A,B}) \sim B.$$

$E_{A,B} \supset \{1, x, x^2 - A\}$. Ils sont 2 à 2 orthogonaux
 image de x

$$\text{et } \text{Tr}(1^2) = 4 \sim 1; \text{Tr}(x^2) = 4A \sim A;$$

$$\text{Tr}[(x^2 - A)^2] = 4(A^2 - B) \sim A^2 - B.$$

Donc \mathcal{Q}_E sous-esp. de dim 3 $\sim \langle 1, A, A^2 - B \rangle$.

D'où $\mathcal{Q}_E = \langle 1, A, A^2 - B, y \rangle$ et en comparant les discriminants on obtient $y = AB(A^2 - B)$.

Rq: Ce calcul permet aussi de voir le sens 1). En effet:

Si k'/k ext. de degré impair,
 $\Leftrightarrow Q$ satisfait (1), ..., (6) sur k'
 $\Leftrightarrow Q$ sur k .

(par exple:
c'est évident pour (1) : cohomologie C_0 cohom.
 (2) : thm de Springer)

On peut donc supposer que $\mathcal{C}(\Gamma_h) \subset S_4$
 est contenu dans un 2-sylow Δ_4 de S_4 .

Lemme: Qd on a une extension \tilde{a} qpe
 Δ_4 , il existe un polynôme bicarré
 qui définit l'alg. étale correspondante

$$\begin{array}{c}
 E \\
 2 \mid \\
 E_2 \\
 2 \mid \\
 k
 \end{array}
 \quad
 \begin{array}{l}
 E = E_2(\sqrt{x}) \quad x \in E_2 \\
 x^2 - 2ax + b = 0 \text{ sur } k \text{ convient.} \\
 (k \neq \emptyset; \text{ donc on peut supposer } x \notin k)
 \end{array}$$

Démonstration de la propriété:

(2) (3) (4) (5) et (6) st équivalentes par
 des arguments élémentaires. Par contre,
 (1) \Rightarrow les autres utilise le thm de
 Nerukjev-Suslin.

Parz: Le thm nous dit dc que
 $n=4$, les formes traces sont caractérisées
 par $\left\{ \begin{array}{l} \textcircled{1} \text{ la condition triviale.} \\ \textcircled{2} N_3 = 0. \end{array} \right.$

Autre qtz: Dém. directe de (4).

$$q_E = \langle 1 \rangle \oplus Q_E \quad d_{-1} Q_E \stackrel{!}{=} 0.$$

Grâce à la caractérisation générale de la nullité des invariants de Witt, il suffit de vérifier (4) lorsque

$$E = E_1 \times E_2, \quad \text{rg } E_i = 2.$$

Dans ce cas $q_E = \langle 2, 2d_1 \rangle \oplus \langle 2, 2d_2 \rangle$
 où $d_i = \text{disc}(E_i)$.

$$\text{De } q_E = \langle 1, 1, \alpha, \beta \rangle \text{ i.e. } Q_E = \langle 1 \rangle \oplus f.$$

$$\text{Mais } d_E Q_E = d_E \langle 1 \rangle d_E f = (1+t) d_E f.$$

$$\text{De } d_{-1} Q_E = 0.$$

(2) \Leftrightarrow (3) est triviale.

(1) \Leftrightarrow (2) par Nerhunjev-Suscin:

Nerhunjev-Suscin dit:

Si D alg. de quat. définie par (a, b)
 et $q_{a,b}$ la forme norme $\langle 1, -a, -b, ab \rangle$
 Soit $c \in k^*$. c est représenté par $q_{a,b}$
 $\Leftrightarrow (a)(b)(c) = 0$ dans $H^3(k)$.

Ou (de façon équivalente)

Si F est une 3-forme de Pfister,
 F n'est pas dans Wk (F hyperbolique)
 \Leftrightarrow Inv. d'Arason de $F = 0$ dans $H^3(k)$.

[En effet
 c représenté par $q_{a,b} \Leftrightarrow q_{a,b} \otimes \langle 1, -c \rangle$
représenté 0 $\Leftrightarrow q_{a,b} \otimes \langle 1, -c \rangle$ est hyperbol.]

Ici :

$$Q = \langle -a, -b, ab \rangle \otimes \langle d \rangle.$$

$$\Delta \langle 1 \rangle \oplus \langle d \rangle \otimes Q = \langle 1, -a, -b, ab \rangle = q_{a,b}$$

Donc on doit considérer $(d)(a)(b) \in H^3(k)$

Puis :

$$N_3(q) = (-ad)(-bd)(abd)$$

$$= (-a)(-bd)(bd) + (d)(-bd)(abd) \quad (\text{car } (a)(-a) = 0)$$

$$= (d)(b)(abd) = (d)(b)(-ab) = (d)(b)(a) !$$

(4) \Rightarrow (2)

$$(4) \text{ s'écrit } \lambda^0 Q - \lambda^1 Q + \lambda^2 Q - \lambda^3 Q = 0$$

$$\text{avec } \lambda^0 Q = \langle 1 \rangle$$

$$\lambda^1 Q = Q$$

$$\lambda^2 Q = \langle d \rangle \otimes Q \quad (\lambda^{n-1} q = \langle d \rangle \otimes q$$

$$\lambda^3 Q = \langle d \rangle \quad \text{si } q \text{ de rang } 1).$$

De

$$(4) \text{ s'écrit } \langle 1 \rangle \oplus \langle d \rangle \otimes Q \cong Q \oplus \langle d \rangle$$

Ainsi (4) \Rightarrow (2) est clair.

(2) \Rightarrow (4)

Réciproquement, (2) entraîne

$$\langle d \rangle \otimes (\langle 1 \rangle \oplus \langle d \rangle \otimes Q) \cong \langle 1 \rangle \oplus \langle d \rangle \otimes Q.$$

Forme \nearrow de Pfister.

C'est (4).

(3) \Rightarrow (5) :

On veut de montrer qu'il existe $a \in k^*$ représenté par Q avec $(a)(d) = 0$.

D'après (3), il existe $a \in k$ et $x \in k + \mathfrak{q}$ $1 = dx^2 + a$, a représenté par Q .

Grâce au lemme suivant, on peut choisir $a \neq 0$:

Lemme: $(k \text{ inf})$ Si x est représenté par $f_1 \oplus f_2$, avec $\text{rg } f_i \geq 1$, alors $\exists x_1$ et x_2 tq $x = f_1 x_1 + f_2 x_2$ avec $f_1 x_1 \neq 0$ et $f_2 x_2 \neq 0$.

Ce a convient car

$$(a)(d) = (1 - dx^2)(d) = (1 - dx^2)(dx^2) = 0.$$

(5) \Rightarrow (6) :

$\exists a \in k^*$ rep. par Q avec $(a)(d) = 0$.

On veut mq $\exists A, B \in k^*$, $A^2 - B \neq 0$ t.q.

$$Q \simeq \langle A, A^2 - B, AB(A^2 - B) \rangle.$$

On sait qu'on peut écrire Q sous la forme $Q = \langle a, b, c \rangle$ $b, c \in k^*$.

$$(a)(d) = 0 \Rightarrow a = u^2 - dv^2 \quad u, v \in k^*.$$

$$\text{On pose : } A = b; \quad B = abc \left(\frac{bv}{u}\right)^2.$$

$$\begin{aligned} A^2 - B &= b^2 - abc \frac{bv^2}{u^2} \\ &= b^2 \left[\frac{u^2 - abc v^2}{u^2} \right] = b^2 \left[\frac{u^2 - dv^2}{u^2} \right] \\ &= b^2 \frac{a}{u^2} \simeq a. \end{aligned}$$

On peut donc écrire

$$Q \simeq \langle A^2 - B, A, AB(A^2 - B) \rangle.$$

$$(\langle AB(A^2 - B) \rangle \simeq \langle abcacnac \rangle).$$

(6) \Rightarrow (3) reste à voir.

Il s'agit

$$\langle A, A^2 - B, AB(A^2 - B) \rangle \simeq \langle AB, A^2 - B, A(A^2 - B) \rangle$$

(en effet

$$\langle 1, B(A^2 - B) \rangle \simeq \langle B, A^2 - B \rangle \text{ car}$$

$$\langle B, A^2 - B \rangle \text{ représente } A^2, \text{ donc } 1).$$

De $d = B$, et $A^2 - B$ est représenté par la forme et vérifie $(B)(A^2 - B) = 0$.

Résultat également obtenu par Epherbus et Krüskemper.

Corollaires (vrais pour $n = 4, 5, 6$).

- ① q est forme trace sur k ssi elle l'est sur une extension de degré impair de k .
- ② Si q est forme trace, il existe une alg. étale E à gpe de Galois G et une 2 gpe avec $q_E = q$.
("à gpe de Gal." : correspondait à un $\varphi: \Gamma_k \rightarrow S_n$ tq $\text{Im}(\varphi)$ est une 2 gpe).

$$\boxed{n=5}$$

q est une forme trace

$$\Leftrightarrow \begin{cases} q \text{ contient } \langle 1 \rangle & q = \langle 1 \rangle \oplus q_4 \\ \text{et} & \\ q_4 \text{ est forme trace a rang 4.} & \end{cases}$$

$$\boxed{n=6} \quad G = 2+4.$$

De la condition triviale pour q est
contenir $\langle 1, 2 \rangle$.

$$q = \langle 1, 2 \rangle \oplus Q \text{ avec } \text{rg } Q = 4.$$

$$d(Q) = 2d \text{ si } d = d(q).$$

Thm: Pour que $q = \langle 1, 2 \rangle \oplus Q$ soit
forme trace, il faut et il
suffit que

(*) $\mathbb{1}$ est représenté par Q sur
le corps $k(\sqrt{2d})$ $d = \text{disc}(q)$
ou de façon équivalente
 q contient $\langle 1, 1, 2 \rangle$ sur $k(\sqrt{2d})$.

Démonstration:

1) Nécessité: Montrons que q_E contient
 $\langle 1, 1, 2 \rangle$ sur $k(\sqrt{2d})$.

Quitte à changer de corps, on peut supposer que $d \geq 2$ (i.e. $h = h(\sqrt{2d})$).

On fait une extension de degré impair de façon à ce que $\varphi(\Gamma_h)$ soit un 2 qpe.
D'où une décomposition $E = E_4 \times E_2$ avec $\text{rg } E_i = i$.

$$\text{On a } q_E = q_{E_4} \oplus q_{E_2}$$

$$q_{E_4} = 1 \oplus Q_3 ; q_{E_2} = \langle 2, 2x \rangle .$$

$$\text{Dc } q_E = \langle 1, 2, 2x \rangle \oplus Q_3$$

$$\text{D'où } d(Q_3) = 2x .$$

$$\text{On a dc } q_E = \langle 1, 2 \rangle \oplus \langle d(Q_3) \rangle \oplus Q_3$$

Mais $Q = \langle d(Q_3) \rangle \oplus Q_3$ représente 1 par le lemme précédent (rang 4).

2) Suffisance.

Lemme: Soit f un f.q. de rang ≥ 2 .

Soit $x, y \in h^*$. Il y a équivalence entre :

$$\begin{aligned} \uparrow (1) & f \supset \langle x, y \rangle \text{ avec } (x)(xy) = 0 \\ \Downarrow (2) & f \text{ représente 1 sur } h(\sqrt{x}) . \end{aligned}$$

Preuve du Lemme:

(1) \Rightarrow (2) :

Il faut voir que $\langle x, y \rangle$ représente
 1 sur $k(\sqrt{x})$. On est ramené à $x=1$.
 Mais $(x)(y) = 0$ signifie qu'il y a une
 solution non triviale de $Z^2 - xX^2 - yY^2 = 0$
 D'où une représentation de 1 par $\langle x, y \rangle$.

(2) \Rightarrow (1) :

Il existe des vecteurs v_1 et v_2 tels que
 $1 = f(v_1 + \sqrt{x} v_2)$.

i.e. $1 = f(v_1) + x f(v_2) + 2\sqrt{x} f(v_1, v_2)$.

D'où $v_1 \perp v_2$. Posons $\begin{cases} f(v_1) = x \\ f(v_2) = y \end{cases}$

$$f \circ \langle x, y \rangle \quad \text{et} \quad 1 = x + xy \\ \Rightarrow (x)(xy) = 0.$$

Pour achever la démon. du thm, on
 applique ce lemme avec $x = 2d$.

$$Q \supset \langle x, y \rangle \text{ avec } (x)(2dy) = 0.$$

$$q = \langle 1, 2, x, y \rangle \oplus q_2 \quad \text{rg } q_2 = 2$$

$$q = \langle 2, y \rangle \oplus q_4 \text{ avec } q_4 = \langle 1, x \rangle \oplus q_2.$$

$\langle 2, y \rangle$ est une forme trace.

Il $\exists E_2$ étale de $\text{rg } 2$ avec

$$\langle 2, y \rangle = q_{E_2}.$$

De $\bar{\mathbb{F}}$, $\exists E_4$, étale de $\text{rg } 4$, avec

$$q_{E_4} = \langle 1, x \rangle \oplus q_2.$$

(En effet, $\langle x \rangle \oplus q_2$ vérifie bien
ces propriétés (1) à (6) précédentes;

$$(5) \text{ p. explic. : } (x)(d(q_4)) = 0$$

$$\text{car : } d = d(q) = (2y d(q_4))$$

$$\text{De } d(q_4) = (2dy) \text{ et on a bien } (x)(2dy) = 0 \quad \text{).}$$

L'automorphisme externe de S_6

$$A_6 \cong \text{PSL}_2(\mathbb{F}_9)$$

X dte projective sur \mathbb{F}_9 .

A_6 peut se représenter comme:

Les permutations de la forme

$$z \mapsto \frac{az+b}{cz+d} \quad a, b, c, d \in \mathbb{F}_9$$

$$ad - bc = \begin{cases} 1 \\ \text{carré} \end{cases}$$

On a envie d'agrandir A_6 en ajoutant

$$\left\{ \begin{array}{l} z \mapsto \frac{az+b}{cz+d} \quad ad - bc \neq 0 \\ z \mapsto \bar{z} \quad \text{où } - \text{ autom. de } \mathbb{F}_9 = \mathbb{F}_3(i) \\ \quad \quad \quad i \mapsto -i \end{array} \right. \quad A_6 \cdot 2$$

On obtient $A_6 \subset A_6 \cdot 2^2$.

Le quotient est de type $(2, 2)$.

L'un des quotients intermédiaires est S_6 .

(En particulier, \rightarrow c'est scindé sur chaque gpe d'ordre 2).

Soit $\sigma \in \text{Aut}(S_6) - S_6$.

E alg. étale de rang 6.

E_σ autre — qui lui correspond par σ .

Pb: q_{E_σ} a t-oms de q_E ?

(On sait d'avance que c'est possible).

Ecrivons $q_E = \langle 1, 2 \rangle \oplus Q_E$

$q_{E_\sigma} = \langle 1, 2 \rangle \oplus Q_{E_\sigma}$

La formule devient

$$Q_{E_\sigma} = d^3 Q_E$$

(3^{ème} puissance extérieure).

Si $d = d(E) = d(E_\sigma)$, cette formule équivaut à

$$Q_{E_\sigma} = \langle 2d \rangle \otimes Q_E$$

Cas particulier: $d=1$ ($\varphi(\Gamma_h) \subset A_6$)

$$Q_{E_\sigma} \simeq \langle 2 \rangle \otimes Q_E.$$

$Q_{E_\sigma} \simeq \langle 2 \rangle \otimes Q_E$ (On a des contre-exemples dans ce cas q_{AE}).

Dém: $A, B, C \in h^*$, $A^2 - B \neq 0$

$$F_{A,B} = X^4 - 2AX^2 + B \quad E_{A,B} \text{ rg } 4$$

$$F_C = X^2 - C \quad E_C \text{ rg } 2$$

$$E_{A,B,C} = E_{A,B} \times E_C$$

On cherche à calculer le transformé de $E_{A,B,C}$ par σ .

$$\text{Posons } \begin{cases} A' = 2AC \\ B' = 4C^2(A^2 - B) \\ C' = BC(A^2 - B) \end{cases}$$

Assertion : $E_{A',B',C'} \stackrel{\sigma}{\sim} (E_{A,B,C})_{\sigma}$

Une telle algèbre correspond à un

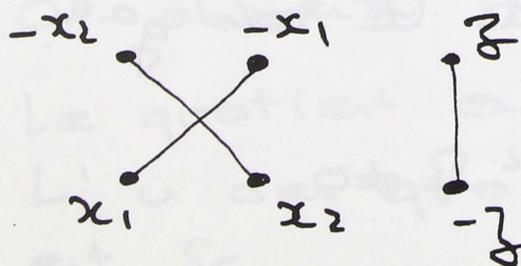
$$\varphi: \Gamma_h \longrightarrow D_4 \times C_2 \xrightarrow{\sigma} S_6$$

2 Sylow \searrow

Les racines de $X^4 - 2AX^2 + B = 0$ peuvent s'écrire $x_1, -x_1, x_2, -x_2$ avec $x_i^2 = y_i$, y_1 et y_2 racines de $X^2 - 2AX + B = 0$.

Les racines de $X^2 - C$ sont z et $-z$.

Act^o de Galois : gpe d'automorphismes de la figure :



On constate que les racines de l'équation ' sont

$$\begin{cases} x'_1 = \sqrt[3]{x_1 + x_2} \\ x'_2 = \sqrt[3]{-x_1 + x_2} \\ \sqrt[3]{3} = \frac{1}{2} \sqrt[3]{x_1 x_2 (y_1 - y_2)} \end{cases}$$

Reste à voir que l'act° est la torsion par σ .

par exple : $(12) \mapsto (12)(34)(56)$
 $(12)(34) \mapsto (12)(34)$

$$\begin{matrix} x_i \text{ inv.} \\ \sqrt[3]{} \mapsto -\sqrt[3]{} \end{matrix} \quad \left. \vphantom{\begin{matrix} x_i \text{ inv.} \\ \sqrt[3]{} \mapsto -\sqrt[3]{} \end{matrix}} \right\} \begin{cases} x'_1 \mapsto -x'_1 \\ x'_2 \mapsto -x'_2 \\ \sqrt[3]{3} \mapsto -\sqrt[3]{3} \dots \end{cases}$$

Avec cette assertion, il ne reste plus qu'à calculer $Q_{E_{A', B', C'}}$.

On trouve $\langle 2d \rangle \otimes Q$.

[Ceci suffit car on peut faire des extensions de degré impair].

Rigue En fait, pour prouver $Q_E = d^3 Q$, on peut supposer $E = L_2 \times L'_2 \times L''_2$ alg. de rang 2

i.e. $\varphi(\sqrt{h}) \subset (2, 2, 2) \subset S_6$.

(Cela revient à supposer $A^2 = B$ et u carré.)
 Mais l'alg. tordue n'est plus un produit
 de 3 quadratiques. ((2,2,2) n'est pas
 envoyé sur lui-même). Donc ici
 cela ne simplifie pas vraiment.

Pqn: En car 0.

S_n ; rep. orthogonale de S_n sur \mathbb{Q} .

E alg. étale de rang n .

$\varphi: \Gamma_n \rightarrow S_n$; $V_\varphi = V$ tordu par φ .

On obtient ainsi un invariant Witt
 par $E \mapsto q_E(V) \in Wk$.

La s'écrit comme combi. lin.
 des $d^i q_E$.

[Ce qu'on vient de faire pour S_6 est
 un cas particulier de cela avec
 $S_6 \xrightarrow{\varphi} S_6 \subset O_6$].

PRm: L'anneau des rep. lin. sur \mathbb{Q} du
 type S_n est engendré (comme d-
 anneau) par la rep. linéaire
 de deg. n évidente $S_n \rightarrow GL_n$.

De l'anneau des rep. orthogonales

$$RO(S_n) \cong W(\mathbb{Q}) \otimes R(S_n).$$

J.-P. Serre A
Cours au collège
de France.
Le 13 décembre 93

X - (1)

On va appliquer les résultats précédents
aux toiseurs sous le gpe $\tilde{A}_6 = 2A_6$.

On a

$$\begin{array}{c} \tilde{A}_6 \\ | \\ A_6 \subset S_6 \end{array}$$

Etant donné h $\text{car } h \neq 2$
et $\varphi: \Gamma_h \rightarrow S_6$ $\Leftrightarrow E$ alg.
ét. de rang 6.

q_E forme trace de rang 6.

$\chi_i(q_E)$ avec $\chi_1 = (d)$ $d = \text{disc}(E)$
 $= \text{disc}(q_E)$.

φ à valeurs dans $A_6 \Leftrightarrow \chi_1 = 0$
(i.e. $d = 1 \text{ ds } h^*/h^{*2}$)

Si $\chi_1 = 0$, on a vu $\chi_2 = \chi_2^q$ 2^{de} classe gal.

Mais χ_2^q est l'obstruction à relever φ
à \tilde{A}_6 .

En particulier

$\chi_2 = 0 \Leftrightarrow$ il existe $\tilde{\varphi}: \Gamma_h \rightarrow \tilde{A}_6$
qui relève φ .

On s'intéresse aux algèbres étalées E avec $\kappa_1 = \kappa_2 = 0$. [Cela revient à considérer les \tilde{A}_6 torseurs modulo la torsion quadratique].

Question: Quelles st les formes traces correspondantes ?

Thm: Soit q une f.q. à 6 variables avec $\kappa_1 = \kappa_2 = 0$. Pour que q soit forme trace, il faut et il suffit qu'il existe $c \in k^*$ avec

- ① $q = \langle 1, 1, c, c, c, c \rangle$
- ② $(2)(c) = 0$ (i.e. $\exists x, y \in k$ tq $c = x^2 - 2y^2$)
- ③ c est une somme de 4 carrés dans $k(\sqrt{2})$.

Rqur: (i) $\Rightarrow \kappa_1 = \kappa_2 = 0$
 $(\kappa_2 = \sum_{6 \text{ fois}} (c)(c) = 0 \text{ car } 6 \equiv 0 \pmod{2})$.

Cor: \exists des algèbres étalées E avec $\kappa_1 = \kappa_2 = 0$ et $q_E \neq \langle 1, 1, \dots, 1 \rangle$.

$$\underline{\text{Rqre:}} \langle 1, 1, c, c, c, c \rangle = \langle 1, 1 \rangle \oplus \langle c \rangle \underbrace{\langle 1, \dots, 1 \rangle}_{\text{forme de Pfister}}$$

Donc

$$\langle c, c, c, c \rangle \simeq \langle c', c', c', c' \rangle \Leftrightarrow c'/c \text{ est représentée par } \langle 1, 1, 1, 1 \rangle \text{ i.e. est } \boxed{4}$$

Et si c n'est pas $\boxed{4}$, alors $q_E \neq \langle 1, 1, 1, 1, 1, 1 \rangle$

On utilise maintenant Keruev. Suscin.
 c est $\boxed{4} \Leftrightarrow (-1)(-1)(c) = 0$ dans $H^3(k)$.

De si l'on associe à E $(-1)(-1)(c) \in H^3(k)$,
 on obtient un inv. corom. $a(E) \in H^3(k)$,
 et $q_E \simeq q_{E'} \Leftrightarrow a(E) = a(E')$.

(N.B. a est un inv. corom. pour \tilde{A}_6).

Démonstration:

① Supposons que q satisfasse à ①, ② et ③, et montrons que c'est une forme trace. On applique le critère qu'on a vu la dernière fois.

Conditions: $\begin{cases} q \text{ contient } \langle 1, 2 \rangle \\ q \text{ contient } \langle 1, 1, 2 \rangle \text{ sur } k(\sqrt{d}) \\ \parallel \\ k(\Gamma) \end{cases}$
 (ici $d=1$).

④

Rqre: $(a)(b) = 0 \Leftrightarrow \langle a, b \rangle \simeq \langle 1, ab \rangle$.

Donc ② donne $\langle 2, c \rangle \simeq \langle 1, 2c \rangle$.

Or $q = \langle 1, 1, c, c, c, c \rangle = \langle 2, 2, c, c, c, c \rangle$.

D'où $q = \langle 2, 1, 2c, c, c, c \rangle$ et q contient $\langle 1, 2 \rangle$

Puis ③ nous dit que c est \square sur $h(\sqrt{2})$.

Donc $\langle c, c, c, c \rangle \simeq \langle 1, 1, 1, 1 \rangle$ sur $h(\sqrt{2})$.

Ainsi sur $h(\sqrt{2})$ $q \simeq \langle 1, 1, 1, 1, 1, 1 \rangle$ et contient bien $\langle 1, 1, 2 \rangle$.

Les deux conditions sont satisfaites.

② Réciproquement

On va utiliser le résultat suivant:

Prop.: Soit Q une forme de rang 5.
Soient $a, b \in k^*$, et soit $q_{a,b}$ la forme norme associée à (a, b) ,
 $q_{a,b} = \langle 1, -a, -b, ab \rangle$.
Il y a équivalence entre:

- ① $N_1(Q) = 0$; $N_2(Q) = (-1)(-1) + (a)(b)$
- ② $\exists c \in k^*$ tq $Q \simeq \langle 1 \rangle \oplus \langle c \rangle \oplus q_{a,b}$

Preuve:

② \Rightarrow ① : c'est du calcul.

① \Rightarrow ② : On regarde $Q_6 := \langle -1 \rangle \oplus Q$.
 Cette forme a les mêmes κ_1 et κ_2
 que la forme $\langle 1, -1 \rangle \oplus q_{a,b}$.

Par un thm. de Pfister (Inv. I p. 123;
 assertion 3'), ceci implique que
 Q_6 est isotrope.

Donc Q représente 1. $Q = \langle 1 \rangle \oplus Q_4$,
 avec $\kappa_1(Q_4) = 0$ et $\kappa_2(Q_4) = (-1)(-1) + (a)(b)$.

Ceci implique $Q_4 = \langle c \rangle q_{a,b}$ où c
 est n'importe quelle valeur de Q_4 .
 [$Q_4 = \langle 1 \rangle \oplus Q_3$ et Q_3 est déterminée
 par ses invariants κ_1 et κ_2].

Ici, $a = b = -1$. La proposition nous
 dit que si $\kappa_1(Q) = \kappa_2(Q) = 0$, alors
 $Q = \langle 1, c, c, c, c \rangle$, $c \in k^*$.

$E; q_E$.

La condition triviale dit que q représente 1.

Donc $q = \langle 1 \rangle \oplus Q$ avec $\text{rg } Q = 5$.

$Q \cong \langle 1, c, c, c, c \rangle$, $c \in k^*$ grâce à la proposition précédente. On a donc bien

$$\textcircled{1} \quad q_E = \langle 1, 1, c, c, c, c \rangle.$$

On veut maintenant modifier c pour qu'il vérifie $\textcircled{2}$.

$q = \langle 1 \rangle \oplus Q$
 q contient $\langle 1, 2 \rangle \Rightarrow Q$ représente 2.

$$Q = \langle 1 \rangle \oplus \langle c, c, c, c \rangle = \langle 1 \rangle \oplus Q_4.$$

On peut de écrire $2 = x^2 + y$ avec y représenté par Q_4 , et on peut supposer x et $y \neq 0$.

Mais si $y \in k^*$ est représenté par Q_4 , alors $Q_4 \cong \langle y, y, y, y \rangle$.

On choisit $c = y$.

$2 = x^2 + c$ implique $(2)(c) = 0$. C'est $\textcircled{2}$.

($(2)(c) = 0 \Rightarrow c = x^2 - 2y^2$. De ce fait
 on a $(2)(-c) = 0$. Mais $(2)(-1) = 0$.
 On a déduit $(2)(c) = 0$.)

Reste à prouver $\textcircled{3}$, i.e. $q_E \cong \langle 1, \dots, 1 \rangle$
 sur $k(\sqrt{2})$.

le 13.12.93

X - 7

Mais $q_E \supset \langle 1, 1, 2 \rangle = \langle 1, 1, 1 \rangle$ sur $k(\sqrt{2})$

De $q_E \cong \langle 1, 1 \rangle \oplus Q_4$ avec Q_4 représenté 1.

Autrement dit $Q_4 = \langle 1, \dots, 1 \rangle$.

Ainsi $\langle c, c, c, c \rangle \cong \langle 1, 1, 1, 1 \rangle$ sur $k(\sqrt{2})$

ce qui signifie $c = \boxed{4}$ sur $k(\sqrt{2})$.

Déf.: On dira que k a la propriété O_6 si pour toute algèbre étale de rang 6 sur k avec $\alpha_1 = \alpha_2 = 0$ on a $q_E \cong \langle 1, 1, \dots, 1 \rangle$.

$\forall c \in k^*$,

$O_6 \iff$ Pour tout $c \in k^*$

$$2c = 0$$

$c = \boxed{4}$ dans $k(\sqrt{2}) \implies c = \boxed{4}$ dans k .

On va regarder quels corps ont cette propriété.

Défa.

1) Si $(-1)(-1) = 0$ dans $H^2(k)$, O_6 est vraie car tout élément est $\boxed{4}$

2) En part., si $\text{car } k \neq 0$, O_6 est vraie.

3) De \hat{m} , si -1 est un carré, _____

4) _____, -2 _____, _____

5) Si k est un corps de nombre (ou un corps local, à c.v. fini), O_6 est vraie.

(En effet, il faut simplement vérifier $\langle -c, 1, 1, 1 \rangle$ est indéfini pour toutes les places réelles de k . Mais place réelle de $k \mapsto$ place réelle de $k(\sqrt{2})$)

6) Si k vérifie O_6 , il en est de même de $K = k(T)$, T indéterminée.

(la dém. sera vue un peu plus tard).

De il faut chercher un contre exemple sur des variétés qui ne sont pas rationnelles.

Pb: Y a-t-il une courbe elliptique C/\mathbb{Q} dont le corps de points ne vérifie pas O_6 ?

De façon plus générale :

Pb 2: Quel est le deg. de tr $/\mathbb{Q}$ minimum d'un corps k ne vérifiant pas O_6 ?

Un espace de corps ne satisfaisant pas à \mathcal{O}_6 .

Q quadrique $X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2 + 7 = 0$.
 $[\varphi = \langle 1, 1, 1, 1, 7 \rangle$. $X = \mathcal{Q}(\varphi)$ quadrique projective définie par $\varphi = 0$.]

$h = \mathcal{Q}(X) = \mathcal{Q}(X_1, X_2, X_3, X_4, \sqrt{7 - X_1^2 - \dots - X_4^2})$.
 Sur ce corps, $c = -1$ convient.

Preuve:

On doit vérifier:

② $(2)(c) = (2)(-1) = 0$.

③ $c = \boxed{4}$ dans $h(\sqrt{2})$.

On va utiliser $7 = \boxed{3}$ sur $\mathcal{Q}(\sqrt{2})$
 $\neq \boxed{3}$ sur \mathcal{Q} .

Sur $h(\sqrt{2})$ $X_1^2 + X_2^2 + \dots + X_5^2 + X_1^2 + X_2^2 + X_3^2 = 0$.

De la forme $\langle 1, \dots, 1 \rangle$ de \mathbb{F}_8 représente 0:
 elle est hyperbolique, et $\langle 1, 1, 1, 1 \rangle \cong \langle -1, -1, -1, -1 \rangle$.
 D'où $-1 = \boxed{4}$ sur $h(\sqrt{2})$.

Supposons maintenant $-1 = \boxed{4}$ sur $h = \mathcal{Q}(\varphi)$
 C'est équivalent à $\varphi = \langle 1, \dots, 1 \rangle$ de \mathbb{F}_8
 est hyperbolique sur $\mathcal{Q}(\varphi)$.

Théorème (W. Scharlau ; p. 155 + Thm 5.4 (ii)) :
 Si on a deux f.q. φ et ψ qui représentent
 1 toutes les deux t.q. φ anisotrope,
 et ψ hyperbolique sur $ho(\varphi)$, alors
 $\varphi \succeq \psi$.

Grâce à ce résultat, on obtient

$$\langle 1, \dots, 1 \rangle = \langle 1, 1, 1, 1, 1, 7 \rangle \oplus \langle x, \mathbb{R} \rangle.$$

Thm de simplification de Witt :

$$\langle 1, 1, 1 \rangle \simeq \langle 7, x, \mathbb{R} \rangle \text{ i.e. } 7 = \boxed{3} / \mathbb{Q}.$$

C'est faux !

On va maintenant démontrer 6)

Prop. : Soit K un corps muni d'une v.d. v
 de corps résiduel k , car $k \neq 2$.

Soit $c \in K^*$ t.q. $(2)(c) = 0$ et
 $c = \boxed{4}$ dans $K(\sqrt{2})$.

Soit $e_c = (-1)(-1)(c) \in H^3(K)$.

Alors $\text{res}(e_c) = 0$ (ds $H^2(k)$).

Notons $e_c = (-1)(-1)(c) \in H^3(K)$.

On veut montrer que $e_c = 0$.

Mais, les résidus de e_c sont nuls.

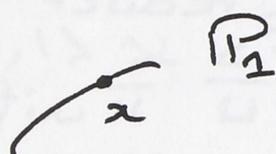
Donc e_c est cte, i.e. $e_c \in H^3(k)$

($0 \rightarrow H^i(k) \rightarrow H^i(K)$).

Reste à voir que c'est 0.

Pour cela, on spécialise.

k de car 0. Donc $k \cong \mathbb{F}_2$.



On peut donc choisir un point rationnel $x \in \mathbb{P}^1(k)$ tq $c(x) \neq 0, \infty$.

Alors $c(x) = \tilde{c} \in k^*$.

$$e_c(x) = (-1)(-1)(\tilde{c})$$

$$= e_c$$

De on peut écrire la valeur cte e_c sous la forme $(-1)(-1)(\tilde{c})$ où

$$\tilde{c} = c(x).$$

Mais $(2)(\tilde{c}) = 0$ (par spécialisation, de $(2)(c) = 0$).

et $(-1)(-1)(\tilde{c}) = 0$ sur $k(\sqrt{2})$. (Idem).

Donc k a la propriété D_6

$$(-1)(-1)(\tilde{c}) = 0.$$

c'est ce qu'on voulait.

On va maintenant appliquer ça au pb de Noether:

G gpe fini; $G \subset S_n$.

$$\mathbb{Q}(T_1, \dots, T_n)^G = K.$$

Question: Quand K est-il une extension pure de \mathbb{Q} ?

- Pour S_n , c'est vrai.
- On a des ctrs explic. (gpe cyclique d'ordre 47!).

Si G est un sous-gpe de \tilde{A}_7 d'indice impair (i.e. contenant un 2-Sylow), alors un tel K n'est pas une extension pure de \mathbb{Q} .

On va en fait montrer un résultat plus fort:

Soit T/K un G torseur versé (e.c.w.o.)
Alors K n'est pas une ext. pure de \mathbb{Q} .

Exemples de tels s_2 gpes: (pas de torseurs versés rationnels sur \mathbb{Q})

$2\text{Sylow} \cong \mathbb{Q}_{16}$ (quat.)

$\tilde{A}_6 = 2 \cdot A_6$; $\tilde{A}_7 = 2 \cdot A_7$; $SL_2(\mathbb{F}_7)$.

$$\left[\begin{array}{ccc} \text{PSL}_2(\mathbb{F}_7) & \cong & \text{SL}_3(\mathbb{F}_2) \hookrightarrow \text{A}_7 \\ 168 & \uparrow & \uparrow \\ \text{SL}_2(\mathbb{F}_7) & \longrightarrow & 2 \cdot \text{A}_7 \end{array} \right]$$

Démonstration:

Soit K de caract. o tel qu'il existe un G torsueur versel sur K .

Le corps K n'a pas la propriété O_6 . (En effet, s'il e'avait, tout corps de caract o e'aurait aussi).

G torsueur $L/h \mapsto a(L) \in H^3(h)$.

$$(G \subset 2 \cdot \text{A}_7$$

$$\downarrow$$

$$\text{A}_7 \subset \text{S}_7$$

De $L \mapsto E_L \in \mathbb{F}_q$ et de $\text{rg } 7$.

$q_{E_L} \cong \langle 1 \rangle \oplus q'$ q' forme trace en $\text{rg } 6$.

$$G \subset 2 \cdot \text{A}_7 \Rightarrow \begin{cases} \alpha_1 \\ \alpha_2 \end{cases} \text{ st nuls } \left\{ \begin{array}{l} \text{pour } q \\ \text{--- } q' \end{array} \right.$$

D'où $a(q') = (-1)(-1)(c) \in H^3(h)$.

De si K vérifiait O_6 , E inv. serait nul $\forall h$, de caro, et $\forall G$ torsion sur h .

Or on va construire un contre expe :

Soit h un corps ne vérifiant pas O_6 .

On sait qu'il existe E de rang 6

t.q. $q_E = \langle 1, 1 \rangle \oplus \langle c, c, c, c \rangle$, c non \square
i.e. $a(q_E) \neq 0$.

Une telle alg. correspond à $\varphi: \Gamma_h \rightarrow A_6$.

Quitte à changer E , on peut supposer que l'image de φ est contenue dans le 2-Sylow de A_6 .

[On peut aussi le faire en faisant une extension de degré impair].

Ceci définit donc un $\tilde{\varphi}: \Gamma_h \rightarrow 2.A_6 \subset 2.A_7$.

L'image de $\tilde{\varphi}$ est contenue dans un 2-Sylow de $2.A_7$, donc dans G .

Donc $u \in G$ torsion, avec $a \neq 0$.

contradiction,