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_>

COLLÈGE DE FRANCE

J-P. SERRE chaire d'Algèbre et Géométrie

Cours 1993-1994

Quelques exemples d'invariants cohomologiques

Notes de Anne Quéguiner

10

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 $\varphi : \Gamma_k \to G$, 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 $\varphi : \Gamma_{K_G} \to G$ 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 $\mathbf{Q}(T_1, \ldots, T_N)$, 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 $q > q(\mathrm{G})$.)

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

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* $q \leqslant 1$, *ou si* $q = 2$ *et* G *opère trivialement sur* M, *aucun élément non nul de* $\mathrm{H}^q(\mathrm{G},\mathrm{M})$ *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* $\mathrm{H}^2(\mathrm{G},\mathrm{M})$ *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 $\hat{\mathrm{G}}$ le pro-p-groupe défini par deux générateurs u,v liés par la relation $uvu^{-1} = v^{1+p}$, et soit $\varphi : \hat{\mathrm{G}} \to \mathrm{G}$ l'unique homomorphisme continu tel que $\varphi(u) = 1$ et $\varphi(v) = s$. On démontre :

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

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

(b) *Si* $q > 2$, *tout élément de* $\mathrm{H}^q(\mathrm{G},\mathrm{M})$ *est négligeable.*

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

(c) *Pour que* $x \in \mathrm{H}^2(\mathrm{G},\mathrm{M})$ *soit négligeable, il faut et il suffit que l'on puisse représenter* x *par un élément de* $\mathrm{Ker}_\mathrm{M}(1 - s)$ *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 $\mathrm{M} = \mathbf{Z}/2\mathbf{Z}$, on peut déterminer pour tout q la partie négligeable de $H^q(G,\mathbf{Z}/2\mathbf{Z})$ lorsque G est l'un des groupes suivants :

$C_2 \times \ldots \times C_2$, 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 $H^q(G,\mathbf{Z}/2\mathbf{Z})$, $q > 2$, 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 $H^q(G,\mathbf{Z}/2\mathbf{Z})$, $q > 2$, 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* $H^q(S_n,\mathbf{Z}/N\mathbf{Z})$, $q > 0$, N *impair, est négligeable.*

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

(b) *Pour qu'un élément de* $H^q(S_n,\mathbf{Z}/2\mathbf{Z})$ *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_o ;

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

A toute extension k de k_o 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 $H^i(.,C)$, 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_o. 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 $H^i(k,C) \to H^i(k',C)$.

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 ($n \geqslant 1$), vu comme groupe algébrique de dimension 0. Dans ce cas, un G-torseur X sur k s'interprête comme :

— un homomorphisme continu $\varphi : \Gamma_k \to S_n$, à conjugaison près ;

— une k-algèbre étale E de rang n, à isomorphisme près.

Un invariant cohomologique de type $H^i(.,C)$ 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_o, 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 $k \times \ldots \times k$).

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

Le cas le plus intéressant est celui où $C = \mathbf{Z}/2\mathbf{Z}$ (k_o 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 $H^i(.,\mathbf{Z}/2\mathbf{Z})$ 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* $H^i(.,C)$ *s'écrit de façon unique sous la forme :*

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

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

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

De plus :

(v) *On a* $w_i^{gal}(E) = 0$ *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 $k \mapsto \mathrm{H}^i(k,\mathrm{C})$ par le foncteur $k \mapsto \mathrm{GrW}(k)$, où $\mathrm{GrW}(k)$ est *l'anneau de Grothendieck-Witt* des classes de formes quadratiques sur k. (On pourrait utiliser aussi l'anneau de Witt usuel $\mathrm{W}(k)$, mais c'est moins commode, car les puissances extérieures λ^i sont définies sur $\mathrm{GrW}(k)$ mais pas sur $\mathrm{W}(k)$.) On obtient ainsi la notion d'*invariant de type* GrW des algèbres étales de rang n. Exemple : l'application

$$\mathrm{E} \mapsto \lambda^i(q_{\mathrm{E}}),$$

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* $\mathrm{GrW}(k_o)$, *des* $\lambda^i(q_{\mathrm{E}})$, $0 \leqslant i \leqslant m = [n/2]$.

Ceci permet de prouver des identités portant sur les $\lambda^i(q_{\mathrm{E}})$ 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 :

$$\omega_n = \left|\begin{array}{l} m\langle 2\rangle = \langle 2, \ldots, 2\rangle \text{ si } n = 2m \\ 1 + m\langle 2\rangle = \langle 1,2, \ldots, 2\rangle \text{ si } n = 2m + 1. \end{array}\right.$$

On obtient ainsi :

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

$$\lambda^n(q_{\mathrm{E}}) \cdot \lambda^i(q_{\mathrm{E}} - \omega_n) = \langle 2^m\rangle \cdot \lambda^{m-i}(q_{\mathrm{E}} - \omega_n) \textit{ pour tout } i.$$

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

(iii') $\lambda^i(q_{\mathrm{E}} - \omega_n) = \langle 2^m d_{\mathrm{E}}\rangle \cdot \lambda^{m-i}(q_{\mathrm{E}} - \omega_n)$ *pour tout* i.

En particulier :

(iv) *On a* $\lambda^i(q_{\mathrm{E}} - \omega_n) = 0$ *pour tout* $i > m$.

3. La forme trace en rang $\leqslant 7$

Soit k un corps de caractéristique $\neq 2$. Soit n un entier $\geqslant 1$. 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 $<1> \oplus q'$, où q' est une forme trace de rang $n-1$.*

3.2. *Caractérisation des formes trace de rang $\leqslant 7$*

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 $<2>$* ;

(pour $n = 4$) *q contient $<1>$ et $w_3(q) = 0$* ;

(pour $n = 6$) *q contient $<1,2>$, et contient $<1,1,2>$ 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 $\mathrm{Out}(S_n) = \mathrm{Aut}(S_n)/\mathrm{Int}(S_n)$ soit non trivial. Si E est une algèbre étale de rang 6, correspondant à $\varphi : \Gamma_k \to S_6$, 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 :

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

Cette formule se simplifie si l'on écrit :

$$q_E = <1,2> \oplus Q \text{ et } q_{E'} = <1,2> \oplus Q',$$

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

$$Q' = \lambda^3(Q) = <2d> \cdot Q, \text{ avec } d = \mathrm{discr}(E) = \mathrm{discr}(E').$$

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) $q \simeq <1,1,c,c,c,c>$.

(i_2) *c est somme de 4 carrés dans* $k(\sqrt{2})$.

(i_3) $(2)(c) = 0$ *dans* $\mathrm{H}^2(k,\mathbf{Z}/2\mathbf{Z})$, *i.e. c est représenté par la forme* $<1,-2>$.

D'après 3.1., il y a un énoncé analogue en rang 7 : dans (i_1) on remplace $<1,1,c,c,c,c>$ par $<1,1,1,c,c,c,c>$.

Disons qu'un corps *k a la propriété* (0) si tout $c \in k^*$ satisfaisant à (i_2) et (i_3) est somme de 4 carrés dans k (ce qui équivaut à $<c,c,c,c>$ isomorphe à $<1,1,1,1>$). 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 $<1,\ldots,1>$. 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* **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 (i_2) et (i_3), mais n'est pas somme de 4 carrés.)

L'exemple donné dans (iv) est de degré de transcendance 4 sur **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* $2.\mathrm{A}_7$

Soit $2.\mathrm{A}_7$ 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 $w_1(q_\mathrm{E}) = w_2(q_\mathrm{E}) = 0$ si et seulement si E est définie par un homomorphisme $\Gamma_k \to \mathrm{S}_7$ qui se factorise en $\Gamma_k \to 2.\mathrm{A}_7 \to \mathrm{A}_7 \to \mathrm{S}_7$. En utilisant les résultats du n° 3.4, on démontre :

(i) *Soit* G *un sous-groupe d'indice impair de* $2.\mathrm{A}_7$ (par exemple $2.\mathrm{A}_7$, $2.\mathrm{A}_6$, $\mathbf{SL}_2(\mathbf{F}_7)$ ou le groupe quaternionien Q_{16}). *Soit* $\mathrm{L_G/K_G}$ *une* G-*extension galoisienne verselle en caractéristique* 0. *Alors* $\mathrm{K_G}$ *n'est pas une extension transcendante pure de* **Q**.

(En effet, soit $k = \mathrm{K_G}$, et soit E la k-algèbre étale de rang 7 associée à

$$\Gamma_k \to \mathrm{Gal}(\mathrm{L_G}/k) = \mathrm{G} \to 2.\mathrm{A}_7 \to \mathrm{A}_7 \to \mathrm{S}_7.$$

Si la forme trace de E était la forme unité $<1, \ldots 1>$, il en serait de même (vu le caractère versel de $\mathrm{L_G}/k$) 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 $\mathbf{Q}$.)

En particulier :

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

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,* Sém. 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* : $X_o(11)$ *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,* Sém. Bourbaki, mars 1994 ;

— *Sous-groupes finis de* $\mathbf{GL}_n(\mathbf{Q})$,..., $E_8(\mathbf{Q})$, Sém. 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* $\mathbf{SO}_3$ *à* $\mathbf{PGL}_2(\mathbf{F}_{31})$ *dans* E_8, Sém. Chevalley, juin 1994 ;

— *λ-opérations et formes quadratiques,* Luminy, juin 1994 ;

— *Galois representations and Chebotarev's density theorem,* Amsterdam, juin 1994.

COLLÈGE DE FRANCE

J-P. SERRE chaire d'Algèbre et Géométrie

Cours 1993-1994

Quelques exemples d'invariants cohomologiques

Notes de Anne Quéguiner

Table des Matières

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 = spec k, k corps), un G-torseur est un espace principal homogène / à G, i.e. un schéma $P_{\to S}$ avec une action de G tq après changement de base fidèle plat $S'_{\to S}$ P devient isomorphe au torseur trivial, i.e. $\simeq G$.

Cas particulier : S = spec(k); G lisse sur k.
On peut prendre S' = spec(k'), et on peut imposer k' de degré fini et séparable /k.
Alors P devient trivial sur $k' \iff P(k') \neq \emptyset$.

(Analogue en topologie : un fibré ppal ayant une section devient trivial.).

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

<u>Exple</u>: formes quadratiques ; $O(q)$.

k est un corps ; car $k \neq 2$.

q et q' sont deux f.q. non dég. de dim. n sur k

P = espace des isomorphismes entre q et q'

$X_1, \ldots, X_n$ variables.

pts de P : matrices $n \times n$ transformant q en q'

le groupe orthogonal de q $O(q)$ agit sur P et en fait un espace principal homogène.

<u>A q fixé</u> : on a ainsi

classes de f.q. q' de même rg que q (i.e. non dég. de dim. n) $\overset{\sim}{\longleftrightarrow}$ classes de $O(q)$ torseurs.

il est bien connu que c'est bijectif.

<u>Autre exple</u> : G gpe fini.

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

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

Il y a bijection entre :

① les G-torseurs sur k

② les hom. continus $\Gamma_k \to G$, à conj. près.

③ les G-alg. gal. sur k.

en prenant l'algèbre affine.

(N.B. : continu = à noyau ouvert.).

<u>Cas particulier :</u>

qd $G = S_n$, gpe sym. en n lettres,

1 2 et 3 st en bijections avec

4 les k alg. étales de rang n sur k.

(les alg. st commutatives, à élt unité).

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

les classes de G-torseurs (G lisse /k) $\Longleftrightarrow$ $H^1(\Gamma_k, G(k_s))$
$$\parallel$$
$H^1(k, G)$.

(Si G est non lisse, il faut prendre H^1_{plat})

<u>Ici</u> : on aura tjrs G lisse /k.

<u>Rappel</u> : Si Γ est un Γ_k module, avec les hyp. habituelles (stabilisateur de tout point ouvert), on notera

$H^q(k, \Gamma) := H^q(\Gamma_k, \Gamma)$.

c'est dans ces gpes qu'on va généralement trouver des invariants.

<u>Inv. cohom.</u>

Ce st dc des applications

$\underset{G\text{-torseurs}}{H^1(k, G)} \longrightarrow H^q(k, \Gamma)$

En g^{al}, R est assez petit.
p.ex., $R = \mathbb{Z}/n\mathbb{Z}$, ou $\mu_n^{\otimes i}$.

<u>Exple</u>: cas des f.q.; car $k \neq 2$.
$G = O(q)$; q de rg n.

On a : $\left.\begin{array}{l}\text{cl. de f.q.}\\ \text{de rg } n\end{array}\right) \xrightarrow[w_q]{} H^q(k, \mathbb{Z}/2\mathbb{Z})$

<u>autre exple</u>: car $k \neq 2$.
$G = G_2$ (déployé).

$H^1(k, G_2) \longrightarrow H^3(k, \mathbb{Z}/2\mathbb{Z})$
$\Updownarrow$
classes d'octonions/k

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

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

où on note (α) l'élé^t de $H^1(k, \mathbb{Z}/2\mathbb{Z})$
correspondant à $\alpha \in k^*/k^{*2}$.

<u>Ici</u>: L'invariant caractérise la classe d'octonions; l'image est constituée des élé^{ts} décomposables.
(Mais ds la pratique, il est difficile de déterminer les élé^{ts} décomposables).

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

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

<u>Cas des f.q.</u> : conj. de Milnor.

q et q' m̂ rang ; on suppose qu'elles ont m̂ w_1 et w_2.

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

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

(conj. de Milnor : $\mathrm{gr}\, W \simeq H^\bullet(k, \mathbb{Z}/2\mathbb{Z})$.)

$$H^1(k, F_4) \to H^3(k, \mathbb{Z}/2\mathbb{Z})$$
$$H^1(k, F_4) \to H^5(k, \mathbb{Z}/2\mathbb{Z})$$
$$H^1(k, F_4) \xrightarrow{\text{Rost}} H^3(k, \mathbb{Z}/3\mathbb{Z}).$$

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

<u>Cas intéressant</u> : Si G est un gpe semi-simple, simplemt connexe.

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

p.ex. $H^1(k, E_8) \longrightarrow H^3(k, \mu_5^{\otimes 2})$.

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

Analogie avec la topologie:

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

$$\begin{tikzcd} & E_G \arrow[d, "G"] \\ S \arrow[r, "f_P"] & B_G \end{tikzcd}$$

unique à l'homotopie près.

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

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

Les classes de Chern attachées à un fibré ppal.

Ceci permet de construire des invariants sur une base qcq.

Mais:

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 qcq.

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

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

Alors si on choisit un G-module Π, un entier $q \geq 0$, et un élt $a \in H^q(G, \Pi)$,
$\forall \varphi : \Gamma_k \to G$ $\varphi^*(a) \in H^q(k, \Pi)$.

On obtient ainsi une flèche
$H^1(k, G) \longrightarrow H^q(k, \Pi)$.

Rque: Les aut. int. de G opèrent trivialement sur $H^q(G, \Pi)$. ($\to$ permet de mq φ et φ' conjugués $\Rightarrow \varphi^*(a) = \varphi'^*(a)$).

précisément:

$g \in G$

$$\left.\begin{array}{l} G \to G \\ x \mapsto g.x.g^{-1} \\ \Pi \to \Pi \\ m \mapsto g.m \end{array}\right\} \text{permettent de définir} \quad H^q(G,\Pi) \longrightarrow H^q(G,\Pi)$$

cette flèche est id.

Déf.: $\boxed{\text{a est nég. (pour la cohom. galoisienne) si } \varphi^*(a) = 0 \text{ pour tout corps } k \text{ et } \forall \varphi : \Gamma_k \to G.}$

Etude plus systématique des classes de cohom. négligeables.

(p.ex., G cyclique d'ordre 9 $\to$???).

Désormais, G est un gpe fini donné. Π est un G-module (le + svt, Π fini). $q \geq 1$; $a \in H^q(G, \Pi)$.
k corps ; $\Gamma_k = \mathrm{Gal}(k_s/k)$.

Déf. : $\boxed{\text{a est } k\text{-négligeable si } \varphi^*(a) = 0 \text{ pour } \forall\, \varphi : \Gamma_k \to G \text{ continu.}}$

X est une catégorie de corps.

Déf. : $\boxed{\text{a est } X\text{-négligeable si a est } k\text{-nég. pour tout } k \in X.}$

Déf. : $\boxed{\text{a est négligeable s'il est } X \text{ nég. pour } X = \text{tous les corps.}}$

Ceci permettra de regarder p.ex. le cas des corps de car $\neq 0$, ou des corps $\supset \sqrt{-1}$ etc.

N.B. : Bogomolov | X cat. des corp. $\supset$ un.
Saltman | corps alg. clos.

cf. aussi Lure (1991).

Prop. : $\boxed{\text{Si a est neg. à coeff, alors a est neg.}}$

<u>Dém.</u> : Soit k, car $k = p$.
On choisit un corps local K, de corps résiduel k, avec car $K = 0$.
Théorie des ramifications (corps locaux) :

$$\Gamma_K \xrightarrow{\pi} \Gamma_k \longrightarrow 1.$$

On sait aussi (cf. cours précédents) que cette flèche est scindée, i.e. il y a un morphisme $\varepsilon : \Gamma_k \longrightarrow \Gamma_K$ tq $\pi \circ \varepsilon = id$.

<u>Donc</u> $H^q(\Gamma_k, C) \hookrightarrow H^q(\Gamma_K, C)$ $\forall (q, C)$.

Soit alors $a \in H^q(G, C)$; $\varphi : \Gamma_k \longrightarrow G$.
<u>mq</u> $\underset{\substack{\| \\ 0}}{\varphi^*(a)} \in H^q(\Gamma_k, C)$.

<u>Mais</u> $\underset{\substack{\| \\ 0}}{\pi^* \circ \varphi^*(a)} \in H^q(\Gamma_K, C)$

(car a nég. en car 0, et $\varphi \circ \pi : \Gamma_K \to G$).
L'injectivité de $H^q(\Gamma_k, C) \xhookrightarrow{\pi^*} H^q(\Gamma_K, C)$ permet alors de conclure. □.

<u>N.B.</u> : La " réciproque " est fausse :
exple de classe b " minimale " $\begin{cases} \text{non nég. en car } 0 \\ \text{nég. en tte car } p > 0 \end{cases}$

On prend $G = \mathbb{Z}/2\mathbb{Z}$.
Pour ce gpe, seule $a = 0$ est nég., car $G = Gal(\mathbb{C}/\mathbb{R}) = \Gamma_{\mathbb{R}}$.

$a \neq 0$
in
$H^2(G, \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$.
$\varphi^*(a) \in H^2(k, \mathbb{Z}/2\mathbb{Z}) = Br_2(k)$.

Mais $\varphi : \Gamma_k \to G = \mathbb{Z}/2\mathbb{Z}$
$\Updownarrow$
$\alpha \in k^\circ/k^{\circ 2}$ $\quad (\alpha) \in H^1(k, \mathbb{Z}/2\mathbb{Z})$.

Alors $\varphi^*(a) = (-1)(\alpha)$.
($\Rightarrow a$ neg. en car p qd $p \equiv 1$ mod. 4).

De m̂ b est non nul dans $H^3(G, \mathbb{Z}/2\mathbb{Z})$
$$\varphi^*(b) = (-1)(\alpha)(\alpha) = \underbrace{(-1)(-1)}_{\substack{\text{quaternions usuels} \\ \text{décomposés en car } p.}}(\alpha) = 0.$$

<u>N.B.</u> : On pourra donc dorénavant supposer car $k = 0$.

<u>Propriétés formelles</u>

<u>Notat°</u> : $H^q_n(G, \Gamma) =$ sgpe de $H^q(G, \Gamma)$ formé des élts négligeables.

$$H^q_e(G, \Gamma) = H^q(G, \Gamma) / H^q_n(G, \Gamma).$$

1) $\Gamma \to \Gamma'$ G-modules
$H^q_n(G, \Gamma) \longrightarrow H^q_n(G, \Gamma')$.

2) $0 \to \Gamma \to \Gamma' \to \Gamma'' \to 0$
$\delta : H^q(G, \Gamma'') \longrightarrow H^{q+1}(G, \Gamma)$
envoie $H^q_n(G, \Gamma'')$ ds $H^{q+1}_n(G, \Gamma)$.

ou encore, on a

$$H^q_e(G,\Pi) \to H^q_e(G,\Pi') \to H^q_e(G,\Pi'') \xrightarrow{\delta} H^{q+1}_e(G,\Pi$$

Cette suite est un complexe, mais n'est pas exacte en gal.

Prop. : $\boxed{\text{Si } q=0 \text{ ou } 1,\ H^q_n(G,\Pi)=0.}$

En effet, on sait que tt G est gpe de Galois d'une extension L/k.
[p.ex. car $G \hookrightarrow S_n$
ou par les corps de nbres].
$\varphi : \Gamma_k \to G$, φ surjectif.

Alors $H^q(G,\Pi) \to H^q(\Gamma_k,\Pi)$

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

Prop. : $\boxed{q=2 \text{ Si } \Pi \text{ est fini, et l'act}^\circ \text{ de } G \text{ triviale, alors } H^2_n(G,\Pi)=0.}$

(la dém. sera donnée ultérieurement).

Par contre : $\exists$ des Π à act° non triviale, avec $H^2_n(G,\Pi)\neq 0$.
expl : $G = C_3$ cyclique d'ordre 3.
Π e.v. de dim 2 sur $\mathbb{F}_3$.
Act° d'un gén. de G donnée par $\begin{pmatrix}1&1\\0&1\end{pmatrix}$.
On vérifie que $H^2(G,\Pi) = \mathbb{Z}/3\mathbb{Z}$ est entièrement négligeable.
(cf. article de Lur).

Prop : $\boxed{\begin{array}{l}\text{Soit } G' \subset G \text{ et } \Gamma \text{ un } G \text{ module.} \\ \text{Res} : H^q(G,\Gamma) \to H^q(G',\Gamma) \\ \text{applique } H^q_n \text{ dans } H^q_n.\end{array}}$

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

$$\Gamma_h \longrightarrow \underset{a'}{G'} \longrightarrow \underset{a}{G}$$

Prop. : $\boxed{\begin{array}{l}\text{Cor} : \underset{\substack{\Psi \\ a'}}{H^q(G',\Gamma)} \to \underset{a = \operatorname{Cor}(a')}{H^q(G,\Gamma)} \\ \text{Alors } a' \text{ nég.} \Rightarrow a \text{ nég.}\end{array}}$

Dém : c'est un peu moins évident.

deux tps :

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

On a

$$\begin{array}{ccc} & L & \\ h' \diagup & \mid G & \\ G' & h & \end{array} \quad \text{et} \quad \begin{array}{ccc}\Gamma_{h'} & \longrightarrow & G' \\ \cap & & \cap \\ \Gamma_h & \longrightarrow & G\end{array} \quad \hat{=} \text{ indice.}$$

Dc

$$\begin{tikzcd} H^q(G')\ a' \arrow[r, "\mapsto 0"] \arrow[d, "\operatorname{Cor}"'] \arrow[dr, phantom, "\text{com}"] & H^q(\Gamma_{h'}) \arrow[d, "\operatorname{Cor}"] \\ H^q(G)_a \arrow[r] & H^q(\Gamma_h) \end{tikzcd}$$

ce diagramme permet de conclure.

② Cas gal : Dx méthodes possibles.

1ère méthode : on utilise le lemme suivant

Lemme : $\boxed{\begin{array}{l}\text{Si } a \text{ est tq } \varphi^*(a) = 0 \text{ pour tout} \\ \varphi \text{ surjectif, alors } a \text{ est nég.}\end{array}}$

<u>2^{nde} méthode</u> : On reprend la dém. précédente. $\Gamma_h \xrightarrow{\varphi} G$
$$G \supset G'$$

Γ_h opère sur G/G' grâce à φ.
("cuisine à la Mackey").
On prend u syst. de rep. g_α des orbites de Γ_h dans G/G'.
$\Gamma_{h\alpha}$ le fixateur dans Γ_h de g_α
on a
$$\Gamma_{h\alpha} \xrightarrow{\varphi_\alpha} G'$$
$$x \longmapsto g_\alpha^{-1} x g_\alpha \in G'.$$

$$\boxed{\varphi^* \mathrm{Cor}_{G'}^{G} a' = \sum_\alpha \mathrm{Cor}_{\Gamma_{h\alpha}}^{\Gamma_h} \varphi_\alpha^* a'}$$

Mais a' nég. $\Rightarrow$ les $\varphi_\alpha^* a'$ st nuls.

On va maintenant donner qques exples de classes de cohom. nég.
Pour certains gpes, il y en a bcp.
On démontrera

<u>Thm</u> : $\boxed{\text{Si } G = S_n, \text{ et } \Gamma \text{ u gpe ab. fini, d'ordre impair, sur lequel } G \text{ opère trivialement, alors tt él}^t \text{ de } H^q(G,\Gamma), q>0 \text{ est nég.}}$

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

On montrera aussi

<u>Thm</u> : $\boxed{\text{Si } |G| \geq 2,\ \exists \text{ des } q, \Gamma \text{ et } a \in H^q(G,\Gamma)\ a \neq 0 \text{ tq } a \text{ nég.}}$

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

Soit donc G un gpe fini qcq, et x et $y \in H^1(G, \mathbb{Z}/2\mathbb{Z})$ $(\Gamma = \mathbb{Z}/2\mathbb{Z})$.
On prend $q = 3$ et $a = x^2y + xy^2 \in H^3(G, \mathbb{Z}/2\mathbb{Z})$.

<u>Alors</u> <u>a est négligeable</u>

<u>Preuve</u> : k ; car $k \neq 2$.
$H^1(k, \mathbb{Z}/2\mathbb{Z}) \simeq k^*/k^{*2}$
$(\alpha) \longleftarrow \alpha$

$\varphi : \Gamma_k \to G$.
$\varphi^* x$ et $\varphi^* y$ s'écrivent (α) et (β).
Alors
$\varphi^*(a) = (\alpha)(\alpha)(\beta) + (\alpha)(\beta)(\beta) = (-1)(\alpha)(\beta) + (-1)(\alpha)(\beta)$
$= 0$ (on travaille modulo 2).

<u>Exercice</u> : Si $x \in H^1(G)$ et $y \in H^2(G)$
mq $(y + x^2)(xy) \in H^4(G)$ est nég.
(Utiliser le thm de Merkurjev sur H^2 : H^2 est eng. par les élts déc.,
i.e. tt élt de H^2 s'écrit $\sum (\alpha_i)(\beta_i)$).

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

G gpe qcq. $\Gamma = \mathbb{Z}/p\mathbb{Z}$.

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

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

u $\delta : H^1(G,\Gamma) \to H^2(G,\Gamma)$ (Bernstein).

Alors $x\,\delta(x)$ est nég.

Preuve :

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

Dc ops ds la dém. que G est cycliq d'ordre p.

Soit k ; car $k \neq p$.

On peut aussi supposer $k \ni \zeta$

ζ racine primitive $p^{\text{ième}}$ de 1.

$\left(\dfrac{k(\mu_p)}{k} \right)$ d° est u div. de $p-1$, dc 1^{er} à p.

D'où cor. ⟶ cor. ...

Théorie de Kummer :

$\varphi : \Gamma_k \to G$; $\varphi^* x \in H^1(k, \mathbb{Z}/p\mathbb{Z})$

$$\begin{aligned} &\| \\ &H^1(k, \mu_p) \simeq k^*/k^{*p} \\ &(\alpha) \leftarrow \varphi_\alpha \end{aligned}$$

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

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

Dc $\varphi^*(x\,\delta x) = \underbrace{(\alpha)(\alpha)}_{=0}(\zeta) = 0$

⟶ Donne u exple de classe nég. ds le H^2 d'u gpe cycliq.

$\boxed{\text{En fait, on montrera que si } \Gamma \text{ est u } C_p\text{-mod fini qcq, tt élt de } H^q(G,\Gamma) \text{ est nég. } q \geq 3}$

J.-P. Serre
Cours au collège de France.
Le 11.10.93

II
1

On va commencer par exposer deux conséquences des propriétés formelles:

1) Soit G fini - M un G-module.
On suppose que $a \in H^q(G,M)$ est d'ordre une puissance de p, i.e. $a \in H^q(G,M)_{(p)}$ (composante p primaire).
Alors si S est un pSylow de G, on a:
$\boxed{a \text{ est neg.} \Leftrightarrow \operatorname{Res}^G_S(a) \text{ est nég.}}$

(preuve: un sens a déjà été vu.
Dans l'autre, on applique la corestriction, et on utilise Cor∘Res = indice

Donc: Dans $H^1(G, \mathbb{Z}/2\mathbb{Z})$ on pourra regarder simplement la restriction à un 2-Sylow,
i.e. $H^1(G,\mathbb{Z}/2\mathbb{Z}) \to H^1(S,\mathbb{Z}/2\mathbb{Z})$.
Si de plus S est abélien, notons N le normalisateur de S ds G et $\mathcal{N} = N/S$.
il suffit de regarder
$$H^1(G,\mathbb{Z}/2\mathbb{Z}) \to H^1(S,\mathbb{Z}/2\mathbb{Z})^{\mathcal{N}}.$$

2) Thm de Shapiro:

Soit G fini, H un ss gpe de G, et M un H module. $\operatorname{Ind}_H^G M = M^*$ G mod. induit.
(un élt de M^* peut-être vu comme $f : G \to M$ tq $f(hx) = h.f(x)$ $\forall h \in H$ et $g.f(x) := f(xg)$ $\forall g \in G$).
On a alors

Lemme de Shapiro (Faddev)
$$\boxed{H^q(G,M^*) \simeq H^q(H,M)}$$
$$a^* \longleftrightarrow a.$$

$\boxed{\text{Alors les classes nég. sont les } \hat{m}.}$

<u>i.e.</u> a nég. $\Longleftrightarrow$ a^* nég.

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

<u>1)</u>

$$\begin{tikzcd} H^q(G,\Pi^*) \arrow[rr, "\sim"] \arrow[dr, "\mathrm{Res}"'] & & H^q(H,\Pi) \\ & H^q(H,\Pi^*) \arrow[ur] & \end{tikzcd}$$

(on a un H morphisme $\begin{array}{l}\Pi^* \longrightarrow \Pi \\ f \longmapsto f(1)\end{array}$)

Grâce aux prop. formelles vues la semaine dernière, on a alors
a^* neg. $\Rightarrow$ a neg.

<u>2)</u> De $\hat{m}$

$$\begin{tikzcd} H^q(H,\Pi) \arrow[rr, "\sim"] \arrow[dr] & & H^q(G,\Pi^*) \\ & H^q(H,\Pi^*) \arrow[ur, "\mathrm{Cor}"'] & \end{tikzcd}$$

(On a un G morphisme
$\Pi \longrightarrow \Pi^*$
$m \longmapsto f_m \begin{cases} G \longrightarrow \Pi \\ f_m(1) = m \text{ et } f_m(x) = 0 \text{ si } x \notin H \end{cases}$

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

<u>cqfd</u>

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

Soit $a \in H^2(G,\Pi)$, avec Π fini.

Concrètement, qu signifie a négligeable ?

a déf. une extension

$1 \to \Pi \to E_a \to G \to 1$.

a nég. $\Leftrightarrow \forall h ; \forall \varphi : \Gamma_h \to G$ continu, φ se relève en $\Gamma_h \to E_a$

$$\begin{tikzcd} & E_a \arrow[d] \\ \Gamma_h \arrow[r] \arrow[ur, dotted] & G \end{tikzcd}$$

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

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

Thm (Luc'e) : Si $|G| > 2$, alors il existe un G module fini Π, et un élt $a \in H^2(G,\Pi)$, $a \neq 0$ qui est nég.

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

Construction :

le groupe G contient un sous groupe H qui est

- cyclique d'ordre 4 — C_4
- ou ab. élém. de type (2,2) — $C_2 \times C_2$
- ou cyclique d'ordre p premier $p \neq 2$ — C_p

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

$$1 \to \underset{\text{ab}}{\Omega} \to G' \to G \to 1.$$

L'ordre de G' sera
$\begin{cases} 32 \text{ ds les dx } 1^{\text{er}} \text{ cas} \\ p^3 \text{ ds le } 3^{\text{ème}}. \end{cases}$

Le module Ω :

C_4 : $0 \to \mathbb{F}_2 \to \mathbb{F}_2[G] \to \Omega \to 0$
Ω est ab. elem. de type $(2,2,2)$
Act° d'un gén. $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$

$C_2 \times C_2$: m̂ construction.

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

C_p : $\Omega = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
Si σ est un gén., on le fait agir par une matrice de Jordan $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
$H^2(G,\Omega) \simeq \mathbb{Z}/p\mathbb{Z}$.

Plutôt que de construire directement des classes de cohom. négligeables, on se place du pt de vue relèvement, en considérant l'extension associée.

① $G = C_2 \times C_2$

On se donne $\Gamma_k \to G$, 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 rg 4 sur k.

un gén. agit par $\begin{cases} X \to -X \\ Y \to Y \end{cases}$ et l'autre $\begin{cases} X \to X \\ Y \to -Y. \end{cases}$

On cherche à écrire

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

$rg(L'/L) = 4$; $rg(L'/L) = 32$

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

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

On défini aussi un σ_2.

On a ainsi un G' $1 \to \Pi \to G' \to G \to 1$.

Π est de type $(2,2,2)$.

Il faut vérifier :

- que G' ne dépd pas de L
- Π cô G module est bien celui qu'on veut
- l'extension $G' \to G$ est non triviale.

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

tq $H^2(G,\Pi) \xrightarrow[\sim]{\delta} H^3(G,\mathbb{Z}/2\mathbb{Z})$

$\qquad u \longmapsto u_3$

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

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

H^3 a cô base A^3, A^2B, AB^2, B^3.

Alors u_3 est déf. par $u_3 = AB(A+B) = A^2B + AB^2$

↑ on a déjà vu que cet élt est bien négligeable.

(2) $G = C_p$, p premier $p \neq 2$.

k corps ; car $k \neq p$.
On suppose k^* $\ni \zeta$ racine primitive $p^{ième}$ de l'unité.

On va exhiber un gpe
$$\begin{array}{cc} G' & p^3 \\ \downarrow & \\ G & p \end{array}$$
on veut mq il a la propriété de relèvement.

Mais :
(1) si car $k = p$, dim col. $cd_p(k) \leq 1$.
De tte flèche se relève.
(2) Si $\zeta \notin k$ $\quad \begin{array}{c} k' = k(\zeta) \\ | \\ k \end{array}$ $\Big\}$ $d^\circ | p-1$, i.e. d° premier à p.

Alors si la prop. de relèvement est vraie pour k', on a $\Gamma_{k'} \subset \Gamma_k$
indice premier à p

$u \in H^2(G, \mathbb{Z})$.
· On sait que $\varphi^*(u)|_{\Gamma_{k'}} = 0$.
Comme indice $\wedge p = 1$, on a bien $\varphi^*(u) = 0$.

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

Soit $\varphi : \Gamma_k \to C_p$.
$\qquad\qquad\quad \updownarrow$
$\qquad\qquad\quad \zeta$

C_p alg. gal. L.
$L = k(\sqrt[p]{\alpha})$ $\alpha \in k^*$, i.e. $L = k[X]/(X^p - \alpha)$.
$\sigma : X \to \zeta X$.

On pose $L' = k(\sqrt[p]{\zeta}, \sqrt[p^2]{\alpha})$,
i.e. $L' = L[Y, Z]/(Y^p - \zeta)(Z^p - X)$.

L' est de rg p^3.

Soit G' le ssgpe de $\mathrm{Aut}(L')$ engendré par $\sigma : \begin{cases} X \longmapsto \zeta X \\ Z \longmapsto YZ \\ Y \longmapsto Y \end{cases}$ et $\tau : \begin{cases} X \longmapsto X \\ Z \longmapsto Z \\ Y \longmapsto \zeta Y. \end{cases}$

On voit facilement $\sigma^{p^2}=1$, $\tau^p=1$ et $\tau\sigma\tau^{-1}=\sigma^{1+p}$ à vérifier

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

$$\begin{array}{c|cc} G' & \sigma & \tau \\ \downarrow & \downarrow & \downarrow \\ G & \text{gén. de } G & 1 \end{array}$$

G' est bien une extension non triviale de G.

Elt négligeable correspondant : de type (p,p) avec act° $\begin{pmatrix}1&1\\0&1\end{pmatrix}$

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

Ceci donne d'autres elts négligeables.

<u>Résultat</u> :

$$\boxed{\begin{array}{l} \text{Soit } \Omega \text{ un } \mathbb{F}_p[G] \text{ mod., } G = C_p, \\ \text{indécomposable, de dim } i \\ 1 \le i \le p \text{ (} \leftrightarrow \text{ forme de Jordan} \\ \text{de dim } i\text{).} \\ H^2(G,\Omega) = \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{si } 1 \le i \le p-1 \\ 0 & \text{si } i = p. \end{cases} \\ \boxed{\begin{array}{l} \text{Si } i=1 \quad H^2_n(G,\Omega)=0 \\ \text{Si } 2 \le i \le p-1 \quad H^2_n(G,\Omega) = \mathbb{Z}/p\mathbb{Z} \end{array}} \end{array}}$$

Ce que l'on vient de faire démontre que pour $i=2$ $H^2(G,\Omega)$ est nég.
Or si $rg(\Omega) > 2$, $\Omega \supset \Omega_2$ tq $H_2(G,\Omega_2) \simeq H^2(G,\Omega)$

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

---

③ <u>$G = C_4$</u> : ops car $k \neq 2$

Pour construire une ext. gal. de type C_4 :

$$\begin{array}{c} k(\sqrt{a+b\sqrt{\varepsilon}}) \\ | \\ k(\sqrt{\varepsilon}) \\ | \\ k \end{array} \quad \varepsilon \in k^*$$

avec $a^2 - \varepsilon b^2 = \varepsilon c^2$
i.e. $\varepsilon = \boxed{2}$ (somme de dx carrés, car les $\boxed{2}$ forment u gpe).

$x = \sqrt{a+b\sqrt{\varepsilon}}$ $\quad \sigma x = \dfrac{c\sqrt{\varepsilon}}{x} = x'$.
car $\sqrt{(a+b\sqrt{\varepsilon})(a-b\sqrt{\varepsilon})} = c\sqrt{\varepsilon}$.
Si k ∞, on peut imposer $\varepsilon, a, b, c \neq 0$.

Maintenant, on pose :
$L = k(\sqrt{\varepsilon}, \sqrt{a+b\sqrt{\varepsilon}}) = k(x)$
$L' = L(i, \sqrt{x}, \sqrt{x'})$ rg 32.

Les aut. de L' st définis ainsi :

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

Lo u certain gpe $G' \supset$ aut. triviaux :

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

Le 11.10.93 ⑨

$1 \to \Pi \to G' \to G \to 1$
de type $(2,2,2)$. mod. d'augmentat°.

On peut vérifier que l'extension n'est pas triviale. $0 \to \mathbb{F}_2 \to \mathbb{F}_2[G] \to \Pi \to 0$.
$\delta : H^2(G,\Pi) \to H^3(G,\mathbb{F}_2) \simeq \mathbb{Z}/2\mathbb{Z}$
D'où $H^3(G,\mathbb{F}_2)$ est négligeable.

Cyclique d'ordre 4.
$H^q(C_4, \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$

$q = $ 0, 1, 2) seul 0 est nég.
3 nég.
4 seul 0
5 nég. (cup produit...)

... $q \geq 3$ { q impair nég. / q pair non nég. (restrict° à un sgpe d'ordre 2).

On a :
Soit $G' \to G$ prop. de relèvement. Π G-module.
Alors $\mathrm{Ker}(H^q(G,\Pi) \to H^q(G',\Pi))$ est un sousgpe de $H^q_n(G,\Pi)$.

En effet si $\varphi : \Gamma_n \to G$,

$$\begin{tikzcd} & G' \arrow[d] \\ \Gamma_n \arrow[ur, "\varphi'"] \arrow[r, "\varphi"'] & G \end{tikzcd}$$

dc c'est trivial.

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

<u>Thm</u> : $\boxed{\text{Si } \Pi \text{ est un } G \text{ module, et } a \in H^q_n(G,\Pi) \text{ alors il existe } G' \text{ ayant la propriété de relèvement et } a \in \operatorname{Ker}(H^q(G,\Pi) \to H^q(G',\Pi))}$.

(La dém. sera vue un peu plus tard. c'est une conséquence directe de l'∃ des G-torseurs versels.)
(Qd $q > 2$ $G' \to G$ n'aura pas, en g^{al}, un noyau abélien).

On va maintenant parler de <u>G-torseurs versels</u>.

(versel = universel - uni.
p.ex. : G ordre 2 en car 0
$\mathbb{Q}(T^{1/2})$
$\big|$) ext. quad.
$\mathbb{Q}(T)$
Si k est un corps qcq, car $k = 0$, et k' une ext. quad. de k, alors on a $k' = k(\sqrt{t})$, $t \in k^*$. Dc k'/k est obtenu par spécialisation par rapport au cas précédent.
<u>mais</u> il n'y a pas unicité de t
Lo pas universel.)

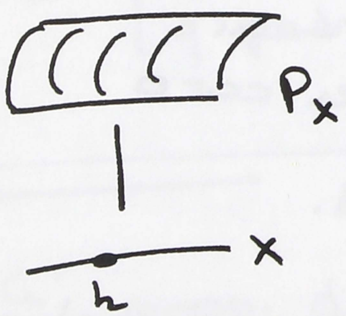
On prend pour G un schéma en groupe lisse sur un corps de base k_0.

Notion de versel 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 P un G torseur sur K.

On dit que P est versel si les propriétés suivantes sont satisfaites:

On peut trouver une k_0 variété lisse, X, irréductible, connexe, et de corps de fcts K. Quitte à la remplacer par un ouvert non vide, on peut supposer que P provient d'un torseur P_X sur X.
Choisissons un tel P_X. (La conditi° qu'on va donner sera indépdte de ce choix).



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

déf.: P est versel si pour toute extension k du corps k_0, infini, et pour tout G torseur Q sur k, et tout ouvert U (de Zariski) non vide de X, il existe $x \in U(k)$ tel que $Q \simeq P_x$.

De façon équivalente,

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

On peut définir cette notion pour des gpes non lisses, mais ici, le cas lisse suffira.

Les versels lisses sont faciles à construire:

{ Si $G = GL_n$, un torseur versel existe.
Si $H \subset G$ et si G a un torseur versel, alors H en a un aussi.

N.B.: il faut supposer G gpe alg. lin.

Construction: On se donne

$G \subset G'$ gpe 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 $\quad G \to G'$ induit P/G' qu'on suppose trivial.

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

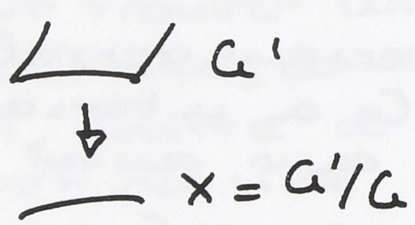
On suppose:

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

• Pour tout corps k ∞, $Y(k)$ est Zariski dense.
(Si k_0 est ∞, cette dernière hyp. revient en fait à $Y(k_0)$ Zariski dense).

Alors $\boxed{Y \text{ est versel pour les } G\text{torseurs qui sont } G' \text{ triviaux.}}$

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



Exple ② G gpe fini.
$G \subset GL_n = \underline{Aut}(V)$ où V esp. de dim n sur k_0.
$Y' = V$. Mais l'act° de G sur V n'est pas libre. Dc on prend Y = l'ouvert de V formé des pts à fixateur trivial.

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

On va maintenant expliquer le thm énoncé p. 10.

1er critère:

Soit k un corps, et Q un Gtorseur$/k$.

On a
$$\begin{array}{ccc} Y/_k & & {}_QY \\ \big\downarrow G & & \big\downarrow \\ X/_k & & X \end{array}$$

Q est isomorphe à la fibre Y_x de Y

$\Updownarrow$

Si on tord $Y/_k$ par le G torseur Q, la variété ${}_QY$ obtenue a un pt rationel au dessus de $x \in X(k)$.

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

$Y \subset Y'$ $\quad {}_QY \subset {}_{Q'}Y'$ où $Q' = Q/_{G'}$ (étendu à G').

$$\begin{array}{c} {}_{Q'}Y' \\ \wr\wr \\ Y' \end{array}$$

dc les pts rationels ont dessus

cqfd.

On vient donc de construire un versel pour les torseurs G' triviaux.

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

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

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

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

(**expl^e** : $G = G_2$ (déployé).

$K = \mathbb{Q}(X, Y, Z)$

G torseurs ↔ alg. d'octonions.

octonion versel : $e_1^2 = X$; $e_2^2 = Y$; $e_3^2 = Z$ ...

Mais : $G = \begin{cases} E_8 \\ F_4 \end{cases}$ ont-ils un torseur versel rationnel ?

(**Autre expl^e** : $G = PGL_2$; $K = \mathbb{Q}(X, Y)$

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 torseurs

↕ G alg. gal.

↕ hom. continus $\varphi : \Gamma_k \to G$, à conj. près.

Partant d'un G torseur versel pour les corps contenant $k_0 = \begin{cases} \mathbb{Q} \\ \mathbb{F}_p \end{cases}$:

c'est un corps K, et un $\Phi : \Gamma_K \to G$.

versel ⇒ Φ est surjectif.

On a dc
$$\begin{array}{ccc} L & & Y \\ \big| G & & \big| G \\ K & & X \end{array}$$
revêt^{ts} gal. X, Y lisses. Act^o libre.

On a dc $1 \to \Gamma_L \to \Gamma_K \to G \to 1$

Soit N un sous gpe normal ouvert de Γ_K contenu ds Γ_L. Posons $G_N := \Gamma_K / N$. $\begin{array}{c} G_N \\ \downarrow \\ G \end{array}$

Lemme : $\boxed{\text{L'extension } \begin{array}{c} G_N \\ \downarrow \\ G \end{array} \text{ a la propriété de relèvement pour la caractéristique étudiée.}}$

Preuve : k corps ∞, de la caract. donnée. $\varphi : \Gamma_k \to G$. On veut mq φ se relève à G_N.

Mais

$$G_N \left(\begin{array}{c} L_N \\ | \\ L \\ |\; G \\ K \end{array} \right) \qquad \begin{array}{c} Y_N \\ | \\ Y \\ | \\ X \end{array}$$

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

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

D'où $\to$ un G_N torseur et dc un $\varphi' : \Gamma_k \to G_N$ relevant φ.

Soit $a \in H^q(G, \Pi)$ ou Π est un G module.

1. a est nég. pour les corps de la car. considérée.

$\Updownarrow$

2. $\Phi^*(a) = 0$ ds $H^q(K, \Pi)$

3. Il existe un $\begin{array}{c} G' \\ \downarrow \\ G \end{array}$ ayant la prop. de relèvement ds la car. étudiée qui tue a.

Le 11.10.93

(17)

Ce thm précise bien la noto de nég.

<u>Dém.</u> : elle est maintenant immédiate

(1) => (2)
$\Uparrow$
(3)

<u>Reste à voir</u> (2) => (3)

Mais a disparait sur K => a disparait déjà sur une ext. gal. finie qu'on suppose contenir L de K. Notons là L_N

On prend $G' = G_N$ le gpe correspondant.

<u>cqfd</u>.

<u>Rque</u> : si on travaille en car 0, on obtient des résultats en toute caract.

(i.e. si en car 0 on a un Kreisel, il nous fournit des G'. Ces G' ont la prop. de relèvement en toute car.)

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

1) <u>Gabber</u> :
L'objet "versel" dont on a parlé ne l'est pas vraiment. Mais les G torseurs qui deviennent triviaux sur G' s'obtiennent bien par image réciproque à partir de cet objet.

2) <u>A propos</u> de la construction d'objets versels :

$$\begin{array}{ccc} G' & & P \\ \downarrow & & \downarrow \\ G'/G & K = \text{corps des fctions de } G'/G & \operatorname{Spec} K \end{array} \Bigg) \text{ est versel.}$$

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

<u>Preuve</u> : Si Q est un G torseur sur k devenant trivial sur G' :

$\left.\begin{array}{l} Q \ G \text{ torseur} /k \\ G \to G' \end{array}\right)$ induisent un torseur Q' sur G' caractérisé par l'existence d'une flèche $Q \to G'$ compatible avec $G \to G'$.

Donc Q est une fibre de l'espace homogène.

le 18.10.93

III - 2

Les différentes façons d'envoyer $Q \to G'$ diffèrent d'un pt de $G'(k)$.
Dc

$$\begin{matrix}\text{les } G \text{ torseurs} \\ G' \text{ triviaux}\end{matrix} \longleftrightarrow \begin{matrix} G'/G\,(k) \text{ modulo} \\ \text{l'act}^{o} \text{ de } G'(k)\end{matrix}.$$

<u>En d'autres termes</u>: on a la suite exacte de cohomologie galoisienne suivante:

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

On va continuer à exploiter l'existence d'objets versels.
On va commencer par montrer le thm suivant:

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

Autrement dit, si on note
$H^q_e(G, \Pi) = H^q(G, \Pi) / H^q_n(G, \Pi)$
(effectif)

<u>Thm 1</u>: $\boxed{2\, H^q_e(G, \Pi) = 0 \text{ si } q > N_1}.$

le 18.10.93

③

En fait, on va même montrer mieux :

Thm 2 : $\hat{m}$ notation et $\hat{m}$ hyp.
Il existe un entier N_2 tel que pour tout $q > N_2$ on ait équivalence entre
(i) x est négligeable
$\Updownarrow$
(ii) la restriction de x à tt sous gpe d'ordre 2 de G est 0.

Rque : (i) $\Rightarrow$ (ii) est clair car
{ restriction d'un nég. est nég.
{ Seul 0 est nég. pour ss 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 torseur versel 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 $\operatorname{cd} K(i) = d+2$.
(Grothendieck ?; Tate, Lang ; Cohom. gal.).
De plus $\operatorname{scd} K(i) \leq d+3$.

Le 18.10.93

III - 4

(Rappel : cd est relative aux mod. de torsion.
scd quelconques

On a donc
$H^q(K(i), \Gamma) = 0$ si $q > d+1 = N$,
$\Downarrow$ par transfert
$2H^q(K, \Gamma) = 0$ si $q > N$, .

Alors si $x \in H^q(G, \Gamma)$
$\downarrow$
$x_K \in H^q(K, \Gamma)$. $2x_K = 0$.

Ici, comme le torseur est usuel, ceci permet de conclure.

On va maintenant démontrer le 2nd thm. On aura besoin d'un certain nbre 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 : $\boxed{\text{Si } \Gamma \text{ est un } \Gamma_K \text{ module (resp. de torsion) ; si } q > n+1 \text{ (resp. } > n\text{) ; et si } x \in H^q(\Gamma_K, \Gamma) \text{ a une restriction nulle à tous les sous gpes d'ordre 2 de } \Gamma_K, \text{ alors } x = 0.}$

Rappels (Artin-Schreier).
Si K est un corps, et $s \in \Gamma_K$ un élt d'ordre fini $m \geq 2$, alors :

1. $\operatorname{car} K = 0$
2. $m = 2$
3. s est la conjugaison complexe associée à une structure de corps ordonné sur K (ou (ce qui revient au même)

$\begin{array}{c} \overline{K} \\ | \\ K \end{array}$ $\overline{K}^{\langle s \rangle}$ est un corps ordonné maximal.

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

Rqe : Soit X l'ens. des élts d'ordre 2 de Γ_K. Γ_K opère sur X par conjugaison. Posons $\Omega = X / \Gamma_K$. Alors

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

X est compact car $\{s \text{ tq } s^2 = 1\}$ l'est et 1 est un élt isolé ds cet ens. (cf. $\begin{array}{c} K(i) \\ | \\ K \end{array}$).

Démonstration de (4) :
Si $t \in \Gamma_K$ commute à s, alors t définit un automorphisme du corps $R = \overline{K}^{\langle s \rangle}$, 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 $\in R$.

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.
Dc t fixe les x_i

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

Thm : $\boxed{\text{Si } \Gamma \text{ est un gpe profini, et } \Gamma_1 \text{ un ss.gpe ouvert de } \Gamma \text{, on a } cd_p \Gamma = cd_p \Gamma_1 \text{, pourvu que } \Gamma \text{ ne contienne pas d'élts d'ordre } p.}$

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

Si K contient i, il n'y a pas d'élts d'ordre 2 ds Γ_K, et le m̂ argument s'applique.

le 18.10.93

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

On se place dans le cas particulier où $\Pi = \mathbb{Z}/2\mathbb{Z}$.
cf. article Colliot-Thélène et Parimala. (Inv. 1989).
Les arguments viennent d'Arason (1975)
cf. article Arason-Elman-Jacob.

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

<u>Passage de la cohomologie d'un gpe à celle d'un ss gpe d'ordre 2.</u>

Soit G un gpe, et G_1 un ss gpe d'indice 2.
$G \xrightarrow{\varepsilon} \{\pm 1\}$; $G_1 = \mathrm{Ker}\,\varepsilon$.
Soit Π un G-module.
Π_ε est le tordu de Π par ε, i.e.
$\Pi_\varepsilon = \Pi \otimes_{\mathbb{Z}} \mathbb{Z}_\varepsilon$,

où $\mathbb{Z}_\varepsilon = \mathbb{Z}$ muni de l'action de G : chgt de signe par ε.
$H^1(\{\pm 1\}, \mathbb{Z}_\varepsilon) \simeq \mathbb{Z}/2\mathbb{Z}$. Notons (ε), l'unique élt canonique d'ordre 2.
On lui associe un élt de $H^1(G, \mathbb{Z}_\varepsilon)$, qu'on note encore (ε)..

Le cocycle correspondant est défini par $s \in G \to \begin{cases} 0 \text{ si } s \in G_1 \\ 1 \text{ si } s \notin G_1. \end{cases}$

Lemme: On a la suite exacte:

$$\cdots \to H^q(G,\Omega) \xrightarrow[\text{Res}]{} H^q(G_1,\Omega) \xrightarrow[\text{Cor}]{} H^q(G,\Omega_\varepsilon) \xrightarrow[\delta]{} H^{q+1}(G,\Omega) \to \cdots$$

Rqe: En fait

$$\begin{tikzcd} H^q(G_1,\Omega) \arrow[r] \arrow[d, equal] & H^q(G,\Omega_\varepsilon) \\ H^q(G_1,\Omega_\varepsilon) \arrow[ur, "\text{Cor}"'] & \end{tikzcd}$$

car $\Omega_\varepsilon = \Omega$ cô G_1 module.

Par ailleurs: $\mathbb{Z}_\varepsilon \otimes \Omega_\varepsilon \to \Omega$.

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

Lemme: Soit $x \in H^q(G,\Omega)$.
$\text{Res}(x) = 0$
$\iff x$ est div. par $(\varepsilon)_1$
i.e. si $\exists\, x' \in H^{q-1}(G,\Omega_\varepsilon)$
tq $x = (\varepsilon)_1 x'$.

(C'est une conséquence directe du lemme précédent: exactitude).
C'est un lemme standard en cohom. d'ordre 2.

Démonstration ds ce cas :

$\tilde{\Pi} := \mathrm{Ind}_{G_1}^{G} \Pi$.

$\tilde{\Pi} = \Pi \oplus \Pi$ cô gpe abélien, muni de l'actº 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

$$0 \to \Pi \to \tilde{\Pi} \to \Pi_\varepsilon \to 0$$ suite exacte de G modules.

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

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

La suite exacte de cohomologie induite est celle q'on veut.

$$\begin{array}{ccccccc} H^q(G,\Pi) & \to & H^q(G,\tilde{\Pi}) & \to & H^q(G,\Pi_\varepsilon) & \xrightarrow{\delta} & H^{q+1}(G,\Pi) \\ & & \| \text{ Shapiro} & \nearrow \text{Cor} & & & \\ & & H^q(G_1,\Pi) & & & & \end{array}$$

(facile à vérifier)

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

<u>Calcul</u> : On part d'un q-cocycle ds Π_ε $m(g_1, \dots, g_q)$. $m \in \Pi_\varepsilon$ peut se relever en $(m, 0)$.

dc

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

On veut calculer

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

On obtient donc

$$\delta \tilde{m}(g_1,\dots,g_{q+1}) = \begin{cases} (g_1 m(g_1,\dots,g_{q+1}),0) \\ \text{ou} \\ (0, g_1 m(g_2,\dots,g_{q+1})) \end{cases} - (m(g_1 g_2,\dots,g_{q+1}),0) \dots \pm (m(g_1,\dots,g_q g_{q+1}),0)$$

suivant que $g_1 \in G_1$ ou non.

Mais m est un cocycle ds $\mathbb{Z}_\varepsilon$. Dc pratiquement H s'en va, et on obtient finalement $\delta\tilde{m} = (\varepsilon)_1 \cdot m$.

Le pt ② d'Artin Schreier explique bien pourquoi les élts de torsion st d'ordre 2.

Si $s \in \Gamma_K$ est d'ordre $n > 2$, alors $\bar{K}^{\{s\}} = K'$; $\Gamma_{K'} = C_n$.

Alors o est le seul élt nég. de la cohomologie de C_n

↳ contradiction.

On a dc $K_1 = K(i)$ (situation du thm. p. ④).

$\begin{array}{c} K_1 = K(i) \\ | \\ K \end{array}$ $\mathbb{Z}$ est un Γ_K module.

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

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

↳ fournit un caractère ε d'ordre 2.

Prop. : Si $q > n+1$, alors le cup produit par $(\varepsilon)_1 \in H^1(\Gamma_K, \mathbb{Z}_\varepsilon)$ est un isom. de $H^q(\Gamma_K, \mathbb{Z}_\varepsilon)$ dans $H^{q+1}(\Gamma_K, \mathbb{Z})$.

<u>Preuve</u>: $H^q(\Gamma_{K_1}, \mathbb{Z}) = 0$. Donc la suite exacte devient

$$0 \to H^q(K, \mathbb{Z}_\varepsilon) \xrightarrow[\sim]{\delta} H^{q+1}(K, \mathbb{Z}) \to 0 \ .$$

On a une sorte de périodicité d'ordre 2.

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

$(\varepsilon)_1 \cdot (\varepsilon)_1 = (\varepsilon)_2 \in H^2(K, \mathbb{Z})$
$\qquad\qquad\qquad\qquad\qquad \Vert$
$\qquad\qquad\qquad\qquad H^1(K, \mathbb{Q}/\mathbb{Z})$.

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

$(\varepsilon)_2$ est la préimage de u.

$$\boxed{H^q(\Gamma_K, \mathbb{Z}) \xrightarrow{\sim} H^{q+2}(\Gamma_K, \mathbb{Z}) \quad \text{par cup produit par } (\varepsilon)_2 .}$$

De façon g$^{\text{ale}}$, si $\varphi : \Gamma_K \to (\pm 1)$, on lui associe :
$$\begin{cases} \varphi \in H^1(\Gamma_K, \mathbb{Z}/2\mathbb{Z}) \\ (\varphi)_1 \in H^1(K, \mathbb{Z}_\varphi) \\ (\varphi)_2 \in H^2(K, \mathbb{Z}). \end{cases}$$

Cô car $K = 0$,

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

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

<u>Lemme</u>: $\boxed{\begin{array}{l} \text{Si } (a)(b) = 0 \text{ ds } H^2(K, \mathbb{Z}/2\mathbb{Z}),\ a, b \in k^* \\ \text{on a } (a)_1 (b)_2 = 0 \text{ ds } H^3(K, \mathbb{Z}(a)). \end{array}}$

En particulier, $(a)_1(-a)_2 = 0$ $\forall a \in K^*$.
(On sait en effet $(a)(-a) = 0$).

<u>Preuve</u>: $0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$

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

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

Posons $(b) = \varphi$

$(a)_1(b)_2 = (a)_1\, \delta(\varphi)$.

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

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

$(a)_1 . \varphi \in H^2(K, \mathbb{Z}_{(a)} \otimes \mathbb{Z}/2\mathbb{Z}) = H^2(K, \mathbb{Z}/2\mathbb{Z})$.

$\delta_{(a)}((a)_1 \varphi) = (a)_1\, \delta(\varphi) = (a)_1 (b)_2$.

Mais $(a)_1 \varphi = (a)(b) = 0$.

Dc $\delta_{(a)}((a)_1\varphi) = 0$. <u>cqfd</u>.

<u>On devrait maintenant pouvoir démontrer le thm 2. (idée d'Arason)</u>.

Soit $x \in H^q(\Gamma_K, \Omega)$ avec $q > n+1$ (resp. $> n$).
On suppose que $\mathrm{Res}_H(x) = 0$ pour tout sous groupe H d'ordre 2. <u>mq</u> $x = 0$.

Supposons $x \neq 0$.
Soit S l'ens. des ss gpes fermés H de Γ_K tels que $\mathrm{Res}_H(x) \neq 0$.
On l'ordonne par inclusion descendante.
Si (H_α) est une famille totalement ordonnée d'élts de S, alors $\bigcap_\alpha H_\alpha$ est ds S
$(H^q(H, \Omega) = \varinjlim (H^q(H_\alpha, \Omega)).)$.

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

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

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

① Γ_K est un pro 2 gpe.
Sinon, soit H un 2 Sylow de Γ_K.
$H \neq \Gamma_K$ et $\mathrm{Res}_H(x) = 0$. contradicto.

② Γ_K est cyclique.

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

Il est clair que $i \notin K$. Dc $K(i)/K$ est
une ext. quadratique. Elle correspond
à un élém^t $(-1) \in H^1(K, \mathbb{Z}/2\mathbb{Z})$.
Dc $\dim \geq 1$.
Si $\dim H^1(K, \mathbb{Z}/2\mathbb{Z}) > 1$, il y aurait un autre
élém^t $a \in K^*$ tq $(a) \neq (0), (-1)$

$x \in H^q(K, \Gamma)$. On restreint x au ssgpe
d'indice 2 défini par a. Par le
lemme, on trouve 0. Dc $x = (a).x'$
avec $x' \in H^{q-1}(K, \Gamma a)$.

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

Donc $x = (-a)_1 x''$ avec $x'' \in H^{q-1}(K, \Pi_{-a})$.

Alors :

$(-1)_2 x = (-1)_2 (a)_1 x' \in H^2(K, \mathbb{Z})$.

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

Donc $(-1)_2 x = (a)_2 (a)_1 x' + \underbrace{(-a)_2 (a)_1 x'}_{0}$.

$(-1)_2 x = (a)_2 (a)_1 x' = (a)_2 x$.

$(-1)_2 x = \underbrace{(a)_2 (-a)_1}_{0} x'' = 0$. Donc $\boxed{(-1)_2 x = 0}$

Mais la multiplication par $(-1)_2$ est injective (cf. lemmes précédents).
Donc $\boxed{x = 0.}$

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

> G gpe profini ; G_1 ss gpe d'indice 2.
> $\varepsilon : G \to \pm 1$ $\quad$ $cd\, G_1 = n < \infty$.
> Pour H ss gpe fermé H de G, et $\forall\, \alpha \in H^1(H, \mathbb{Z}/2\mathbb{Z})$ on a $\alpha . \alpha = \varepsilon_H . \alpha$
> où $\varepsilon_H = \mathrm{Res}_H\, \varepsilon$.

- Γ_K est donc un pro 2 gpe tq $H^1(K, \mathbb{Z}/2\mathbb{Z})$ est de dim. 1.
  Mais le H^1 d'un pro p gpe détermine les générateurs de ce gpe.
  Donc Γ_K est engendré par un élém^t.

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

<u>Déjà</u> $\alpha > 1$ est imp. par Artin-Schreier.
<u>De plus</u> pour $\mathbb{Z}_2$
$H^q(\mathbb{Z}_2, \Gamma) = 0$ si $q \geq 3$.
Or ds le thm, $q \geq 3$
La contradict° car $x \neq 0$, $x \in H^q(\ldots)$.

<u>Supplément au thm</u> (Arason-Elman-Jacobi, Colliot-Thélène et Parimala).

<u>Cas où $\Gamma = \mathbb{Z}/2\mathbb{Z}$.</u>
$H^q(K, \mathbb{Z}/2\mathbb{Z}) \simeq \mathcal{C}(\Omega, \mathbb{Z}/2\mathbb{Z})$ (fct°ˢ continues).
où $\Omega = \{$structure d'ordre sur $K\}$
$= \{$él^{ts} d'ordre 2, à conj. près$\}$.
s d'ordre 2 $\in H^1(C_2, \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$.

<u>Ds le cas g^{al}</u>:
Sur Ω, on peut mettre deux faisceaux Γ^+ et Γ^-:
Si Γ est vu cô u faisceau cst sur Ω, on définit des sous-faisceaux:

$\Omega = \Gamma_2/\text{conj.}$ $\Gamma_2 = \{$él^{ts} de Γ_K d'ordre 2$\}$.
On a $1 \to \Gamma_{K_1} \to \Gamma_K \to C_2 \to 1$
pas de torsion.
Dc Ω revient à prendre les sect°ˢ qui st des ss gpes, à conj. près.

le 18.10.93

III - 16

On peut de trouver une section continue $\omega \in \Omega$ avec $s_\omega \in \Gamma_2$.

Du coup, on peut définir

$$\mathrm{Ker}(1-s_\omega)\Gamma / \mathrm{Im}(1+s_\omega)\Gamma = \Gamma_+(\omega) = H^{\text{pair}}(C_2,\Gamma)$$

et

$$\mathrm{Ker}(1+s_\omega)\Gamma / \mathrm{Im}(1-s_\omega)\Gamma = \Gamma_-(\omega) = H^{\text{impair}}(C_2,\Gamma)$$

Il paraît naturel que

$$H^q(V_1,\Gamma) \simeq H^0(\Omega, \Gamma_\pm)$$

$\begin{cases} + \text{ si } q \text{ pair} \\ - \text{ si } q \text{ impair.} \end{cases}$

(Mais ce n'est pas encore démontré.)

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

Ceci serait vrai pour

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

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 :

<u>Thm 2</u> : $\exists$ une cte N_2 (dpdt de G) telle que si Π est un G module, $q \geq N_2$ et $x \in H^q(G,\Pi)$, 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 <u>versel</u>, où on a K ext. de t.f. de $\mathbb{Q}$ et ext. gal L/K de gpe G.
L/K correspond à $\varphi : \Gamma_K \to G$.
x nég. $\iff \varphi^* x = 0$ ds $H^q(\Gamma_K, \Pi)$

On prend $N_2 = \deg \operatorname{tr} K + 3$.
On regarde $K(i)$ $\operatorname{cd} \Gamma_{K(i)} = \deg \operatorname{tr} K + 2$.
Alors si $K = K(i)$ pas de pb : $H^q(\Gamma_K, \Pi) = 0$.
Sinon $\Gamma_{K(i)} \subset \Gamma_K$ et on applique le thm démontré la dernière fois, qui dit que la cohom. est détectée par les ss gpes d'ordre 2. Si $\{1,c\} \subset \Gamma_K$ est un tel ss gpe $\{1,c\} \hookrightarrow \Gamma_K \xrightarrow{\varphi} G$
$\varphi(c)$ est d'ordre 1 ou 2 ds G.
ce qui permet de conclure

le 25.10.93

②

<u>Application</u>: $\Omega = \mathbb{Z}/2\mathbb{Z}$ $\quad H^q(G,\Omega) = H^q(G)$.

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

$H^\bullet(G)_e := H^\bullet(G) / H^\bullet(G)_n$

↑ On cherche à décrire ceci.

<u>Quillen</u>: a donné une description de Spec $H^\bullet(G)$ (encore valable en car. mod. p) en négligeant les élts nilpotents.

Pour car. mod. p:

$I \subset G$ élémentaire abélien $(p,\dots,p)$.

$I \subset I^{vect}$ $\quad I^{vect} = \operatorname{Spec} \operatorname{Sym}_{\mathbb{F}_p}(I^*)$.

Ex si p.ex. I est cyclique d'ordre p,

$I^{vect} = \mathbb{G}_a = \operatorname{Spec} \mathbb{F}_p[T]$ (dte affine).

Il est facile de voir que

$\operatorname{Spec} H^\bullet(I) = I^{vect}$. On a dc des flèches $I^{vect} \longrightarrow \operatorname{Spec} H^\bullet(G)$.

<u>Thm de Quillen</u>:

1) $\operatorname{Spec} H^\bullet(G) = \bigcup$ des images des I^{vect}

2) donne la rel. d'équiv. (induite par conj.).

2): si I_1, I_2 et g tq $gI_1g^{-1} \subset I_2$ on obtient des flèches entre les cohomologies, qui donnent l'identité au niveau de $\operatorname{Spec} H^\bullet(G)$.

Ds le cas où on a un p-Sylow élémentaire $(p, \dots, p)$, on a

$$\operatorname{Spec} H^\bullet(G) = \text{Sylow}^{\text{vect}} / \text{Norm}.$$

En particulier,

dim Spec $H^\bullet(G)$ = rg maximal des ss gpes élémentaires de type $(p, \dots, p)$.

Regardons maintenant $H^\bullet_e(G)$ ds le cas $\underline{p=2}$.

Proj. $(H^\bullet_e(G))$ est de dimension 0. Il est formé des classes de conjugaisons des involutions de G. C'est dc un ens. fini Ω. (Ce st des pts rationnels sur $\mathbb{F}_2$).

Spec $H^\bullet_e(G)$ = cone sur Ω.

En particulier, si $2 \mid |G|$, on voit que dim Spec $H^\bullet_e(G) = 1$.

i.e. dim $H^q_e(G)$ est bornée qd q varie.

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

---

le 25.10.93

IV-④

<u>Qques exples :</u> (sans démonstration).

<u>C_2</u> : $H^\bullet = H^\bullet_c = \mathbb{F}_2[t]$ t de degré 1.

<u>C_4</u> : $\dim H^q = 1$ $\forall q$. Notons α_1 et α_2 les élts non nuls de degré 1, 2, ils engendrent la col. avec la relation $\alpha_1^2 = 0$.

$(1, \alpha_1, \alpha_2, \alpha_1\alpha_2, \alpha_2^2, \dots)$

On mq $\alpha_1\alpha_2$ est nég., et engendre l'idéal des nég.

D $H^\bullet_c$: $1, \alpha_1, \alpha_2, 0, \alpha_2^2, 0, \alpha_3^2$.

Ceci dit, $H^3(C_4, \mathbb{Z}/4\mathbb{Z}) = \mathbb{Z}/4\mathbb{Z}$

Si on note β_3 u gén., $2\beta_3$ est nég. (mod. 2, c'est nég.) ; mais on peut mq β_3 n'est pas nég.

<u>S_4</u> : gpe symétrique d'ordre 4.

De façon gale, $H^\bullet(S_n) \supset w_i$

w_i = classes de Stiefel Whitney.

($S_n \longrightarrow O_n$

$B_{S_n} \longrightarrow B_{O_n}$ ← classes naturelles.

$H^\bullet(B_{S_n}) = H^\bullet(S_n)$.

donnent des élts ds

Ainsi w_1 correspond à $\mathrm{sgn} : S_n \longrightarrow \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$)

:

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

$$\begin{array}{llll} 1 & w_1^2 & w_1^3 & w_1^4 \quad \cdots \\ & w_2 & w_1 w_2 & w_1^2 w_2 \\ & & w_3 & w_2^2 \end{array}$$

Le Spec est de dim 2, formé de deux composantes irréductibles.

($\Updownarrow$
S_4 a deux types de ss gpes $(2,2)$:
1 contenu dans $\mathfrak{A}_4$ $\rightsquigarrow w_1 = 0$

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

Qd on passe à $H^\bullet_e(S_4)$ on introduit les rel. $\begin{cases} w_3 = 0 \\ \text{et} \\ w_1 w_2 = 0. \end{cases}$

i.e. $H^\bullet_e(S_4)$ engendré par w_1, w_2 avec la relat° $w_1 w_2 = 0$.

Groupe diédral d'ordre 8 : D_4

H^1 a une base $\{t_1, t_2\}$

$$\left.\begin{array}{l} t_1 \\ t_2 \end{array}\right\} : D_4 \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

à noyau de type $(2,2)$

La relat° $t_1 t_2 = 0$.

H^2 a comme base (t_1^2, t_2^2, e)
e est l'uniqu élément dt les restrict° aux ss gpes d'ordre 2 st $\neq 0$.

$H^\bullet(D_4)$ est engendré par (t_1, t_2, e) avec l'uniqu relat° $t_1 t_2 = 0$.

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

Bc $H^\bullet_e(D_4)$: 1 ; $\begin{matrix} t_1 \\ t_2 \end{matrix}$; $\begin{matrix} t_1^2 \\ t_2^2 \\ e \end{matrix}$; $\begin{matrix} t_1^3 = e t_1 \\ t_2^3 = e t_2 \end{matrix}$; $\begin{matrix} t_1^4 = e t_1^2 \\ t_2^4 = e t_2^2 \\ e^2 \end{matrix}$

Pour mq $t_i^3 + e t_i$ st négligeables, on peut regarder les dx plongements $D_4 \hookrightarrow S_4$. $\mathfrak{A}_3$ ds S_4 est nég., et ces dx élem^{ts} st ceux de D_4 qui donnent $\mathfrak{A}_3$.

<u>Q_8 gpe des quaternions d'ordre 8 :</u>

c'est un gpe à coh. périodique :

$H^\bullet(Q_8)$: 1 ; $\begin{matrix} t_1 \\ t_2 \end{matrix}$; $\begin{matrix} t_1^2 \\ t_2^2 \end{matrix}$; $\begin{matrix} t_1^2 t_2 \\ \| \\ t_2^2 t_1 \end{matrix}$; e_4 ; $\begin{matrix} e t_1 \\ e t_2 \end{matrix}$

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 $t_1^3 = t_2^3 = 0$

Le 25.10.93

⑦

On montre que $t_1^2 t_2 = t_2^2 t_1$ est négelig.
e n'est pas nég. ; et_1 et et_2 les$t$.
Dc

$$H_c^\bullet(Q_8) : 1 ; \begin{matrix} t_1 \\ t_2 \end{matrix} ; \begin{matrix} t_1^2 \\ t_2^2 \end{matrix} ; 0 ; \underset{\substack{\uparrow \\ \dim 4}}{e} ; 0 ; 0 ; 0 ; \underset{\substack{\uparrow \\ \dim 8.}}{e^2} ; \ldots$$

<u>Rqe</u>. $H^3(Q_8, \mathbb{Z}/8\mathbb{Z}) \simeq \mathbb{Z}/8\mathbb{Z}$ (Cartan Eilenberg).
Soit u un générateur.
On peut mq $\left\{ \begin{array}{l} 2u \text{ neg.} \\ u \text{ non neg.} \end{array} \right.$

Donc si $\begin{array}{c} L \\ | \; Q_8 \\ k \end{array} \longleftrightarrow \varphi : \Gamma_k \to Q_8$

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

<u>Thm</u>. $\boxed{\text{Les applications naturelles car} \neq 2 \quad H^3(k, \mathbb{Z}/2\mathbb{Z}) \to H^3(k, \mathbb{Z}/4\mathbb{Z}) \to H^3(k, \mathbb{Z}/8\mathbb{Z}) \text{ sont injectives.}}$

(conséquence d'un thm de Merkurjev)

<u>Preuve</u> : pour $H^3(k, \mathbb{Z}/4\mathbb{Z}) \to H^3(k, \mathbb{Z}/8\mathbb{Z})$.
On a $0 \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$.
Il faut de démontrer

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

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

Dx : $? \longrightarrow (x)(y)$.

$$H^2(k, \mu_8^{\otimes 2}) \quad x \mapsto \begin{cases} (x) \in H^1(k, \mu_2) \\ (x)_8 \in H^1(k, \mu_8). \end{cases}$$

$(x)_8 (y)_8$?

Mais $\mu_8^{\otimes 2} \simeq \mathbb{Z}/8\mathbb{Z}$. Si u racine primitive 8ème de 1,

$u \otimes u \in \mu_8^{\otimes 2} \longmapsto 1 \in \mathbb{Z}/8\mathbb{Z}$.

De tout ça, il résulte que si on a L/k Q_8 on peut lui attacher un inv. cohom. dans $H^3(k, \mathbb{Z}/2\mathbb{Z})$.

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

et $2\varphi^*(u) = 0$ implique que

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

<u>cf</u> article E. Bayer – Bases normales autoduales.

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

P.ex., on regarde q_L forme trace de L
c'est une f.q. de 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 $C = \{1,-1\}$ centre de Q_8.

$$\begin{array}{l} L \\ \big| \, 2 \\ L^C \\ \big| \\ k \end{array} \qquad \underset{\substack{\uparrow \\ \text{forme trace} \\ = \text{forme unité.}}}{L = L^C} \oplus L^-$$

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

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

On pose $b(L/k) = (-1)(-1)(x) \in H^3(k, \mathbb{Z}/2\mathbb{Z})$
($b(L/k) = (-1)(-1)(-1) +$ Arason).
$b(L/k) = 0$ si et seulement si $q_L \simeq \langle 1, \cdots, 1\rangle$
si et seulement si L/k a une base
normale autoduale.

$$\boxed{b = a \quad ?}$$

le 25.10.93

G gpe fini.

On va maintenant montrer deux thms :

Thm : $\boxed{\text{Si } a \in H^2(G,\Pi) \text{ et si l'act° de } G \text{ sur } \Pi \text{ est triviale, alors } a \text{ nég.} \iff a = 0}$

(Π de type fini).

On peut se ramener à $\Pi = \mathbb{Z}$; $\Pi = \mathbb{Z}/p^\alpha\mathbb{Z}$ p prem $\alpha \geq$

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

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

$G \to C_n \quad n \geq 1.$

D° $\Pi = \mathbb{Z}$ est un cas très simple.

$\Pi = \mathbb{Z}/p^\alpha\mathbb{Z}$: $\underset{\neq 0}{x} \in H^2(G,\mathbb{Z}/p^\alpha\mathbb{Z})$

mq x n'est pas nég. Il faut donc exhiber un corps...

pt essentiel de la dém. : soit k_0 le corps des racines $p^{\alpha \text{ième}}$ de 1 (sur $\mathbb{Q}$). Alors k_0 ne contient pas de racines primitives $p^{\alpha+1}$ ième de 1.

(Irréductibilité du pol. cyclotomique).

D° $C_{p^\alpha} \subset k^*$.

Lemme : Soit F un corps de nbre et μ_F le ss gpe des racines de l'unité de F. Alors $F^* \simeq \mu_F \times L$ L ab. libre.

Preuve : E unités de F.
Dirichlet : $E = \mu_F \times L_1$
Mais $F^\times/_E \simeq$ id. ppx $\subset$ gpe des idéaux.
Or gpe des id. est libre, de base les id. premiers. Dc (tt ss gpe d'un libre est libre) $F^\times/_E \simeq L_2$
et $F^\times = \mu_F \times L_1 \times L_2$.

Ainsi C_{p^α} est facteur direct dans $\bar{k_0}^*$.
$\mu_{\bar{k_0}^*} = C_{p^\alpha} \times$ reste.
Dc $\boxed{H^2(G, C_{p^\alpha}) \hookrightarrow H^2(G, \bar{k_0}^*)}$

On va maintenant faire le calcul sur un corps voisé.
On choisit p.ex. un plongement de G ds S_n, et on fait opérer G sur
$L = k_0(T_1, \dots, T_n)$.
$K = L^G$ invariants.
On va mq la classe $x_K \in H^2(K, \mathbb{Z}/p^\alpha\mathbb{Z})$ est non nulle.
$\mathbb{Z}/_{p^\alpha}\mathbb{Z} \simeq \mu_{p^\alpha}$.
Dc $H^2(K, \mathbb{Z}/p^\alpha\mathbb{Z}) = H^2(K, \mu_{p^\alpha}) \simeq Br_{p^\alpha}(K)$.

On a

$$1 \to h_0^* \to L^* \longrightarrow \mathrm{Div} \to 1 .$$

(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.

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

$$\mathrm{Dirr} = \coprod_\alpha G/G_\alpha .$$

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

(un gpe fini n'a pas d'hom. non trivial ds $\mathbb{Z}$)

Dc $\quad H^2(G, C_{p\alpha}) \hookrightarrow H^2(G, h_0^*)$

$$0 \to H^2(G, h_0^*) \longrightarrow H^2(G, L^*)$$
$$ \cap$$
$$ Br(K).$$

$$\begin{matrix} \psi \\ x \end{matrix} \quad \longmapsto \quad \text{un él}^t \neq 0.$$

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

Rest un G module qcq.

Soit Γ le gpe profini produit semi direct $\Gamma = \mathbb{Z}_p . U_p'$.
($U_p = \mathbb{Z}_p^*$; $U_p' = 1 + p\mathbb{Z}_p \hookrightarrow U_p'$).

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

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

$\varepsilon : \Gamma \to C_p$

$\begin{cases} \sigma \mapsto \sigma_p \in C_p \\ \tau \mapsto 1 \in C_p \text{ (élt neutre)}. \end{cases}$

Thm : ① La projection $\varepsilon : \Gamma \to C_p$ a la propriété de relèvement. (i.e. tout hom. continu $\Gamma_k \to C_p$ se relève à $\Gamma \to C_p$).
② Il existe un corps k, de car 0, avec $\Gamma_k = \Gamma$.

Cor 1 : Une classe $x \in H^q(C_p, \mathbb{Z})$ est nég. ssi $\varepsilon^* x = 0$ ds $H^q(\Gamma, \mathbb{Z})$.

Cor 2 : Si $q \geq 3$, x est nég.

Cor 2 :

Γ est un gpe de Lie de dim 2 p adique, réalisé par $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ $\begin{cases} a \in U_p^1 \\ b \in \mathbb{Z}_p \end{cases}$.

Dc $\operatorname{scd}\Gamma = 2$

et $H^q(\Gamma, \Pi) = 0 \quad \forall q \geq 3$,

Cor 1 :

$\Rightarrow$ évident.

$\Leftarrow$ vient du relèvement.

$H^2(C_p, \Pi)$, Π C_p module.

c'est $\Pi^{C_p} / (1 + \sigma_p + \dots + \sigma_p^{p-1})\Pi$ $\quad \sigma_p$ générateur de C_p.

Cor 3 : Soit dc $x \in \Pi^{C_p}$.

$x \mapsto$ classe négligeable

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

où $y \in \Pi$ et $z \in \Pi$, z p primaire.

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

Dc : si l'act° est triviale, rien n'est négligeable à part 0.

Par contre Π de type (p, p), σ_p agissant par $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \longrightarrow H^2(C_p, \Pi) \neq 0$ mais nég.

Le 25.10.93

IV-(15)

Principe de la dém. du cor 3 :

$x \in H^2(G_p, Z)$

$$\begin{tikzcd}
 & 0 \arrow[d] \\
 & Z \arrow[d] \\
 & E_x \arrow[d] \\
\Gamma \arrow[r, "\varepsilon"] \arrow[ur, dotted] & G_p \arrow[d] \\
 & 0
\end{tikzcd}$$

ε doit se relever. le relèvement est dét. par les images de σ et τ. La relation imposée à σ et τ donne φ et γ.

Dém. du thm :

(2) On veut donc construire un corps k, avec $\Gamma_k \simeq \Gamma$.

Soit k_1 un sous corps de $\overline{\mathbb{Q}}$ contenant $\sqrt[p]{1}$ tq $\chi_p : \Gamma_k \to U_p$ soit un isom.

$\Gamma_k \xrightarrow{\sim} U_p'$.

Un tel corps existe :

$\chi_p : \Gamma_k \to U_p$.

(p Sylow) $S \to U_p'$ p Sylow

12

$\mathbb{Z}_p \subset S \to \mathbb{Z}_p$ libre

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

Le 25.10.93

(16)

Posons $k_2 = k_1((T))$.

Γ_{k_2}.

$$1 \to \varprojlim \mu_n \longrightarrow \Gamma_{k_2} \longrightarrow \Gamma_{k_1} \longrightarrow 1$$

$$\overset{\Vert}{\prod_{\ell} \mathbb{Z}_\ell(1)}$$

) muni de l'action naturelle de Γ_{k_1}.

$$k = \bigcup_{(m,p)=1} k_2(T^{1/m}) \quad \left(\text{Choisir } \begin{array}{l} T = T_m^{\,m} \\ T_m = T_{mn}^{\,n} \end{array}\right).$$

D'où

$$1 \to \mathbb{Z}_p \longrightarrow \Gamma_k \to \mathfrak{V}_0' \longrightarrow 1.$$

cqfd.

Reste à mq Γ a la propriété de relèvement. Il suffit de le faire en car 0.

On suppose $k \ni \sqrt[p]{1}$.

L
|
k cyclique de d° p.

z_1 racine primitive $p^{\text{ième}}$ de 1.

$L = k(\sqrt[p]{x}),\ x \in k^*$

Act° : $\sqrt[p]{x} \mapsto z_1 \sqrt[p]{x}$.

Relever $\Gamma_k \to \Gamma$ revient à trouver une ext. gal. de k dt le gpe de gal. se plonge dans h.

Le 25.10.93

17

On adjoint à k ttes les racines p^{α} ièmes de 1 et de x.

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

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

Si $s \in \mathrm{Gal}(L/k)$:

$s(z_\alpha) = z_\alpha^{\chi(s)}$ $\quad \chi(s) \in U_p^1$.

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

Si $s \longmapsto \begin{pmatrix} \chi(s) & n(s) \\ 0 & 1 \end{pmatrix}$

On obtient un plongement $\mathrm{Gal} \to \Gamma$

Qd $k \not\supset {}^p\Gamma_1$ (cas général)

Si $k' = k({}^p\Gamma_1)$ $\quad \Gamma_{k'}$ $\quad [\Gamma_k : \Gamma_{k'}]$ est d'ordre premier à p.

$$\begin{array}{cc} k' & \Gamma_{k'} \\ | & \cap \\ k & \Gamma_k \end{array}$$

$$\begin{tikzcd} & \Gamma \arrow[d] \\ \Gamma_k \arrow[ur, dashed, "?"] \arrow[r, "\varphi"'] & C_p \end{tikzcd}$$

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

$$1 \to p\mathbb{Z}_p \to \Gamma \to C_p \times U_p^1 \to 1$$

$$(x, y) \mapsto (x \bmod p, y)$$

Le 25.10.93

(18)

L'extension est décrite par un élt de $H^2_{cont.}(C_p \times U_p', p\mathbb{Z}_p)$.

De plus

$$\begin{tikzcd} \Gamma_h \arrow[r, "\langle \chi_p \rangle"] \arrow[dr, "\text{caract. cyclotom.}"'] & U_p' \\ & U_p = C_{p-1} \times U_p' \arrow[u] \end{tikzcd}$$

$$\Gamma_h \longrightarrow C_p \times U_p'$$
$$\psi = (\varphi, \langle \chi_p \rangle).$$

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

Le $u \in H^2_{cont}(C_p \times U_p', p\mathbb{Z}_p)$.
$\psi^* u = 0$ ds $H^2_{cont}(\Gamma_h, p\mathbb{Z}_p)$ si $h \ni \sqrt[p]{1}$.

On invoque coros
$(\Gamma_h : \Gamma_{h'})$ premier à p
$\Rightarrow H^2_{cont}(\Gamma_h, \mathbb{Z}_p) \hookrightarrow H^2_{cont}(\Gamma_{h'}, \mathbb{Z}_p)$.
(vrai ; démontré par un élève de Lastra).
Ceci permet de conclure.

<u>Pb</u> : C_{p^2} ??

On n'a pas de $\Gamma \to C_{p^2}$ qui soit
{ relèvement
{ gpe de gal. ab. d'un corps.

J.-P. Serre V
Cours au collège
de France.
le 08 novembre 93

V-1

Qques commentaires sur le cours précéd^t:

1) U Jannsen:
Soit k u.c. de nbres totalem^t imag.,
et K une ext. de k de deg. de tr d.
$\Gamma_K = \mathrm{Gal}(\bar{K}/K)$. Alors $scd(K) \leq d+2$.
($cd(K) \leq d+2$ était déjà connu.
Il y a égalité si K/k de t. fini).
(Cela revient à mq $H^{d+2}(K, \mathbf{Q}/\mathbf{Z}) = 0$.).

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

2) On a montré que (G fini)
si Γ est u G module, à action triviale,
et si Γ est de t. fini sur $\mathbf{Z}$,
alors 0 est le seul él^t nég. de
$H^2(G, \Gamma)$.
Enfait l'hypothèse "Γ de t. fini"
est inutile.
En effet Γ qcq $H^i(G,\Gamma)_n = \varinjlim H^i(G,\Gamma_\alpha)_n$
où les Γ_α st les sous $\mathbf{Z}[G]$ modules
de t. fini de Γ.
(Cela résulte de l'existence
d'objets versels. $\Gamma_K \to G$).

3) Cohom. de $G = Q_8$ gpe des quat.
d'ordre 8.

$H^i(G)$ mod. 2 a été mal décrit

$i =$	0	1	2	3
dim	1	2	2	1
base	1	x, y	x^2, y^2	$x^2y = xy^2$

$x^3 = y^3 = 0$.

<u>en effet</u>: $x^2+xy+y^2 = 0$ (1)

$x^3 + x^2y + xy^2 = 0$

$x^2y + xy^2 + y^3 = 0$.

On applique d à (1) $x^2y + xy^2 = 0$.

Dc $x^3 = y^3 = 0$.

<u>On va mq</u> x^2y est nég.

$h \quad \Gamma_h \to G$

x et y donnent $x_h \in H^1(h)$.

Mais $x_h^2 = (-1)x_h$.

Dc $(-1)x_h + x_h y_h (-1) y_h = 0$.

Dc $\underbrace{(-1)(-1)x_h}_{= x_h^3} + \underbrace{(-1)x_h y_h}_{= x_h^2 y_h} + \underbrace{(-1)(-1)y_h}_{= y_h^3} = 0$.

Mais $= x_h^3 \quad = x_h^2 y_h \quad = y_h^3$.

Dc ($x_h^3 = y_h^3 = 0$) $x_h^2 y_h = 0$

et x^2y est bien nég.

Invariants cohomologiques attachés à des G torseurs.

On a un corps de base k_0.
(e.g. $k_0 = \mathbb{Q}$).
G est un gpe alg. lin. lisse 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 torseurs sur k. On notera
$P(G,k)$ = classes d'isom. de tels torseurs.
$$P(G,k) = H^1(k,G).$$

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.
en car. 0 : classes d'alg. de Lie de type E_8.

Si $G = S_n$ $\quad P(G,k)$ = classes d'isom. d'algèbres étales sur k de rang n.

Invariants cohomologiques :
On fixe un Γ_{k_0}-module C.
On suppose que C est fini, et d'ordre premier à la caract.
(i.e. C est un gpe abélien fini sur lequel Γ_{k_0} opère continuement).
Exple : $\mu_n^{\otimes i}$, n premier à la caract.

$C_{/k} = C$. $\quad H^i(k, C)$.

Un invariant cohom. pour G de type (i, C) est une règle qui associe à tout torseur T sur G, déf/k un élt $a(T) \in H^i(k, C)$, avec axiomes (1) et (2).

C'est de la donnée pour tout k/k_0 d'une app $a : P(G,k) \to H^i(k,C)$ avec (1) et (2).

(1) dit que si on a un homomorphisme $k \to k'$

$$\begin{tikzcd} P(G,k) \arrow[r] \arrow[d, "a"'] \arrow[dr, phantom, "\circlearrowright"] & P(G,k') \arrow[d, "a"] \\ H^i(k,C) \arrow[r] & H^i(k',C) \end{tikzcd}$$

En g^{ale}, 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.
$k_0 \to R \to k$. k est une k_0 algèbre.
On suppose K est complet.
Soit T un G torseur sur Spec$R$.
$R \to k$, $\to K$. Dc on a T_k, T_K G torseurs sur k, K
(Situation de "bonne réduction").

$a(T_k) \in H^i(k,C)$.
$a(T_K) \in H^i(K,C)$.

<u>Axiome (2)</u> $H^i(k,C) \xrightarrow{\varepsilon} H^i(K,C)$ envoie $a(T_k)$ sur $a(T_K)$

ε vient de l'existence d'une flèche $\Gamma_K \to \Gamma_k$. ε est inj.

<u>Rappel</u>: $\Gamma_K \to \Gamma_k$ est surjective. Elle est également scindée. (Δ l'image de $H^i(k,C)$ 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 k ds R: il existe $k \to R$ tq $k \to R \to k$ est l'identité. (Vrai pour tt anneau noeth. complet en égale caract.).

Mais
$$\begin{tikzcd} k_0 \arrow[r] \arrow[dr] & R \arrow[d] \\ & k \end{tikzcd}$$

(*) | Supposons que le relèvement de k prolonge celui de k_0

(*) est vérifiée en car 0 (Bourbaki).

En car p, si k est une ext. sép. de t. finie de k_0, alors (*) est vérifiée.

le 08.11.93

(7)

[mod. EGA 0_{IV} ? 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_k par le plongement $\varphi : k \to R$.
En fait $T' \simeq T$, car ce st dx torseurs sur R qui ont m̂ réductⁿ mod. l'id. max.
[et Grothendieck-Hensel:
Torseurs sur R $\leftrightarrow$ torseurs sur k].
Dc $T_{/k}$ $\quad \underbrace{T_{/R}}_{T'}$ $\quad T_K$.

$a(T_k) = a(T_K)$ résulte maintenant du chgt de base pour $k \to K$.

Dc sur un corps parfait, et a car 0, axiome (2) ne sert à rien.

Notation pour les inv. cohom. d'un type donné: $A(G, k_0, i, C)$.

Pb : calculer explicitement ?
$A(G, k_0, i, C)$

Invariant cst :

On se donne $\alpha \in H^i(k_0, C)$.
$\forall k$, on a déduit $\alpha_k \in H^i(k, C)$.
$a(T) = \alpha_k$ qq soit $T \in P(G, k)$.
On notera $A_{cst}(G, k_0, i, C)$ {inv. csts}.
$\quad\quad\quad\quad\quad\quad\quad\quad \wr\!\wr$
$\quad\quad\quad\quad\quad\quad\quad\quad H^i(k_0, C)$.

Inv. normalisé : $a(T) = 0$ si T est trivial.
A_0 ss gpe des inv. norm.
On a $\boxed{A = A_{cst} \oplus A_0.}$

Un exple : (dpdt de $j = 1, 2, 3$).
(1) $G = C_2$ gpe cycl. d'ordre 2
(2) $G = PGL_2$ quotient de GL_2/centre
(3) $G = G_2$ déployé.

$C = \mathbb{Z}/2\mathbb{Z}$. On notera $H^i(k) = H^i(k, \mathbb{Z}/2\mathbb{Z})$.
car $k_0 \neq 2$. i qcq.

Ds chacun de ces cas, il existe un $a_i \in A(G, k_0, i, C)$ canonique.

(1) C_2 torseur $\leftrightarrow$ ext. quad. de k $\leftrightarrow$ hom. continus Γ_k ds $\mathbb{Z}/2\mathbb{Z}$
$$\overset{\shortparallel}{H^1(k)}.$$

$$k[X]/_{X^2-\alpha} \longmapsto (\alpha) \in H^1(k).$$

Donne un a_1 à val. ds H^1.

(2) PGL_2 torseurs $\leftrightarrow$ alg. de quat. /k

$$\begin{cases} i^2 = \alpha \\ j^2 = \beta \\ ij = -ji \end{cases}$$

alg. de quat $(\alpha, \beta) \longmapsto (\alpha)(\beta) \in H^2(k)$.

a_2 à val. ds $H^2(k)$.

(3) G_2 torseurs $\leftrightarrow$ octonions.
inv. dû à Arason
$(\alpha, \beta, \gamma) \longmapsto (\alpha)(\beta)(\gamma) \in H^3(k)$.
a_3 à val. ds $H^3(k)$.

Thm. Ds ces 3 cas, tt inv. cohom. $\in A(G, k_0, j, \mathbb{Z}/2\mathbb{Z})$ s'écrit de façon !
$a = x_0 + (x_1)(a_i)$
$x_0 \in H^j(k_0)$; $x_1 \in H^{j-i}(k_0)$.

En d'autres termes :

$$\boxed{\begin{array}{l} A(G,k_0) := \bigoplus_{i=0}^{\infty} A(G,k_0,i,\mathbb{Z}/2\mathbb{Z}). \\ A(G,k_0) \text{ est un } H^0(k_0) \text{ module libre,} \\ \text{de base } (1, a_i). \end{array}}$$

<u>Cor</u> : tt inv. normalisé est un multiple de l'invariant fondamental a_i (à val. ds H^i).

<u>Rques</u>

1) En part., on a $a_i^2 = x_0 + x_1 a_i$.

Cela donne

$a_i^2 = \varepsilon^i a_i$ $\quad \varepsilon^* = (-1) \in H^1(k_0)$.

2) Oct $\simeq$ 3-f. de Pfister $\hookrightarrow$ elt de $H^3(k)$

Rost, Merkurjev, Suslin.

$H^1(k, G_2)$ = ss ens. de $H^3(k)$ formé des elts décomposables (au sens strict).

3) On pourrait étudier des inv. cohom. associés aux r formes de Pfister. La dém. qui suit s'applique.

4) Cas de F_4 (déployé).

<u>inv. col. mod. 2</u>

On trouve dx inv. $\begin{cases} a_3 \in H^3(k) \\ a_5 \in H^5(k) \end{cases}$

qui a fait ass $\begin{cases} 3 \\ 5 \end{cases}$ formes de Pfister.

On peut mq inv. col. de F_4 mod. 2 forment u mod. libre de base $1, a_3, a_5$.

<u>inv. col. mod. 3</u> $\quad \mu_3^{\otimes 2}$ N.B.

inv (Rost) $\in H^3(k, \mathbb{Z}/3\mathbb{Z})$.

m̂ genre de résultat.

(N.B. : Conjecturalement $H^i(k, \mu_n^{\otimes(i-1)}) \xrightarrow{\text{inj?}} H^i(k, \mu_{nm}^{\otimes(i-1)})$).

<u>Pb</u>, Un torseur sous F_4 est-il déterminé par ses deux inv. mod. 2 et son inv. mod. 3 ?

---

5) <u>Pb</u>, Y a-t-il u inv. col. pour E_8 norm., nn identiqumt nul, à valeurs ds $H^3(k, \mathbb{Z}/2\mathbb{Z})$? (Oui, Rost ?).

On va maintenant démontrer le thm.
On se place (p. ex.) ds le cas $i=2$.
$PGL_2 \leftrightarrow$ alg. de quaternions.

h_0 est fixé.
$h = h_0(X,Y)$ X et Y indéterminées.
Alg. de quat. $i^2 = X$; $j^2 = Y$; $ij = -ji$.
$a(T) \in H^\bullet(h) = H^\bullet(h_0(X,Y), \mathbb{Z}/2\mathbb{Z})$.

<u>1ère étape</u> Soit $a \in \overline{A}$.
<u>mq</u> $a(T) = x_0 + x_1(X) + x_2(Y) + x_3(X)(Y)$
avec $x_i \in H^\bullet(h_0)$; écriture unique.
$(X) =$ élt de $H^1(h)$ déf. par X ....

<u>Raison</u>: cette classe de cohom. n'a pas de pôles sur l'esp. affine $\mathbb{A}^2$ en dehors de $X=0$ et $Y=0$.

<u>2nde étape</u>:
En fait $x_1 = 0$; $x_2 = 0$.

<u>3ème étape</u>: 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.
Dc $a = a'$.

Détails

1ère étape :

k corps ; v valuation discrète, égale car.
$\alpha \in H^\circ(k)$.

On dit que α est hol. en v si :
$\hat{k}_v$ complété ; $\tilde{k}_v$ corps résiduel.
$\alpha_v \in H^\circ(\tilde{k}_v) \subset H^\circ(\hat{k}_v)$.

On définit alors le résidu de α en v :
$\alpha_v \in H^i(\hat{k}_v) \xrightarrow{\text{res}} H^{i-1}(\tilde{k}_v)$.

Axiome (2) $\Rightarrow$ si W 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 W.

Autre méthode (qui n'utilise pas axiome (2)).

$k_0 \infty$.
$\mathbb{A}^2 \quad X, Y \xmapsto{\sigma_{\lambda,\mu}} \lambda^2 X, \mu^2 Y \quad \lambda, \mu \in k_0^*$.
le torseur est inv. par $\sigma_{\lambda,\mu}$.
Dc $\quad a(T)$ ________________ :
{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.

le 08.11.93

2nde étape

$$a(T) = x_0 + x_1(X) + x_2(Y) + x_3(X)(Y).$$

mq $x_1 = x_2 = 0$.

On peut supposer $a_0 = 0$, i.e. a normalisé.

$$\begin{tikzcd} h(X^{1/2}, Y) \arrow[d, dash] & 0 \\ h(X,Y) & a(T) \arrow[u] \end{tikzcd}$$

(Ajouter Γ tsz l'alg. de quaternions).

Mais l'image de $a(T)$ est $x_2(Y)$.

Dc $x_2(Y) = 0$ ds $h(X^{1/2}, Y)$.

Par le résidu, on a déduit $x_2 = 0$.

3ème étape : $a(T) = 0 \Rightarrow a = 0$.

(spécialisation).

Soit $T_{\alpha,\beta}$ alg. de quat. sur un corps $h \supset h_0$ déf. par $\alpha, \beta \in h^*$.

$a(T_{\alpha,\beta}) \overset{?}{=} 0$.

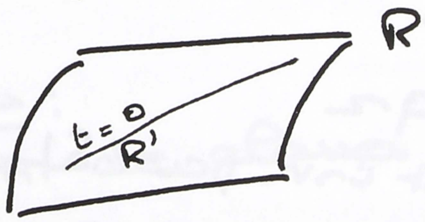
$h_1 = h(X,Y)$ $\quad T_{X,Y}$ sur h_1.

$a(T_{X,Y}) = 0$ car $a(T) = 0$.

Lemme: Soit R une alg. locale régulière sur k_0, de corps résiduel k. Soit U un G torseur sur $\mathrm{Spec}(R)$. $K = \mathrm{Fr}(R)$. U_k, U_K les torseurs correspondant. 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 avd. o.p.s. R complets, et K
et axiome (2) s'applique.
$a(U_k)=a(U_K)=0$.

Cas g^{al}: récurrence.



$t \in \mathfrak{m} - \mathfrak{m}^2$

K' = corps des fct^{ons} sur $R' = R/tR$
$a(U_{K'})=0$ par spécialisat^{o} $K \to K'$.
Puis (hyp. de réc.): id. sur k.

N.B.: En fait, on pourrait faire cela sans l'axiome (2).

<u>Un procédé de construction d'inv. cohom. pour G qcqve:</u>

$G \hookrightarrow H = SL_N$ N convenable

$X = H/G$ esp. hom.

$x \in H^i_{et}(X, C)$ C coef.

T torseur sous G déf./k.

Il est obtenu à partir d'un pt k rat.

$x \in X$, défini à conj. près par l'acté de $SL_N(k)$.

$\varphi_x : \operatorname{Spec} k \to X$.

$a_x(T) = \varphi_x^*(u)$.

<u>Thm</u>: cette classe de cohom. est indpdte de x.

(Il suffit de voir que $u_k \in H_{et}(X/k, C)$ est inv. par $SL_N(k)$.

<u>Preuve</u>: Quitte à lui ajouter une ind., ops k ∞.

ks clôture sép. $H^0(X/k_s, C)$.

Γ_k opère:

$$H^\bullet(\Gamma_k, \underbrace{H^\bullet(X/k_s, C)}_{\text{gpes finis.}}) \Rightarrow H^\bullet_{et}(X, C).$$

L'action de $SL_N(k)$ dessus est triviale.

<u>Lemme</u>: Soit $0 = A_0 \subset A_1 \ldots \subset A_n = A$ une filtration d'un gpe ab. A.
Les aut. de A qui respectent la filtration, et agissent trivialement sur $gr A = \bigoplus A_i / A_{i-1}$ est un gpe nilpotent.

Or l'image de $SL_N(K)$ ds $\mathrm{Aut}(H^i_{et}(X, C))$ est un gpe nilpotent.
$\Rightarrow$ action $SL_N(k)$ triviale.

Les axiomes st faciles à vérifier.

<u>Alors</u>:
Partir de classes de col. ds $H^{\bullet}_{et}(X, C)$.
↳ exple
$u \in H^3_{et}(X, \mu_5^{\otimes 2})$. $G = E_8 \hookrightarrow SL_{248}$
$\to$ cl. fondamentale de $H^3(SL_N)$.
déf. op. cohom. à val. dans $H^3(k, \mu_5^{\otimes 2})$.
(?) $a \neq 0$.

Retour sur le dernier cours.

Exple concret de constructº d'invariant.

$G = G_2 \subset SL_7 = S$

$G = E_8 \subset SL_{248} = S$

On se place sur le <u>corps $\mathbb{C}$</u>

$X = S/G$.

$\pi_1 = \pi_2 = 0$; $\begin{cases} \pi_3(G) \cong \mathbb{Z} \\ \pi_3(S) \simeq \mathbb{Z}. \end{cases}$

Dc $\begin{cases} \mathbb{Z} \to \mathbb{Z} \to \pi_3(X) \to 0 \\ \pi_1(X) = \pi_2(X) = 0. \end{cases}$

$\pi_3(X) = \mathbb{Z}/d\mathbb{Z}$ (on peut montrer facilement $d \neq 0$).

<u>1er cas</u>: $d = 2$.

<u>2nd cas</u>: sauf erreur, $d = 60 = 2h$
$\uparrow$
nbre de Coxeter de E_8.

Dc <u>pour G_2</u> on calcule mod. 2
$H^3(X, \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$.

<u>pour E_8</u> $60 = 4 \times 3 \times 5$ $H^3(X, \mathbb{Z}/4\mathbb{Z})$ cycl. d'ordre 4
$-(\ , \mathbb{Z}/3\mathbb{Z})$ 3
$-(\ , \mathbb{Z}/5\mathbb{Z})$ 5

Prenons pour $k = k(V)$, V variété complexe
Quitte à restreindre V, u G torseur
sur k $\Leftrightarrow$ G fibré principal sur V
qui devient trivial sur S.
ce fibré provient d'une flèche $V \xrightarrow{f} X$ $\overset{S/G}{\shortparallel}$
$u \in H^3(X, \mathbb{Z}/d\mathbb{Z})$
On attache au fibré
$f^* u \in H^3(V, \mathbb{Z}/d\mathbb{Z}) \longrightarrow H^3(k, \mathbb{Z}/d\mathbb{Z})$.

<u>Cas G_2</u> : On retrouve l'invariant
d'Arason défini la dernière fois.
(Comment le prouver ??).
[En prenant $V = \mathrm{Aff}^3$ − plans coord.
i.e. $\{(x_1, x_2, x_3) \quad x_i \neq 0\}$.
Torseur versel pour G_2
$\Leftrightarrow$ octonions avec $e_i^2 = x_i \quad i = 1, 2, 3$.
$V = G_m^3 \xrightarrow{f} X$
(f obtenue à partir de

$$\begin{tikzcd} G_m^3 \arrow[r] \arrow[d, "2"] & S \arrow[d] \\ G_m^3 \arrow[r] & X \end{tikzcd}$$

).

$S_1 \times S_1 \times S_1 \longrightarrow X$.
Il faudrait mq la classe de
cohom. ds X donne bien la classe
fond. dans $S_1 \times S_1 \times S_1$].

<u>Autre complément</u> :
On a déf. des inv. cohom.
G-torseur $\longmapsto$ coh. $H^i(k, C)$.
On peut aussi regarder des invariants
G-torseur $\longmapsto$ | gpe de Witt de k
| $K_i(k)/mK_i(k)$.

Pour <u>gpe de Witt</u> : on suppose car $k \neq 2$.

W_k anneau de Witt
= classes de f.q. (f. hyp. $\to 0$
i.e. $\langle 1,-1\rangle = 0$ ds W_k).

Parfois, on travaille sur le groupe
de Witt-Grothendieck GrW_k

$\left.\begin{array}{l}\text{diagramme}\\ \text{cartésien}\end{array}\right.$
$$\begin{array}{ccc} GrW_k & \longrightarrow & \mathbb{Z} \\ \downarrow & \square & \downarrow \\ W_k & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \end{array}$$
$\{(n,q)$
$n \equiv \deg q \bmod. 2\}$.

Plus tard, nous regarderons les λ opérateurs.
Or elles ne st pas définies sur W_k.
Par contre, elles le st sur GrW_k.

"<u>Bonne réduction</u>" : Si k complet, val. dis.,
corps résiduel $\tilde{k}$ de car $\neq 2$,
On a
$$0 \to GrW\tilde{k} \to GrW_k \xrightarrow{\partial_\pi} W_{\tilde{k}} \to 0.$$
$\langle x_1, \dots, x_n\rangle \longmapsto \langle \bar{x}_1, \dots, \bar{x}_n\rangle$.
$\bar{x}_i \in$ anneau de val., associé à x_i

vu cô gpe additif.

On peut choisir n'importe quel relèvement $\alpha_i \to \bar{\alpha}_i$.
Par contre, ∂_π dpd du choix de l'uniformisante :
$q = \langle \alpha_1, \dots, \alpha_n, \pi\beta_1, \dots, \pi\beta_m \rangle$ π unif. α_i, β_j unités.

$\downarrow$

$\langle \tilde{\beta}_1, \dots, \tilde{\beta}_n \rangle = \partial_\pi q$.

[Elle est bien à valeurs ds $W\tilde{h}$, car
$q = \langle \pi\alpha, -\pi\alpha \rangle$ $\partial_\pi q = \langle \tilde{\alpha}, -\tilde{\alpha} \rangle$.
Or $q \simeq \langle 1, -1 \rangle$. Dc il faut que $\langle \tilde{\alpha}, -\tilde{\alpha} \rangle$ soit nul.].

On peut définir un résidu qui ne dpde pas du choix d'une unif. :
$V = m/m^2$. V^* est un $\tilde{h}^*$-torseur.
Or $\tilde{h}^*$ opère sur $W\tilde{h}$. Dc on peut tordre $W\tilde{h}$ par le torseur en question.
Ls fournit un opérateur à val. ds $W\tilde{h}$.

Opération à val. ds GrW

c'est la donné pour tout G torseur T sur $h \supset h_0$ d'un élt $a(T) \in \mathrm{GrW}(h)$ avec les axiomes (1) et (2)

(1) $h \to h'$
(2) val. discrète d'égale car.

Travailler ds GrW est plus précis que coh. mod. 2 et permet d'utiliser les op. ∂.

le 15.11.98

(5)

<u>Exemple</u> : $G = G_2$ déployé.

G_2 torseur $\Longleftrightarrow$ alg. d'octonions.

$\Downarrow$

f. trace 3 forme de Pfister q.

Dc à H torseur T on peut associer $q_T := a(T$

<u>Thm.</u> Toute GrW opération sur les G_2 torseurs s'écrit de façon unique

$\boxed{T \longmapsto q_0 + q_1 \otimes a(T)}$,

avec $q_0, q_1 \in$ GrWho.

<u>Exple</u> (cf. cours précédents)

$T \mapsto$ forme de G_2 : G_2^T

Killing$(G_2^T) = b(T)$ de rg 14.

On a

$$\boxed{\text{Killing}(G_2^T) = \langle -1,-3\rangle \otimes (a(T) - \langle 1\rangle).}$$

ie. $q_0 = -\langle -1,-3\rangle$ et $q_1 = \langle -1,-3\rangle$.

<u>sur $\mathbb{R}$</u> f compacte $a(T) = \langle 1, \dots, 1\rangle = 8$.

La démonstration est essentiellement la m̂ que celle de la dernière fois :

On choisit $h = ho(X, Y, Z)$) T^{ver}/h.

Octonion $e_1^2 = X, \dots, e_3^2 = Z$

$a(T^{ver}) \in$ GrW h.

le 15.11.93

⑥

Cet élt a bonne réduction sur l'esp. affine à 3 dim. privé de $\left|\begin{array}{l} X=0 \\ Y=0 \\ Z=0 \end{array}\right.$.

(bonne réduction pour les val. d. attachée aux div. irréd.).

Puis, avec des suites exactes de Milnor :
Les élts de GrWh ayant bonne réductᵒ ont cô base
$\langle 1\rangle, \langle X\rangle, \langle Y\rangle, \langle Z\rangle, \langle XY\rangle, \ldots, \langle XYZ\rangle$.
Dc
$a(T^{ver}) = d_0 + d_1\langle X\rangle + d_2\langle Y\rangle + d_3\langle Z\rangle + d_4\langle XY\rangle + d_5\langle XZ\rangle + d_6\langle YZ\rangle + d_7\langle XYZ\rangle$

Ici, $d_0 = \langle 1, X, XY, \ldots, XYZ\rangle$.
Dc on veut mq ts les d st égaux (sf d_0).
En fait :
si l'on remplace X par -1, alors $a(T)$ devient hyperbolique, et ne dpd pas de Y et Z.
Dc $a(T) = d_0 + d_1\langle -1\rangle + d_2\langle Y\rangle + d_3\langle Z\rangle + d_4\langle -Y\rangle + d_5\langle -Z\rangle + d_6\langle YZ\rangle + d_7\langle -YZ\rangle$

donne :

<u>En fait</u> on travaille ds <u>Wh</u>

↳ $d_2 = d_4$
$d_3 = d_5$
$d_6 = d_7$ ....

Une fois qu'on a le cas universel, on spécialise.

Opérations sur les f.p. de Pfister $\longmapsto W, GrW$

p.ex.: Si q est une forme de Pfister

$d^i q = a \oplus b q$ $\left| \begin{array}{l} a, b \in \mathbb{Z} \\ a, b \text{ dpdt de } i \text{ et de } n \end{array} \right.$

Invariants $\left\{ \begin{array}{l} \text{cohom.} \\ \text{Witt} \end{array} \right.$ du groupe S_n.

Dictionnaire:

Torseurs sous S_n $\longleftrightarrow$ algèbres étales de deg. n

Si S est un schéma

X $\quad$ X fini, étale, partout de d^o n.

$\downarrow \pi$ $\quad$ ($\pi_* O_X$ est loc. libre de rg n) $\quad \Longleftrightarrow$ S_n torseurs sur S.

S

$\Longrightarrow$:

Si $X \to S$, on forme le produit

$X^n_S = X \times_S \dots \times_S X$ (n fois).

"fat diagonal"

Δ_n formé des pts ayant au moins deux coordonnées égales, $\Delta_n = \cup \Delta_{i,j}$

le 15.11.93

$T_X = X^n_S - \Delta n$.

S_n agit librement sur T_X.

T_X est bien un torseur : on le vérifie qd $X = S \amalg S \cup .. \amalg S$ (n fois).

$\underline{\Leftarrow}$: si T est un S_n torseur, 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 élt ; $S_I = \mathrm{Sym}(I)$

$X \longmapsto$ torseur sous S_I $\quad X^I - \Delta$.

on regarde $S \times I$

$\downarrow$

S

Cas des corps : si $S = \mathrm{Spec}\, k$

S_n torseur sur k $\iff$ k algèbre étale L de rg n.

$L = \prod k_i \quad k_i/k$ sép.

et $\Sigma [k_i : k] = n$.

---

k_0 corps de base.

C Γ_{k_0} module fini, d'ordre premier à la caract.

i.

Le 15.11.93

VI-9

Sn torseur sur $h \supset h_0$ $\longmapsto H^i(h, C)$.

i.e. $L \longmapsto a(L) \in H^i(h, C)$.

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 $L = h \times \cdots \times h$). 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 $L = L_1 \times \cdots \times L_m$ avec $\deg L_i = 1, 2$.

Récurrence sur le nbre r de fact. de deg. 2.

$r=0$ $\left.\begin{array}{l} L \cong h \times \cdots \times h \\ a \text{ normalisé} \end{array}\right\} \Rightarrow a(L)=0.$

On peut supposer $\begin{cases} L_1, \ldots, L_r \text{ de deg. } 2 \\ L_i = h \quad i > r. \end{cases}$

On peut aussi supposer
que L_r est un corp. Sinon
hyp. de réc. marche.
Soit k' ce corps. $[k':k]=2$.
Soit
$L' = L_1 \times \cdots \times L_{r-1} \times \underbrace{k \times k} \times k \times \cdots \times k$

$2a(L')=0$, par hyp. de réc.

De plus L et L' deviennent isom.
après ext. des scalaires à k'. Donc
leurs invariants sur k' sont les m.
i.e.
$a(L)-a(L')$ est tuée par l'ext. k'/k.
Mais k'/k de degré 2.
Donc (argument de cores. habituel:
Cor $(a(L)/_{k'} - a(L')/_{k'}) = 0$)
$2(a(L)-a(L'))=0$.
Donc $2a(L) = 2a(L') = 0$.

cqfd

La dém. du thm 1 utilise l'algèbre verselle. Récurrence sur n.

Cas versel: n degré fixé

$k = k_0(A_1, \ldots, A_n)$ A_i n indéterminées.

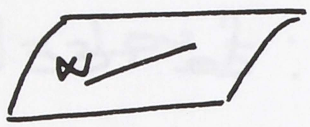
$L^{ver} = k[X]/_{P_n(X)}$. $P_n = X^n + A_1X^{n-1} + \cdots + A_n$

L^{ver} est étale de rg n.
(C'est $\simeq$ un corps).

Regardons $a(L^{ver}) \in H^i(k, C)$.

<u>Assertion</u> : la classe a n'a pas de pôles sur Aff^n.

W div. irred. ds Aff^n.



On veut mq $a(L^{vers})$ n'a pas de pôles en W.

Mais P_n définit une algèbre

$R = k_0[A_1, \dots, A_n, X] / (P_n)$.

Si $S = k_0[A_1, \dots, A_n] =$ alg. affine de Aff^n.

R est une S alg. libre de base $1, X, \dots, X^{n-1}$

$\Updownarrow$

n revêtement ramifié $\quad X_n \to Aff^n$.

Si Δ est le pol. discriminant, $\Delta(A_1, \dots, A_n)$,

$\boxed{X_n \text{ est non ramifié en dehors de } \Delta = 0.}$

$\begin{cases} \Delta \text{ est irred. en car} \neq 2 \\ \Delta \text{ est le carré d'un pol. irred. en car } 2. \end{cases}$

Dc $a(L^{vers})$ n'a pas de pôles en W se décompose en

$\begin{cases} (1) \text{ pas de pôles si } W \neq (\Delta = 0). \\ (2) \text{ ——————— } W = (\Delta = 0). \end{cases}$

(1) est une conséquence de l'axiome
(2) des invariants cohomologiques.
Pour montrer (2), on va utiliser l'hyp. $a(L) = 0$ si L est produit d'alg. de dim. ≤ 2.
Donc on peut supposer thm 1 vrai en deg. $< n$.

<u>Prop.</u>: Soit $k \supset k_0$ muni d'une val. disc. triviale sur k_0, et complet. (corps résiduel $\tilde{k}$).
Soit $\varphi : \Gamma_k \to S_n$ un hom.
Soit $I \subset \Gamma_k$ le gpe d'inertie.
Supposons que $\varphi(I)$ soit un ss 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.

<u>Preuve</u>: Faisons opérer Γ_k sur $[1, \dots, n]$ grâce à φ. L'image de I opère en fixant $n-2$ pts de $[1, n]$ et en permutant les deux autres. (disons 1, 2).
I est normal ds Γ_k. Donc cette déc. de $[1, n] = [1, 2] \cup [3, n]$ est stable par Γ_k.
D'où $L_\varphi = L_2 \times L_{n-2}$ avec rg $L_i = i$.
Donc $a(L_\varphi) = 0$, par le lemme qui suit.

Le 15.11.93

(13)

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 une opérat° cohom. b sur les algèbres étales sur les ext. de k de degré n'' par :

si Π est une telle algèbre, sur $k' \supset k$

$b(\Pi) = a(L'/_{k'} \times \Pi)$.

b a la propriété de s'annuler sur les algèbres décomposables en alg. de d° ≤ 2 ...

Par hyp. de réc., ceci $\Rightarrow b = 0$.

D'où le lemme avec $\Pi = L''$.

Regardons Aff^n. S_n opère en permutant les coordonnées.

$\forall\ (1 \leq i < j \leq n$ $\quad D_{ij}$ diag. $x_i = x_j$.

$D = \cup D_{ij}$

S_n opère librement sur $\mathrm{Aff}^n - D$.

$$\begin{array}{ccc} D \subset & \mathrm{Aff}^n & \\ \downarrow & \downarrow & \text{quotient par } S_n \\ \Delta = 0 & \mathrm{Aff}^n & \end{array}$$

X_i variables "en haut".
A_i ——— "en bas".

$X_1 + A_1 X^{n-1} \ldots = \Pi (X - X_i)$

i.e. $-A_1 = \Sigma X_i$

$\ldots$

$$\Delta = \prod_{i<j} (X_i - X_j)^2.$$

Dc $\Delta=0$ est clairement irred.
Pour gpe d'inertie :
On relève Δ en $D_{1,2}$
Gpe d'inertie = ss gpe de S_n fixant D_{12}
$= \{1, (1,2)\}$.

Le résultat précédent s'applique :
a n'a pas de pôle en $\Delta=0$.
(Le lemme précédent s'applique au complété de $k_0(A_1,\dots,A_n)$ pour la val. définie par Δ).

On a donc démontré que $a(L^{ver}) \in H^i(k_0(A_1,\dots,A_n), C)$ n'a pas de pôles. Dc il $\in$ aussi que "cst" $H^i(k_0, C)$. Notons α cet élt de $H^i(k_0, C)$.
Reste à mq $\begin{cases} \alpha=0 \\ \forall L \ a(L)=0. \end{cases}$

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 $a - \alpha$.
Arguments de spécialisations...
(Déjà fait).

Prenons $h = h_0$.
Supposons tt d'abord $|h_0| \geq n$.
Prenons $h = h_0$ et $P = \prod_{i=1}^{n} (X - \lambda_i)$
$\lambda_i \in h_0$, $\lambda_i \neq$

$L_P = h \times h \times \cdots \times h$.
$a(L_P) \underset{hyp}{=} 0 = \alpha$. Dc $\alpha = 0$.

Sinon, $\hat{\imath}$ argument appliqué à $h_0(U)$ (U indéterminée), en utilisant colom. Cq colom.

Ainsi a s'annule sur toutes les alg. étales qui possèdent un gén.
("Générateur d'une h alg. étale L: c'est un $x \in L$ tq $1, x, \ldots, x^{n-1}$ base de L)

$\begin{cases} \text{Si } h \ \infty : \text{ tte alg. étale a un gén.} \\ \text{Si } |h| \geq n : \text{ ————— de rg } n \text{ —————} \end{cases}$

Si $h \ \infty$, tte alg. étale $\simeq L_P$. OK.
Sinon, on remplace h par $h(U)$.

<u>Explication</u> : de $k\infty$

Thm alg. ét. a un gén.

$\boxed{\begin{array}{l}L \text{ étale de rg } n/k. \\ \exists \text{ un nbre fini de } k \text{ sev de } L\text{, de} \\ \text{codim} \geq 1 \quad V_j \text{ tels que tt élt} \\ x \in L - \cup V_j \text{ soit un générateur.}\end{array}}$

base $(e_1, \dots, e_n)$ de L.

$x = x_1 e_1 + \dots + x_n e_n \quad x_i \in k$.

x^k comb. des e_i à coeff. pol. $(x_1, \dots, x_n)$.

$x^i = \sum_j a_{ij}(x) e_j \quad a_{ij}(x_1, \dots, x_n)$ pol.

$\det(a_{ij}(x)) = R(x)$

R n'est pas identiquemt nul.

(chgt de base : il suffit de le vérifier pour $L = k \times \dots \times k$, et $e_i = (0, \dots, 0, 1, 0, \dots, 0)$.

Ds ce cas $x^i = (x_1^i, \dots, x_n^i)$ et

$R(x) = \prod_{i > j} (x_i - x_j)$ (= VdM).

$$\begin{tikzcd} L \arrow[r, "\varphi_1, \dots, \varphi_n"] \arrow[d, dash] & \bar{k} \\ k & \end{tikzcd}$$

$\cup V = \{x \text{ tq } \exists i \neq j$ avec $\varphi_j(x) = \varphi_i(x)\}$.

Cas des corps fini :

k fini à q élts.

Si $n \geq q$ l'alg. déc. $k \times \cdots \times k$ de q^n

n'a pas de générateurs.

($x = (x_1, \ldots, x_n)$ 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 différente, ...)

il est commode de supposer $\mathcal{O}_F = \mathbb{Z}[x]$.

Ce n'est pas tjrs vrai.

En fait, ce n'est pas vrai ma[?] plus localement, à cause de ce qui précède

(Les fact. excep. des disc.).

$\Rightarrow$ Il faut localiser a[?] faut,

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 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 : $\boxed{\text{Si } q \geq n,\ L \text{ a un générateur. (Si } q < n, \text{ l'algèbre déployée } k \times \cdots \times k \text{ de rg } n \text{ n'a pas de générateurs).}}$

Preuve du thm :

Notons $m(q,d)$ = nbre de polynômes unitaires irreductibles de degré d sur $k = \mathbb{F}_q$.

Lemme : $\boxed{m(q,d) \geq q/d}$

Admettons le lemme pour l'instant.
Décomposons $L = \prod (\mathbb{F}_{q^d})^{n_d}$.
$n = \sum d n_d$. Donc $n_d \leq n/d \leq q/d$.
Grâce au lemme, il existe donc des polynômes $P_{d,1}$; .. ; P_{d,n_d} irred. unitaires distincts de degré d.

Posons $P = \prod_{d,i} P_{d,i}$. Il est unitaire, sans facteurs carrés, et $L \simeq k[X]/(P(X))$.

Preuve du lemme :

$k_d = \mathbb{F}_{q^d}$. $[k_d : k] = d$.
Il existe un générateur $x \in k_d$.
$k_d = k[x] \to$ fournit un polynôme P irred. de degré d. (polynôme minimal (x))
Alors $\lambda \in k$ $P_\lambda := P(X+\lambda)$.
P_λ est aussi irred. unitaire de degré d.
λ fixé. le nbre de ν tq $P_\lambda = P_\nu$ $\leq d$.
[$x+\lambda$ et $x+\nu$ st conjugués si $P_\lambda = P_\nu$].
Ceci fournit un nombre de polynômes $\geq q/d$.

Revenons aux nbres $m(q,d)$

(1) $\boxed{q^n = \sum_{d|n} d\, m(q,d).}$

$x \in k_{q^n} \mapsto$ pol. min. de x. Il est irred. de degré $d|n$.

(2) $$\boxed{\frac{1}{1-qt} = \prod_{d=1}^{\infty} \frac{1}{(1-t^d)^{m(q,d)}} = \prod_{\substack{P \text{ unit.} \\ \text{irred}}} \frac{1}{1-t^{\deg P}}}$$

C'est l'écriture habituelle de la fct° zêta de la dte affine.
$\prod$ = produit eulérien.

Le 22.11.93

$X = \mathbb{A}\mathrm{ff}^1 / \mathbb{F}_q$; $Z_X(t) = $ zêta de X.

(3) Moebius :

$$\boxed{m(q,n) = \frac{1}{n} \sum_{d|n} \mu(d)\, q^{n/d}}$$

$m(q,1) = q$

$m(q,2) = \frac{1}{2}(q^2 - q)$

$m(q,3) = \frac{1}{3}(q^3 - q)$

La formule (2) intervient dans la théorie des alg. de Lie libres :

$/\mathbb{Q}$; $q \geq 1$.

On peut définir l'algèbre de Lie libre en $x_1, \dots, x_q$. C'est une alg. graduée

Notons $Lie = Lie(x_1, \dots, x_q)$.

Appelons $M(q,d)$ la dim. de $Lie(x_1, \dots, x_q)^d$.

[$d = 1$ $x_1, \dots, x_q$ $M = q$

$d = 2$ $[x_i, x_j]$ $i < j$ $M = \frac{q^2 - q}{2}$].

Thm : $\boxed{M(q,d) = m(q,d)}$.

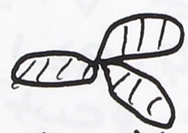
Dém : On regarde l'algèbre envelop-pante de Lie : $U Lie$ = alg. associative libre en $x_1, \dots, x_q$. Sa série de Poincaré est $1/1 - qt$.

Mais $gr\, U Lie = Sym\, Lie$ et sous cette forme, la série de Poincaré est $\prod \frac{1}{(1-t^d)^{M(q,d)}}$.

ce qui démontre le thm.

Ceci permet également de redémontrer $m(q,d) \geq q/d$:

$[x_1, [x_1, [\cdots [x_1, x_2] \cdots]$ permet de prouver l'existence d'au moins un polynôme irreductible de degré d.
En fait, leur nbre est $\geq q-1$.
(Remplacer x_2 par $x_3, \cdots, x_q$).

La formule (2) intervient aussi en topologie :
r impair ≥ 3
$X = S_r \vee \cdots \vee S_r$ (q copies)
(bouquet de sphères ).
ΩX espace des lacets de X.
La série de Poincaré de ΩX est $\dfrac{1}{1-qt^{r-1}}$
$H^*(\Omega X, \mathbb{Q})$ algèbre de polynômes en des variables de degré $(r-1)d$, en nombre $N(q,d)$.

Thm : $\boxed{N(q,d) = m(q,d) = \frac{1}{d}\sum_{d'|d} \mu(d') q^{d/d'}}$.

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
Rang $\pi_{d(r-1)+1}(X) = m(q,d)$
Rang $\pi_i = 0$ si $i \not\equiv 1 \bmod.(r-1)$.

Invariants cohom. des alg. étales.

k_0 corps de base.
C module fini sur Γ_{k_0}; $(|C|, \mathrm{car}\, k_0) = 1$.
$n \geq 1$ rg des alg. étales.
L/k
$k \supset k_0$ $\quad L \longmapsto a(L) \in H^{\cdot\cdot\cdot}(k, C)$.

On a montré qu'un invariant cohom. qui est nul sur les alg. $L = \prod L_i$ avec $\mathrm{rg}\, L_i \leq 2$ est nul.

On commence par s'intéresser au cas où $C = \mathbb{Z}/2\mathbb{Z}$ (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 $\varphi_L : \Gamma_k \longrightarrow S_n$
déf. à conj. près.

Dc on peut définir $a_x(L) = \varphi_L^*(x)$.
C'est un inv. cohom.
Dc
tt $x \in H^\bullet(S_n) \rightsquigarrow$ inv. cohom. a_x.

Classes de Stiefel-Whitney:
ce st des $w_i \in H^i(S_n)$ définis de la façon suivante:

$S_n \hookrightarrow O_n$ gpe orthogonal.
Dc $BS_n \longrightarrow BO_n$
et $H^\bullet(BO_n) \longrightarrow H^\bullet(BS_n) = H^\bullet(S_n)$
$\quad\ \wr\!\wr$
$\mathbb{F}_2[w_1, \dots, w_n] \rightsquigarrow w_1, \dots, w_n \in H^\bullet(S_n)$.

$w_1 \in H^1(S_n) = \mathrm{Hom}(S_n, \mathbb{Z}/2\mathbb{Z})$: signature.
$w_2 \in H^2(S_n)$ correspond à une extension
$\tilde{S}_n$ de S_n par $\mathbb{Z}/2\mathbb{Z}$.

On notera l'invariant correspondant
$a_{w_i}(L) = w_i(L)^{gal}$

2^{nd} exple d'invariants.

$L \longmapsto q_L$ f.q. de rg n
$x \longmapsto \mathrm{Tr}_{L/K}(x^2)$.

Mais $q \longmapsto w_i(q) \in H^i(k)$
Si $q = \langle \alpha_1, \dots, \alpha_n \rangle$ $\quad w_i(q) = \sum_{j_1 < \dots < j_i} (\alpha_{j_1}) \dots (\alpha_{j_i})$.

où (α) est l'élt de $H^1(k)$ correspondant à $\alpha \in K^*$.

On notera l'invariant correspondant
$w_i(L) = w_i(q_L)$.

Thm 1 : $\boxed{w_i(L)^{gal} = 0 \text{ si } i > [\tfrac{n}{2}]}$

Thm 2 : B. Kahn Inv. M 1984
$w_i(L)^{gal} = w_i(L)$ si i impair
$w_i(L)^{gal} = w_i(L) + (2) w_{i-1}(L)$ si i pair.

$(2) \in H^1(k)$

$(2) = 0$ si et seulement si 2 est un carré ds k.

Grâce au thm qui précède, o.p.s.

$L = \prod L_i$ avec $\operatorname{rg} L_i \leq 2$.

$\varphi_L : \Gamma_k \to S_n$.

Appelons H_n le ss gpe de S_n de type $(2, \dots, 2)$ formé des permutations qui laissent stables $\{1,2\}; \{3,4\}; \dots$

$$\begin{array}{l} L = \prod L_i \\ \operatorname{rg} L_i \leq 2 \end{array} \iff \begin{tikzcd} \Gamma_k \arrow[r, "\varphi_L"] \arrow[dr] & S_n \\ & H_n \arrow[u] \end{tikzcd}$$

Mais

$$\begin{array}{ccc} S_n & \hookrightarrow & O_n \\ \cup & & \\ H_n & \hookrightarrow & O_m \end{array} \qquad m = \left[\frac{n}{2}\right]$$

$$\left(s \in O_m \mapsto \left(\begin{array}{c|c} s & 0 \\ \hline 0 & 1_{\cdot\cdot\cdot 1} \end{array}\right)\right).$$

Mais O_m n'a plus de classes de Stiefel Whitney au delà de la dim. m.

Dc $w_i(L)^{gal} = 0$ si $i > \left[\frac{n}{2}\right]$.

<u>Pour le 2^nd thm :</u>

① Le thm est vrai si $n = 2$: ($n = 1$ évident)

$L = k[x]/(x^2 - \alpha)$ $\quad \alpha = \operatorname{disc} L$

$w_1^{gal} = (\alpha)$; $w_2^{gal} = 0$.

Forme trace : Ds la base $(1, \sqrt{\alpha})$, on obtient $q_L = \langle 2, 2\alpha \rangle$

Dc $w_1(L) = (4\alpha) = (\alpha) = w_1^{gal}(L)$

$w_2(L) = (2)(2\alpha) = (2)(2) + (2)(\alpha)$

Mais $(2)(2) = (-1)(2) = 0$.

et $w_2^{gal}(L) = 0 = w_2(L) + (2)(K)$

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.

Mais $\begin{cases} \text{on sait multiplier les Stiefel Whitney} \\ \text{forme trace} = \oplus \text{ formes traces.} \end{cases}$

↳ on va m.q. les deux membres sont multiplicatifs.

$w = \sum w_i \in H^*(k) = \oplus H^i(k)$.
$= w_{pair} + w_{impair} \quad (= w_+ + w_-)$.

On veut montrer que $\boxed{w_{gal} = w + (2) w_-}$

Mais :

1) $w^{gal}(L \times L') = w^{gal}(L) \cdot w^{gal}(L')$
(clair : multiplicativité).

2) $w(q_1 \oplus q_2) = w(q_1) w(q_2)$
& $w(L \times L') + (2) w_-(L \times L')$
$= w w' + (2)(w_+ w'_- + w_- w'_+)$
$= w w' + (2)(w w'_- + w' w_-)$
$= (w + (2) w_-)(w' + (2) w'_-)$
car $(2) w_- (2) w'_- = 0$ vu que $(2)(2) = 0$.

cqfd

Rque : On peut refaire tout ça en remplaçant S_n par un groupe de Weyl d'un système de racines. (Du moins si k_0 est de car 0).

Notons le W. $n = \mathrm{rg}\, W$.

Repr. naturelle sur $\mathbb{Q}^n$ engendré par des réflexions.

H_n est remplacé par des sous groupes de type $(2,2,\dots,2)$ obtenus ainsi:

On considère des hyperplans radiciels 2 à 2 orthogonaux.

Le ss gpe de Weyl engendré par les symétries par rapport à un hyperplan.

Les inv. colom. seront détectés par ces sous groupes de type $(2,\dots,2)$.

$[\mathrm{Aff}^n/W \simeq \mathrm{Aff}^n]$

Est-ce encore vrai en car p?

<u>Détermination explicite des inv. colom. des alg. étales de rg $n = \begin{cases} 2m \\ 2m+1 \end{cases}$</u>

<u>Thm</u>: $\boxed{\text{Les inv. colom. pour } S_n \text{ et } S_{n+1} \text{ st les mêmes si } n \text{ est pair.}}$

(Vrai pour la colom. ds C, pas uniquement modulo 2).

<u>Plus précisément</u>. $H \subset G$

Res: inv. col. de $G \to$ inv. col. de H

Cor: ——— $H \to$ ——— G

Res o Cor = indice de H ds G

($\varphi : \Gamma_k \to G \rightsquigarrow a(\varphi) \in H^0(k, C)$
Mais $\varphi : \Gamma_k \to H \hookrightarrow G$ ...).

Thm : $\boxed{\text{Res : inv. coh. de } S_{n+1} \to \text{inv. coh. de } S_n \text{ est un isomorphisme si } n \text{ est pair.}}$

Dém : Il suffit de le voir pour les invariants normalisés. $2.\text{inv.} = 0$.
Or $[S_{n+1} : S_n] = n+1 \equiv 1 \bmod. 2$.
Donc Res $\circ$ Cor est l'identité sur les inv. normalisé
$\rightsquigarrow$ Res est surjectif.

Res est aussi injectif. En effet si a inv. coh. de S_{n+1} tq Res $a = 0$, on a $a(L) = 0$ pour $L = L_n \times k$ rg $L_n = n$
Mais cô $n+1$ est impair, si $L = \prod L_i$ avec rg $L_i \leq 2$, on peut forcément écrire $L = L_n \times k$.
Ceci suffit à prouver que a est nul.

[Lien avec thm de Mestre:
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 : $\boxed{\text{Les inv. cohom. des algèbres étales de rang } n \text{ sur des extensions de } k_0 \text{ forment un } H^\circ(k_0) \text{ module libre de base } 1, w_1^{gal}, \dots, w_m^{gal} \quad m = [\tfrac{n}{2}].}$

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. cohom. de H_n

Pour C_2 : Les inv. cohom. forment un mod. libre de rang 2, de base 1, "(x)".
L'Algèbre étale donnée par $x \in k^\circ/k^{\circ 2}$
$\mapsto (x) \in H^1(k)$.
On a montré que tout invariant est de la forme $L \mapsto \lambda_0 + \lambda_1 (x)$. $\lambda_i \in H^\circ(k_0)$

$\varphi : \Gamma_k \to H_n$.
Une alg. galoisienne à groupe $H_n = C_2 \times \dots \times C_2$ est définie par m élts $\alpha_1, \dots, \alpha_m \in k^\circ/k^{\circ 2}$.
$\mapsto (\alpha_i) \in H^1(k) \quad x_i(\varphi) \quad i = 1, \dots, m)$.

Thm : $\boxed{\text{Les inv. cohom. mod. 2 des } H_n \text{ torseurs ont pour base les cup produits } x_{j_1} \cdots x_{j_c}(\varphi) \text{ avec } j_1 < \dots < j_c}$

le 22.11.93

VII-12

($m=2$: $1, x_1, x_2, x_1x_2$).

<u>Preuve</u> (m̂ dém. que précédemment).

$h = h_0(X_1, \ldots, X_m)$

φ^{univ} correspondant à $x_i = X_i$

$a(\varphi^{\text{univ}}) \in H^\circ(h)$.

Pas de pôles en dehors des $X_i = 0$.

D'où l'écriture voulue.

Par spécialisation, on démontre le thm.

$I \subset [1, \ldots, m]$ $\quad I = \{i_1, \ldots, i_\ell\}$ $i_1 < \cdots < i_\ell$.

$x_I(\varphi) = \prod_{k=1}^{\ell} x_{i_k}(\varphi)$.

Les x_I forment une base des inv. colom.

Si a est un inv. col. de S_n

$a_{/H_n} = \sum \lambda_I x_I$ $\quad \lambda_I \in H^\circ(h_0)$.

Le gpe sym. S_m opère sur H_n,

i.e. on a $\quad H_n \subset \underset{\text{normal}}{N} \subset S_n$ (permuter les paires)

$$N/H_n \simeq S_m$$

La restriction de a à H_n est invariante par l'action de S_m.

Donc $\lambda_I = \lambda_J$ si $|I| = |J|$.

D'où

$a_{/H_n} = \sum_{i=0}^{m} \lambda_i \left(\sum_{|I|=i} x_I \right)$.

Mais $\sum_{|I|=i} x_I = w_i^{\text{gal}}$.

Donc $a_{/H_n} = \sum_{i=0}^{m} \lambda_i w_i^{\text{gal}}$. $\square$

Cas général (C qcque).

Thm : $\boxed{\text{Tout invariant cohomologique normalisé s'écrit de façon unique sous la forme } \sum_{i=1}^{m} \lambda_i w_i \quad \lambda_i \in H^0(k_0, C(-i))_2}$

Explicat° :

$\lambda_i \in H^0(k_0, C(-i))_2$
signifie que $\lambda_i \in H^0(k_0, C(-i))$ et $2\lambda_i = 0$.

Si $nC = 0$ $n \wedge \operatorname{car} k_0 = 1$, $n \geq 1$.
$C(-i) \stackrel{\text{déf.}}{=} \operatorname{Hom}(\mu_n^{\otimes i}, C)$. (torsion à la Tate).

$$\left.\begin{array}{l} w_i \in H^i(k, \mathbb{Z}/2\mathbb{Z}) \\ \lambda_i \in H^i(k, C(-i)), 2\lambda_i = 0 \end{array}\right\} \overset{?}{\longrightarrow} \lambda_i w_i \in H^i(k, C)$$
"cup produit".

On peut supposer $n = 2^k$
si $x \in H^0(k, \mu_n^{\otimes i})$, alors $\lambda_i x$ (cup. prod.) a un sens dans $H^0(k, C)$.
Mais $C(-i) \otimes \mu_n^{\otimes i} \longrightarrow C$.

Lemme $\boxed{\text{(trivial) : } w_i \text{ est relevable dans } H^i(k, \mu_{2^k}^{\otimes i}) \text{ pour tt } k.}$

car :
1) Un élt de degré 1 est tjrs relevable
$x \in H^1(k, \mathbb{Z}/2\mathbb{Z}) = H^1(k, \mu_2)$ $x = (\gamma)$ $\gamma \in k^*$.
théorie de Kummer : le $\hat{\ }$ γ définit un élt de $H^i(k, \mu_{2^k}^{\otimes i})$.

2) cup produits et sommes d'élé^{ts} relevables st relevables.

3) Les x_i st C.L. de cup produits. (cf. formule de B. Kahn).

On choisit une classe $\tilde{x}_i \in H^i(h, \mu_{2^{k+1}}^{\otimes i})$

<u>Lemme</u>: $\boxed{\text{Si } \lambda \in H^0(h, C(-i)),\ 2\lambda = 0, \text{ alors } \lambda \tilde{x}_i \in H^0(h, C) \text{ ne dpd pas du choix de } \tilde{x}_i \text{ (mais seulem}^{t} \text{ de } x_i\text{)}.}$

C'est cet élé^t qu'on notera λx_i.

$$0 \to \mu_{2^k}^{\otimes i} \to \mu_{2^{k+1}}^{\otimes i} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

$$\tilde{x}_i \longmapsto x_i$$

$\tilde{x}_i$ est déterminé à l'addition près d'un $j(z)$, $z \in H^0(h, \mu_{2^k}^{\otimes i})$.

On $\lambda \tilde{x}_i$ ———————— $\lambda j(z)$.

Mais λz existe ds $H^0(h, C)$, et on peut voir que $\lambda j(z) = 2\lambda z = 0$ (car $2\lambda = 0$).

<u>cqfd</u>

<u>Thm</u>: $\boxed{\lambda_i \in H^0(h_0, C(-i)). \text{ tt inv. coh. normalisé est de la forme } \sum_{i=1}^{m} \lambda_i x_i.}$

On se ramène au gpe $H_n \simeq \underbrace{C_2 \times \cdots \times C_2}_{m}$.

Argument versel.

On est ramené à déterminer coh. gal. de C de $k_0(x_1, \dots, x_n)$ non ramifiée en dehors de $x_i = 0$.

$\uparrow$

Ecriture ! sous la forme $\sum_{I \subset [1,n]} \lambda_I x_I$

$\lambda_I \in H^0(k_0, C(-|I|))$.

x_I = cup produit des $x_j \in H^1(k, M_n)$, $j \in I$.

$2\lambda_I = 0$

$\lambda_I = \lambda_J$ si $|I| = |J|$ ...

(m̂ dém.).

<u>Inv. de les gpes de Witt :</u>

$L \longrightarrow a(L) \in \begin{cases} \mathrm{Gr}W k \\ W k \end{cases}$

Cas évident : la forme trace $L \longrightarrow q_L$.

et aussi : $\Lambda^i q_L \ \forall i \quad (0 \leq i \leq n)$.

<u>Thm</u> : $\boxed{\text{Tt invariant à val. de } Wk \text{ des alg. étales de rg } n \text{ s'écrit de façon uique } L \longmapsto \sum_{i=0}^{n} \lambda_i \Lambda^i q_L \quad \lambda_i \in Wk.}$

i.e. les $\Lambda^i q_L$ forment une base des invariants.

<u>Cor</u> : On a des formules pour $\Lambda^{n+1} q_L, \dots$

Quelques compléments sur les invariants cohomologiques usuels.

Thm : $\boxed{\begin{array}{l}\text{Soit } x \in H^i(S_n, \Gamma). \\ \text{On suppose } \begin{cases} i \geq 1 \\ \text{Act}^{\circ} \text{ de } S_n \text{ sur } \Gamma \text{ triviale.} \end{cases} \\ \text{Alors } 2x \text{ est négligeable.}\end{array}}$

Preuve :

o.p.s. Γ est de type fini, i.e. $\Gamma = \mathbb{Z}$ ou $\mathbb{Z}/m\mathbb{Z}$

De plus le cas $\mathbb{Z}$ se ramène à $\mathbb{Z}/m\mathbb{Z}$ car

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

$\begin{cases} H^i(G, \mathbb{Z}) \simeq H^{i-1}(G, \mathbb{Q}/\mathbb{Z}) \\ H^1(G, \mathbb{Z}) = 0 \end{cases}$ de torsion

---

En car 0

k; $\varphi : \Gamma_k \to S_n$ $\qquad \varphi^*(2x) \overset{?}{=} 0$

La classe de $2x$ définit une opération cohomologique sur les algèbres étales de rang n sur $k \supset k_0 = \mathbb{Q}$: $\varphi \mapsto \varphi^*(x)$.

Elle est normalisée, car $\varphi = 1 \Rightarrow \varphi^*(x) = 0$ (vu que $i \geq 1$).

Dc $2\varphi^*(x) = 0$.

Plus précisément :

$H = \underbrace{C_2 \times \cdots \times C_2}_{[\frac{n}{2}] \text{ termes}} \subset S_n$

H engendré par $(1,2)$; $(3,4)$; ...

<u>Thm</u> : $\boxed{\text{$x \in H^i(S_n, \Pi)$ est négligeable ssi sa restriction à H est nég.}}$

<u>Cas particulier</u> : $\Pi = \mathbb{Z}/2\mathbb{Z}$.

<u>Thm</u> : $\boxed{\text{$x \in H^i(S_n, \mathbb{Z}/2\mathbb{Z})$ est négligeable ssi sa restriction aux ss gpes d'ordre 2 de S_n est 0.}}$

=> est clair

<= Considérons $x_{|H} \in H^i(H, \mathbb{Z}/2\mathbb{Z})$
H de type $(2, 2, \ldots, 2)$.

On sait $H^\bullet(H) = \mathbb{F}_2[x_1, \ldots, x_N]$ $N = [\frac{n}{2}]$

Dc x est un polynôme en les x_i, qui est nul cô fct° 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 $x_j^q x_i - x_j x_i^q$.

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

$H^2(A_6, \mathbb{Z}/3\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$

$C_3 \times C_3$ $\quad u$ op. cohom. correspondant.

Thm : $\boxed{\text{Les inv. cohom. de } A_6 \text{ torseurs à coeff. mod. 3 sur } k_0 \text{ forment un } H^0(k_0, \mathbb{Z}/3\mathbb{Z}) \text{ module libre de base } \{1, u\}.}$

$\boxed{\text{Tout inv. cohom. de } A_6 \text{ mod. 5 normalisé est 0.}}$

Sylow $C_3 \times C_3$ ~~a~~ $\to u$

$C_5 \subset D_5$ normalisateur.

Mais : Inv. cohom. mod. 3 de A_9 ?
(le Sylow est plus compliqué).

On a vu que les inv. cohom. mod. 2 pour S_n ont pour base les classes
$w_i(q_L) = w_i \quad (0 \leq i \leq m \,;\, m = [\frac{n}{2}]$
ou bien w_i^{gal}.
On a vu aussi $w_i^{gal} = 0$ si $i > m$.

$$\begin{cases} w_i^q = w_i + (2) w_{i-1} & \text{si } i \text{ pair} \\ w_i^q = w_i & \text{si } i \text{ impair.} \end{cases}$$

On peut énoncer ce résultat autrement :
Si n est pair : $\boxed{w_i^q = w_i(2q_L)}$.

Rqe : Forme trace (du pt de vue torsion).

Forme standard $\langle 1, \dots, 1 \rangle$ $x_1^2 + \dots + x_n^2$.
$\varphi : \Gamma_k \longrightarrow S_n$.
L'act° 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 :

$w^q = \sum_i w_i^q$; $w = \sum_i w_i$. $\quad w_1 = (d)$.

On a $\boxed{w^q = w(1 + (2)(d))}$.

Pour le démontrer, on a besoin d'identités entre les classes de Stiefel-Whitney (J. Milnor ; Inv 10).

Ces identités st valables pour les w_i de f.q. qcques :
On écrit i sous forme dyadique
$i = \sum_{d \in I} 2^d$ $\quad I \subset \mathbb{N}$.

$\boxed{w_i = \prod_{d \in I} w_{2^d}}$ $\qquad$ expl : $w_7 = w_1 w_2 w_4$.

Alors si $i = \sum_{\lambda \in I} 2^\lambda$ $j = \sum_{\mu \in J} 2^\mu$

$\boxed{w_i w_j = u^r w_e}$ où $\begin{cases} u = (-1) \in H^1 \\ e = \sum_{\nu \in I \cup J} 2^\nu = i + j - r \end{cases}$

Exple : $w_7 = w_1 w_2 w_4$
$w_{10} = w_2 w_8$

$\rightarrow$ $w_7 w_{10} = w_1 w_2^2 w_4 w_8 = u^2 w_1 w_2 w_4 w_8$
$= u^2 w_{15}$

(Si $x \in H^i(k, \mathbb{Z}/2\mathbb{Z})$ est décomposable,
alors $x^2 = u^i x$).

Généralisation aux $\mathrm{Tr}(\alpha X^2)$

$n \left(\begin{array}{c} L \\ | \\ k \end{array} \right.$ $\alpha \in L^*$
$q_{L,\alpha}$ forme de rang n.
$w_i(q_{L,\alpha})$.

Mais on peut aussi associer des w_i^q,
car la donnée de (L, α) équivaut
à la donnée d'un torseur sous $S'_n = 2^n S_n$
(permutat^{os} et chgt de signe de n lettres)
$S'_n \subset O_n(\mathbb{R}) \rightarrow w_i \in H^i(S'_n)$.

Formule $\boxed{\begin{array}{l} \text{(B. Kahn)} \\ w^q = w(1+(2)(d)) \text{ où } d = \mathrm{disc}(L) \end{array}}$

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 thm sur les invariants à valeurs dans Wh.

Thm : $\boxed{\text{Ces invariants forment un } Wh_0\text{ module libre de base les } d^i(q),\ 0 \le i \le m, \text{ où } q \text{ est la forme trace.}}$ $m = [n/2]$.

Dém : Elle est presque identique à celle pour les invariants cohom.

1ère étape :

Soit a un tel invariant.

Thm : $\boxed{\text{Si } a \text{ est } 0 \text{ pour les alg. } L = \prod L_i \text{ avec } \mathrm{rg}(L_i) \le 2, \text{ alors il est } 0.}$

$h = h_0(A_1, \dots, A_n)$

L^{ve} déf. par $X^n + A_1 X^{n-1} + \dots + A_n$.

$a(L^{ver}) \in \mathcal{K}h = \underline{\mathcal{K}ho(A_1, \dots, A_n)}$

corps des fct^{os} sur $\mathbb{A}ff^n$.

On montre que a est non ramifié :

$\mathcal{K}$ irred. $\neq$ disc $= 0$: c'est axiome (2)

$\mathcal{K} =$ disc : L se décompose en $L_2 \times L_{n-2}$ sur le complété.

Un raisonnement par récurrence permet de conclure.

D'où $a(L^{ver}) \in \mathcal{K}ho$.

Par spécialisation, on en déduit $a = 0$.

<u>2nde étape</u> :

Supposons p.ex. $n = 2m$.

$L_1, \dots, L_m$ $\quad L_i = h[X]/(X^2 - x_i)$ $\quad x_i$ inv.

Cas versel : $h = ho(x_1, \dots, x_n)$ x_i ind.

$a(L^{ver}) \in \mathcal{K}h$ sans pôles en dehors des hyperplans $x_i = 0$.

<u>Prop.</u> : Les élé^{ts} de $\mathcal{K}h$ n'ayant pas de pôle en dehors des hyperplans $x_i = 0$ forment un $\mathcal{K}ho$ module libre de base $1, \langle x_1 \rangle, \dots, \langle x_n \rangle, \langle x_{i_1} \rangle \cdots \langle x_{i_m} \rangle, \dots$ $i_1 < \dots < i_m$.

$I \subset [1, m]$ $\quad x_I = \prod_{i \in I} x_i$ $\quad$ base : $\langle x_I \rangle$ $I \subset [1, m]$.

Dc $a(L^{v\sigma}) = \sum c_I \langle x_I \rangle$ $c_I \in W_{k_0}$.
C'est invariant par l'act° de S_n (qui permute les facteurs) : dc c_I ne dpd que de $|I|$.

$$a(L^{v\sigma}) = \sum_{i=0}^{m} c_i \left(\sum_{|I|=i} \langle x_I \rangle \right).$$

$L^{v\sigma} = \prod L_i \quad L_i = h(\sqrt{x_i})$.

$q_{L^{v\sigma}} = \oplus \langle 2, 2x_i \rangle$.

$2q_{L^{v\sigma}} = \oplus \langle 1, x_i \rangle = \langle \underbrace{1, \dots, 1}_{m} \rangle \oplus q'$

où $q' = \langle x_1, \dots, x_m \rangle$.

i.e. $2q = m + q'$.

Dc les $(\lambda^i q')_{0 \le i \le m}$ forment une base.

Mais on a une matrice triangulaire inversible qui fait passer aux $\lambda^i q$:

$q = \langle 2 \rangle m + \langle 2 \rangle q'$

$$\lambda^i q = \sum_{a+b=i} \underbrace{\lambda^a(\langle 2 \rangle m)}_{\text{cte}} . \lambda^b(\langle 2 \rangle q')$$

$\square$

<u>Exple</u> : $n = 6$.

S_6 a un automorphisme externe :

$1 \to S_6 \to \mathrm{Aut}(S_6) \to C_2 \to 1$

En effet

$S_5 \longrightarrow S_6$ ss gpe transitif) En permutant les 6 5-Sylows de S_5.

$X = S_6/S_5$ a 6 élts.

S_6 opère sur X.

D'où $S_6 \to \mathrm{Aut}(X) \simeq S_6$.

Soit dc $\sigma \in \mathrm{Aut}(S_6)$, $\sigma \notin S_6$.

Soit L une alg. étale de rg 6 sur k.

$\varphi : \Gamma_k \to S_6$

$\sigma\varphi : \Gamma_k \to S_6 \rightsquigarrow L_\sigma$ (à isom. près).

(cf., en termes de polynômes, la résolvante sextique).

$q(L_\sigma) = ?$

Grâce au thm précédent, on sait que $q(L_\sigma)$ s'écrit comme C.L. à coeff. dans $\mathbb{N}$ (corps premier) de $1, \lambda q_L, \lambda^2 q_L, \lambda^3 q_L$.

$$\boxed{\begin{aligned} q_{L_\sigma} &= \lambda^3 q_L - \langle 1,2\rangle \otimes \lambda^2 q_L \\ &\quad + \langle 1,1,2\rangle \otimes q_L - \langle 1,2\rangle . \end{aligned}}$$

Forme Trace :

Dans la dernière partie du cours, on s'intéresse à la forme trace.
En part., on regardera les cas $\begin{cases} n=3,4,5 \\ n=6,7. \end{cases}$

Question : $\boxed{\text{Soit } k \text{ un corps ; car } k \neq 2,\ n \text{ entier} \geq 1. \text{ « Quelles sont » les f. quad. } q \text{ à } n \text{ variables }/k \text{ qui sont égales à } q_E \text{ pour } E \text{ alg. étale de rg } n\ /k\,?}$

Condition triviale :

$n = \sum_{\lambda \in I} 2^\lambda$ écriture dyadique de n.
$I = \{i_1, \dots, i_\ell\}$ $i_1 < \dots < i_\ell$.

Prop. : $\boxed{q_E \text{ contient la forme quadratique } \langle 2^{i_1}, \dots, 2^{i_\ell}\rangle, \text{ de rg } \ell = |I|.}$

Exple : $n=7$ $\langle 1,2,4\rangle \simeq \langle 1,1,2\rangle$.

[contient signifie $q_E \simeq \langle 2^{i_1}, \dots, 2^{i_\ell}\rangle \oplus q'_E$
avec $\operatorname{rg} q'_E = n - \ell$].

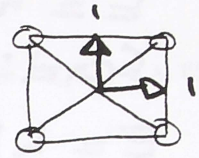
Preuve:

Springer: h'/h de deg. impair.
Si q_1 et q_2 st des f.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".

$\varphi : \Gamma_h \to S_n$.
Après ext. de deg. impair, l'image de φ est contenue dans un 2 Sylow de S_n.
Si $n = 2^{i_1} + \dots + 2^{i_\ell}$ $\quad \overset{\Omega}{\overset{\shortparallel}{[1, n]}} = \coprod_j \Omega_j \quad |\Omega_j| = 2^{i_j}$
2 Sylow de $S_n = S_\Omega$
$= \prod$ 2 Sylows de S_{Ω_j}.
Donc $\Omega = \coprod \Omega_j$ est la décomposition de Ω en orbites d'un 2 Sylow de S_n.
Γ_h préserve cette décomposition de Ω
$\iff E = \prod E_j$ avec $\operatorname{rg} E_j = 2^{i_j}$.

Or la forme trace représente n (si $n \neq 0$ ds h) car $\operatorname{Tr}(1^2) = n$.
Donc q_{E_j} représente 2^{i_j} et $q_{E_j} = \langle 2^{i_j} \rangle \oplus q'_j$.
D'où $q_E = \oplus q_{E_j} = \dots$

Mais $\begin{cases} \langle 4\rangle \simeq \langle 1\rangle \\ \langle 2,2\rangle \simeq \langle 1,1\rangle \end{cases}$



Δ on peut réduire la partie triviale à $\langle 1,\dots,1\rangle$ ou $\langle 1,\dots,1,2\rangle$.

<u>Exercice</u>:

Démontrer que q' n'a pas de "partie fixe".

Précisément : $\begin{cases} k \text{ corps} & \text{car } k \neq 2 \\ n \text{ entier} \geq 1. \end{cases}$

<u>mq</u> : $\exists\, K/k$ et $\exists$ une alg. étale E sur K de rang n dt la forme q'_E ne représente aucun élt de k.

<u>Indication</u> : construire une ext. multiquadratique, à Galois de type $(2,\dots,2)$ avec des indéterminées.

<u>exple</u> : $n = 7 = 1+2+4$.

ici ; $E = K \times K(\sqrt{x}) \times \underbrace{K(\sqrt{y},\sqrt{z})}_{K(\sqrt{y})\otimes K(\sqrt{z})}$

x, y, z indéterminées $/k$.

<u>Thm</u> : $\boxed{\text{Si } n \leq 3, \text{ la condit}^{\text{o}} \text{ triviale suffit pour qu'une forme donnée soit forme trace.}}$

Dém :

n=1 $E = k$; $q_E = \langle 1 \rangle$.
Condit° triviale : contenir $\langle 1 \rangle$.

n=2 $E = k[X]/(X^2-d)$ $q_E \simeq \langle 2, 2d \rangle$.
Condit° triviale : contenir $\langle 2 \rangle$.

n = 3 = 1+2 $q_E = \langle 1, 2, x \rangle$
Si $q = \langle 1 \rangle \oplus \langle 2, x \rangle$
$E = k \times E_2$ avec $q_{E_2} = \langle 2, x \rangle$.

Thm (Restre) k ; car $k \neq 2$
Si n est impair ≥ 1, et E étale de rang n, $\exists\, E'$ de rg $n-1$ telle que $q_E \simeq \langle 1 \rangle \oplus q_{E'}$, i.e. E et $k \times E'$ ont m̂ forme trace

D. ex. : $n = 3$
E ; d = disc. de E
$E' = k[X]/(X^2-d)$
E et $k \times E'$ ont m̂ forme trace.

Cor : Si q est de rg impair ≥ 1, vérifiant la condition triviale, On peut écrire $q = \langle 1 \rangle \oplus q_0$.
Alors q forme trace en rang n
$\Longleftrightarrow q_0$ ——— $n-1$

Dém. du thm de Mestre :

On peut supposer k ∞.
(Corps fini : il faut faire une vérification directe).

"déformations équitraces".

$P_t = P - tQ$; $\begin{cases} P \text{ unitaire de deg. } n \\ Q \text{ de degré} < n. \end{cases}$

P_t est unitaire de deg. n. $\quad \mathrm{Res}(P, Q) = 1$.
On suppose P séparable. $\mathrm{disc}(P) \neq 0$.
Alors $\mathrm{disc}(P_t) \neq 0$ pour tout $t \notin$ ens. fini.

$E_t = k[X]/(P_t)$; q_{E_t}

On dit que c'est une déformation "isotrace" si on a

(*) ① $q_{E_t} \simeq q_E$ t générique / $k(t)$ t ind.
ou
② $q_{E_\alpha} \simeq q_E$ $\forall \alpha \in k'$ / $\mathrm{disc}(P_\alpha) \neq 0$
k' ext. de k

① $\Leftrightarrow$ ②
($\Leftarrow$ clair ; $\Rightarrow$ par spécialisation).

Thm : Si n est impair, pour tt E, $\exists$ P et Q tq
1) les E_t vérifient (*)
2) $E \simeq E_0 = k[X]/(P)$.

Admettons ce résultat pour l'instant.
Choisissons α tq $P - \alpha Q$ ait une racine dans k.

p. ex. $\alpha = \dfrac{P(z)}{Q(z)}$ pour $z \in k$ tq $Q(z) \neq 0$,
et α tq $\mathrm{disc}(P - \alpha Q) \neq 0$.
$P - \alpha Q = (X - z) P_{n-1}$ où P_{n-1} est de deg. $n-1$.
D'où $E_\alpha = k \times E_{n-1}$.

<u>N.B.</u> : 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 $\deg Q, \deg R < n$

$$\begin{cases} ① \; PQ' - QP' = R^2 & (n \text{ impair}). \\ ② \; (P, Q) = 1 \,;\; (P, R) = 1 \end{cases}$$

<u>Construction</u> :
$P(X) = \prod (X - x_i)$

$$\frac{Q}{P} = \sum \frac{q_i}{X - x_i} \,; \quad \frac{R}{P} = \sum \frac{r_i}{X - x_i}.$$

$$\left(\frac{Q}{P}\right)' = \frac{R^2}{P^2}.$$

i.e. $$\sum \frac{-q_i}{(X - x_i)^2} = \sum_{i,j} \frac{r_i r_j}{(X - x_i)(X - x_j)}$$

$$= \sum \frac{r_i^2}{(X - x_i)^2} + \sum_{i \neq j} \frac{r_i r_j}{x_i - x_j} \frac{1}{X - x_i}.$$

Ceci donne $q_i = -r_i^2$.
On trouve que ça marche si les r_i st sol. du syst. $\sum_{i \neq j} \alpha_{ij} r_i = 0$
avec $\alpha_{ij} = \dfrac{1}{x_i - x_j}$

Or (α_{ij}) est alternée (dc de rg pair) de type $n \times n$ avec n impair.
Dc $\exists$ une solut° 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 Castelle :
① + ② $\Rightarrow$ (*) (isotrace).

(En car 0 : la dérivée a une valuat° paire (R^2)

$$\begin{array}{c} X \\ \downarrow \pi \\ \mathbb{P}_1 \end{array}$$ différente est un carré.) .

<u>Exple</u> : $P = X^3 + pX + q$:
On peut écrire Q et R ...

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 f.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 car $\neq 2$.
Dans les dém., k sera le plus souvent supposé infini.

Rque : $\boxed{\text{car } 2}$

On a un analogue de la forme trace :
E/k de rang n.

$x \in E \qquad \begin{array}{l} E \to \bar{k} \\ x \mapsto \sigma(x) \end{array}$

On remplace $\sum \sigma(x)^2$ par
$f(x) = \sum_{\sigma < \tau} \sigma(x)\,\tau(x)$ (2^{nd} 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.-M. Bergé et J. Martinet ont montré que f est déterminée par n et le disc. additif de E.

(disc. additif : $\Gamma_k \xrightarrow{\varphi} S_n \xrightarrow{sgn} \mathbb{Z}/2\mathbb{Z}$
$\mathrm{Hom}(\Gamma_k, \mathbb{Z}/2\mathbb{Z}) \simeq k/\wp k \quad \wp x = x^2 + x$).

Précisément :
$\frac{n}{2} - 1$ fois forme hyperbolique $\oplus\ x^2 + xy + by^2$.

Exercice : mq il n'y a pas d'invariant des alg. étales en car. 2 normalisés, à valeurs dans le gpe de Brauer non nul.

Le rang 4

E alg. étale $/k$ de rang $n = 4$.
q_E contient $\langle 1 \rangle$.
$q_E = \langle 1 \rangle \oplus Q_E$ rg $Q_E = 3$.

On désire caractériser les formes Q_E de rang 3 qui interviennent.

Prop. : Soit Q une forme de rg 3, de discriminant d. Il y a équivalence entre :

(1) $w_3(Q) = 0$ dans $H^3(k, \mathbb{Z}/2\mathbb{Z})$.

(2) d est représenté par la 2 forme de Pfister $\langle 1\rangle \oplus \langle d\rangle \otimes Q$

(3) 1 est représenté par $\langle d\rangle \oplus Q$.

(4) $\lambda_{-1} Q = 0$ dans Wk (ou $GrWk$).
i.e. $\underset{1}{\lambda^0 Q} - \lambda^1 Q + \underset{Q}{\lambda^2 Q} - \lambda^3 Q = 0$

(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. $Q \simeq \langle A, A^2 - B, AB(A^2-B)\rangle$.

Rques:

- Notat° : $\lambda_t q = \sum_{i=0}^{\infty} t^i \lambda^i q$ (q forme quad.)
- Si $d(Q) = 1$, $\langle 1\rangle \oplus Q$ est une 2 forme de Pfister. ($Q = \langle a, b, ab\rangle \to \langle 1\rangle \oplus Q = \langle 1, a, b, ab\rangle$).

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, q_E satisfait aux conditions (1), .., (6).

p.exple : (1) est vraie. (thm g^{al} sur les λ_i ; on est en rang 4).

2) Réciproquement, on a :

Lemme : $\boxed{\begin{array}{l}\text{Soient } A, B \in k^*,\ A^2-B \neq 0. \\ \text{Soit } F(X) = X^4 - 2AX^2 + B. \\ E_{A,B} = k[X]/(F). \text{ Alors} \\ q_{E_{A,B}} = \langle 1 \rangle \oplus \langle A, A^2-B, AB(A^2-B) \rangle\end{array}}$

Preuve :

$d(E_{A,B}) \sim B$.

$E_{A,B} \supset \{1, x, x^2 - A\}$. Ils st 2 à 2 orthogonaux
(↑ image de X)

et $Tr(1^2) = 4 \sim 1$; $Tr(x^2) = 4A \sim A$;

$Tr[(x^2-A)^2] = 4(A^2-B) \sim A^2-B$.

Dc $q_{E|\text{sous esp. de dim } 3} \sim \langle 1, A, A^2-B \rangle$.

D'où $q_E = \langle 1, A, A^2-B, y \rangle$ et en comparant les discriminants on obtient $y = AB(A^2-B)$.

Rqe : Ce calcul permet aussi de voir le sens 1). En effet :

Si k'/k ext. de degré impair,

Q satisfait (1), .., (6) sur k'

$\Updownarrow$ Q ——————————— k.

(par exple :

c'est évident pour (1) : cohomologie co cohom.

(2) : thm de Springer)

On peut donc supposer que $\varphi(\Gamma_k) \subset S_4$

est contenu dans un 2 sylow D_4 de S_4.

Lemme : $\boxed{\text{Qd on a une extension à gpe } D_4\text{, il existe un polynôme bicarré qui définit l'alg. étale correspondant}}$

$$\begin{array}{l} E \\ 2 \mid \\ E_2 \\ 2 \mid \\ k \end{array}$$

$E = E_2(\sqrt{x}) \quad x \in E_2$

$x^2 - 2ax + b = 0$ sur k convient.

($k\infty$; donc on peut supposer $x \notin k$).

Démonstration de la propriété :

(2) (3) (4) (5) et (6) sont équivalentes par des arguments élémentaires. Par contre, (1) $\Rightarrow$ les autres utilise le thm de Merkurjev-Suslin.

Rque : Le thm nous dit de que $n=4$, les formes traces sont caractérisées

par $\begin{cases} \text{① la condition triviale.} \\ \text{② } w_3 = 0. \end{cases}$

Autre rqu : Dém. directe de (4).

$q_E = \langle 1 \rangle \oplus Q_E$. $\quad d_{-1} Q_E \overset{?}{=} 0$.

Grâce à la caractérisation générale de la nullité des invariants de Witt, il suffit de vérifier (4) lorsque $E = E_1 \times E_2$, $rg\, E_i = 2$.

Ds ce cas $q_E = \langle 2, 2d_1 \rangle \oplus \langle 2, 2d_2 \rangle$ où $d_i = \mathrm{disc}(E_i)$.

Dc $q_E = \langle 1, 1, \alpha, \beta \rangle$ i.e. $Q_E = \langle 1 \rangle \oplus f$.

Mais $d_t Q_E = d_t \langle 1 \rangle\, d_t f = (1+t)\, d_t f$.

Dc $d_{-1} Q_E = 0$.

---

(2) <=> (3) est trivial.

---

(1) <=> (2) par Merkurjev-Suslin :

Merkurjev-Suslin 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 $q_{a,b}$
> $\iff (a)(b)(c) = 0$ ds $H^3(k)$.

Ou (de façon équivalente)

> Si F est une 3 forme de Pfister,
> F nulle ds Wk (F hyperbolique)
> $\iff$ Inv. d'Arason de F = 0 dans $H^3(k)$.

Le 06.12.93 ⑦

[En effet
c représenté par $q_{a,b} \iff q_{a,b} \otimes \langle 1,-c\rangle$
représente $0 \iff q_{a,b} \otimes \langle 1,-c\rangle$ est hyperbol.]

Ici :
$Q = \langle -a,-b,ab\rangle \otimes \langle d\rangle$.
Dc $\langle 1\rangle \oplus \langle d\rangle \otimes Q = \langle 1,-a,-b,ab\rangle = q_{a,b}$
Donc on doit considérer $(d)(a)(b) \in H^3(k)$.
Mais :
$w_3(q) = (-ad)(-bd)(abd)$
$= (-a)(-bd)(bd) + (d)(-bd)(abd)$ (car $(a)(-a)=0$)
$= (d)(b)(abd) = (d)(b)(-ab) = (d)(b)(a)$!

---

(4) => (2)

(4) s'écrit $\lambda^0 Q - \lambda^1 Q + \lambda^2 Q - \lambda^3 Q = 0$
avec $\lambda^0 Q = \langle 1\rangle$
$\lambda^1 Q = Q$
$\lambda^2 Q = \langle d\rangle \otimes Q$ ($\lambda^{n-1} q = \langle d\rangle \otimes q$
$\lambda^3 Q = \langle d\rangle$. si q de rg n).
Dc
(4) s'écrit $\langle 1\rangle \oplus \langle d\rangle \otimes Q \simeq Q \oplus \langle d\rangle$
Ainsi (4) => (2) est clair.

---

(2) => (4)

Réciproquement, (2) entraîne
$\langle d\rangle \otimes (\langle 1\rangle \oplus \langle d\rangle \otimes Q) \simeq \langle 1\rangle \oplus \langle d\rangle \otimes Q$.
$\underbrace{\qquad\qquad\qquad\qquad}$
forme 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 $x \in k$ tq $1 = dx^2 + a$, a représenté par Q.
Grâce au lemme suivant, on peut choisir $a \neq 0$:

Lemme : $\boxed{\text{(k } \infty\text{) Si } \alpha \text{ est représenté par } f_1 \oplus f_2 \text{, avec rg } f_i \geq 1 \text{, alors } \exists x_1 \text{ et } x_2 \text{ tq } \alpha = f_1 x_1 + f_2 x_2 \text{ avec } f_1 x_1 \neq 0 \text{ et } f_2 x_2 \neq 0.}$

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 $Q = \langle a, b, c \rangle$ $b, c \in k^*$.
$(a)(d) = 0 \Rightarrow a = u^2 - dv^2$ $u, v \in k^*$.
On pose : $A = b$; $B = abc\left(\frac{bv}{u}\right)^2$.

$$A^2 - B = b^2 - abc\,\frac{bv^2}{u^2}$$
$$= b^2\left[\frac{u^2 - abcv^2}{u^2}\right] = b^2\left[\frac{u^2 - dv^2}{u^2}\right]$$
$$= b^2 \frac{a}{u^2} \sim a.$$

On peut donc écrire
$Q \simeq \langle A^2-B, A, AB(A^2-B)\rangle$.
($AB(A^2-B)$ nbabca nc.)

---

(6) => (3) reste à voir.

Mais
$\langle A, A^2-B, AB(A^2-B)\rangle \simeq \langle AB, A^2-B, A(A^2-B)\rangle$
(en effet
$\langle 1, B(A^2-B)\rangle \simeq \langle B, A^2-B\rangle$ car
$\langle B, A^2-B\rangle$ représente A^2, donc 1).

Dc $d = B$, et A^2-B est représenté par la forme et vérifie $(B)(A^2-B)=0$.

<u>Résultat</u> également obtenu par Epkenhans et Krüskemper.

<u>Corollaires</u> (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 un 2 gpe avec $q_E = q$.
("à gpe de Gal." : correspondant à un $\varphi : \Gamma_k \to S_n$ tq $\mathrm{Im}(\varphi)$ est un 2 gpe).

$\boxed{n=5}$

q est une forme trace

$\Longleftrightarrow \begin{cases} q \text{ contient } \langle 1 \rangle & q = \langle 1 \rangle \oplus q_4 \\ \text{et} \\ q_4 \text{ est forme trace en rang } 4. \end{cases}$

$\boxed{n=6}$ $6 = 2+4$.

La condition triviale pour q est contenir $\langle 1,2 \rangle$.

$q = \langle 1,2 \rangle \oplus Q$ avec $\operatorname{rg} Q = 4$.

$d(Q) = 2d$ si $d = d(q)$.

Thm : Pour que $q = \langle 1,2 \rangle \oplus Q$ soit forme trace, il faut et il suffit que

(*) 1 est représenté par Q sur le corps $k(\sqrt{2d})$ $d = \operatorname{disc}(q)$

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 $d \sim 2$ (i.e. $k = k(\sqrt{2d})$).

On fait une extension de degré impair de façon à ce que $\varphi(\sqrt{n})$ soit un 2 gpe.

D'où une décomposition $E = E_4 \times E_2$ avec $\operatorname{rg} E_i = i$.

On a $q_E = q_{E_4} \oplus q_{E_2}$

$q_{E_4} = 1 \oplus Q_3$; $q_{E_2} = \langle 2, 2\alpha \rangle$.

Dc $q_E = \langle 1, 2, 2\alpha \rangle \oplus Q_3$

D'où $d(Q_3) = 2\alpha$.

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 thm précédent (rang 4).

2) Suffisance :

Lemme : Soit f une f.q. de rang ≥ 2. Soit $\alpha \in k^*$. Il y a équivalence entre :

(1) $f \supset \langle x, y \rangle$ avec $(x)(\alpha y) = 0$
$\Updownarrow$
(2) f représente 1 sur $k(\sqrt{\alpha})$.

Preuve du lemme :

(1) => (2) :

Il faut voir que $\langle x, y\rangle$ représente 1 sur $k(\sqrt{\alpha})$. On est ramené à $\alpha = 1$.
Mais $(x)(y) = 0$ signifie qu'on 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
$1 = f(v_1 + \sqrt{\alpha}\, v_2)$.
i.e. $1 = f(v_1) + \alpha f(v_2) + 2\sqrt{\alpha}\, f(v_1, v_2)$.
D'où $v_1 \perp v_2$. Posons $\begin{cases} f(v_1) = x \\ f(v_2) = y \end{cases}$

$f \supset \langle x, y\rangle$ et $1 = x + \alpha y$
$\Rightarrow (x)(\alpha y) = 0$.

Pour achever la dém. du thm, on applique ce lemme avec $\alpha = 2d$.
$Q \supset \langle x, y\rangle$ avec $(x)(2dy) = 0$.
$q = \langle 1, 2, x, y\rangle \oplus q_2$ rg $q_2 = 2$
$q = \langle 2, y\rangle \oplus q_4$ avec $q_4 = \langle 1, x\rangle \oplus q_2$.
$\langle 2, y\rangle$ est une forme trace.
Donc $\exists E_2$ étale de rg 2 avec
$\langle 2, y\rangle = q_{E_2}$.
De même, $\exists E_4$, étale de rg 4, avec
$q_{E_4} = \langle 1, x\rangle \oplus q_2$.

(En effet, $\langle x \rangle \oplus q_2$ vérifie bien les propriétés (1) à (6) précédentes :
(5) p. exple : $(x)(d(q_4)) = 0$
car : $d = d(q) = (2y\, d(q_4))$
Dc $d(q_4) = (2dy)$ et on a bien
$(x)(2dy) = 0$).

L' automorphisme externe de S_6

$A_6 \simeq PSL_2(\mathbb{F}_9)$

X dte projective sur $\mathbb{F}_9$.

A_6 peut se représenter comme :

Les permutations de la forme

$$z \mapsto \frac{az+b}{cz+d} \qquad a,b,c,d \in \mathbb{F}_9$$
$$ad - bc = \begin{cases} 1 \\ \text{ou} \\ \text{carré} \end{cases}$$

On a envie d'agrandir A_6 en ajoutant

$$\left\{ \begin{array}{ll} z \mapsto \dfrac{az+b}{cz+d} \quad ad-bc \neq 0 & A_6 \cdot 2 \\ z \mapsto \bar{z} \quad \text{où } \bar{\ } \text{ autom. de } \mathbb{F}_9 = \mathbb{F}_3(i) & \\ \qquad\qquad\qquad i \mapsto -i & \end{array} \right.$$

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, $\to$ c'est scindé sur chaque gpe d'ordre 2).

Soit $\sigma \in \mathrm{Aut}(S_6) - S_6$.
E alg. étale de rang 6.
E_σ autre —— qui lui correspond par σ.

Pb : q_{E_σ} en termes 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 $\boxed{Q_{E_\sigma} = \lambda^3 Q_E}$

(3^{eme} puissance extérieure).

Si $d = d(E) = d(E_\sigma)$, cette formule équivaut à

$$\boxed{Q_{E_\sigma} = \langle 2d\rangle \otimes Q_E}$$

Cas particulier : $d = 1$ $(\varphi(\Gamma_k) \subset A_6)$

$Q_{E_\sigma} \simeq \langle 2\rangle \otimes Q_E$.
$q_{E_\sigma} \simeq \langle 2\rangle \otimes q_E$ $\leftarrow$ On a des contre expls ds le cas gal.

Dém : $A, B, C \in k^*$, $A^2 - B \neq 0$

$F_{A,B} = X^4 - 2AX^2 + B$ $\quad E_{A,B}$ rg 4

$F_C = X^2 - C$ $\quad E_C$ 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.

Posons $\begin{cases} A' = 2AC \\ B' = 4C^2(A^2-B) \\ C' = BC(A^2-B) \end{cases}$

<u>Assertion</u>: $\boxed{E_{A',B',C'} \simeq (E_{A,B,C})_\sigma}$

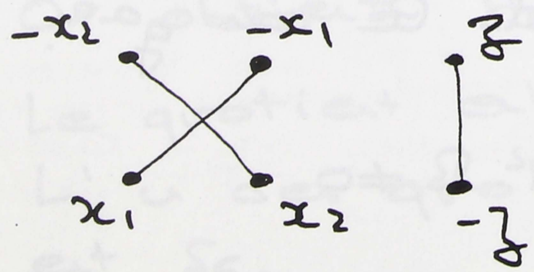
Une telle algèbre correspond à un

$$\varphi : \Gamma_k \longrightarrow \underset{2\,\text{Sylow}}{D_4 \times C_2} \xrightarrow[\sigma]{} S_6$$

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 $Z^2 - C$ sont z et $-z$.

Act° de Galois : gpe d'automorphismes de la figure:



On constate que les racines de l'équation ' sont

$$\begin{cases} x'_1 = z\,(x_1 + x_2) \\ x'_2 = z\,(-x_1 + x_2) \\ z' = \frac{1}{2}\, z\, x_1 x_2 (y_1 - y_2) \end{cases}$$

Reste à voir que l'act° est la tordue par σ.
par exple : $(1\,2) \mapsto (1\,2)(3\,4)(5\,6)$
$(1\,2)(3\,4) \mapsto (1\,2)(3\,4)$

$$\left.\begin{array}{l} x_i \text{ inv.} \\ z \mapsto -z \end{array}\right) \quad \begin{cases} x'_1 \mapsto -x'_1 \\ x'_2 \mapsto -x'_2 \\ z' \mapsto -z' \ldots \end{cases}$$

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].

Rque En fait, pour prouver $Q_\sigma = d^3 Q$, on peut supposer $E = L_2 \times L'_2 \times L''_2$
alg. de rang 2
i.e. $\varphi(\Gamma_k) \subset (2,2,2) \subset S_6$.

(Cela revient à supposer A^2-B est un carré.) Mais l'alg. tordue n'est plus un produit de 3 quadratiques. ((2,2,2) n'est pas envoyé sur lui même). Donc <u>ici</u> cela ne simplifie pas vraiment.

<u>Rque</u> : En car 0.

S_n; rep. orthogonale de S_n sur $\mathbb{Q}$.
E alg. étale de rang n.
$\varphi : \Gamma_k \to S_n$; V_φ = V tordu par φ.

On obtient ainsi un invariant Witt par $E \mapsto q_E(V) \in Wk$.
↳ 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 $S_6 \xrightarrow{\sigma} S_6 \subset O_6$].

<u>Thm</u> : $\boxed{\text{L'anneau des rep. lin. sur } \mathbb{Q} \text{ du gpe } S_n \text{ est engendré (comme } \lambda\text{-anneau) par la rep. linéaire de deg. n évidente } S_n \to Gl_n.}$

Dc l'anneau des rep. orthogonales $RO(S_n) \simeq W(\mathbb{Q}) \otimes R(S_n)$.

J.-P. Serre X
Cours au collège de France.
Le 13 décembre 93

X - 1

On ~~va~~ applique les résultats précédents aux torseurs sous le gpe $\tilde{A}_6 = 2A_6$.

On a
$$\begin{array}{c} \tilde{A}_6 \\ | \\ A_6 \subset S_6 \end{array}$$

Etant donnés k car $k \neq 2$
et $\varphi : \Gamma_k \longrightarrow S_6$ $\leadsto$ E alg. ét. de rang 6.

q_E forme trace de rang 6.

$w_i(q_E)$ avec $w_1 = (d)$ $d = \mathrm{disc}(E)$
$= \mathrm{disc}(q_E)$.

φ à valeurs dans $A_6 \iff w_1 = 0$
(i.e. $d = 1$ ds k^*/k^{*2})

Si $w_1 = 0$, on a vu $w_2 = w_2^g$ 2nde classe gal.
Mais w_2^g est l'obstruction à relever φ à $\tilde{A}_6$.

En particulier
$w_2 = 0 \iff$ il existe $\tilde{\varphi} : \Gamma_k \longrightarrow \tilde{A}_6$ qui relève φ.

On s'intéresse aux algèbres étales E avec $w_1 = w_2 = 0$. [Cela revient à considérer les $\tilde{A}_6$ torseurs modulo la torsion quadratique].

<u>Question</u> : Quelles st les formes traces correspondantes ?

<u>Thm</u> : $\boxed{\text{Soit } q \text{ une f.q. à 6 variables avec } w_1 = w_2 = 0. \text{ Pour que } q \text{ soit forme trace, il faut et il suffit qu'il existe } c \in k^* \text{ avec } \begin{cases} ① & q = \langle 1,1,c,c,c,c\rangle \\ ② & (2)(c) = 0 \text{ (i.e. } \exists x,y \in k \text{ tq } c = x^2 - 2y^2) \\ ③ & c \text{ est une somme de 4 carrés dans } k(\sqrt{2}). \end{cases}}$

<u>Rque</u> : (i) => $w_1 = w_2 = 0$

($w_2 = \sum_{6 \text{ fois}} (c)(c) = 0$ car $6 \equiv 0 \bmod. 2$).

<u>Cor</u> : $\boxed{\exists \text{ des algèbres étales } E \text{ avec } w_1 = w_2 = 0 \text{ et } q_E \neq \langle 1,1,\ldots,1\rangle.}$

<u>Rque</u> : $\langle 1,1,c,c,c,c\rangle = \langle 1,1\rangle \oplus \langle c\rangle \underbrace{\langle 1,\dots,1\rangle}_{\text{forme de Pfister}}$

Donc

$\langle c,c,c,c\rangle \simeq \langle c',c',c',c'\rangle \iff c'/c$ est représentée par $\langle 1,1,1,1\rangle$ 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 Merkurjev-Suslin.

c est $\boxed{4} \iff (-1)(-1)(c) = 0$ dans $H^3(k)$.

Dc si l'on associe à E $(-1)(-1)(c) \in H^3(k)$

On obtient un inv. cohom. $a(E) \in H^3(k)$,

et $q_E \simeq q_{E'} \iff a(E) = a(E')$.

(<u>N.B.</u> a est un inv. cohom. pour $\tilde{A}_6$).

<u>Démonstration</u> :

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 : $\begin{cases} q \text{ contient } \langle 1,2\rangle \\ q \text{ contient } \langle 1,1,2\rangle \text{ sur } k(\sqrt{2d}) \end{cases}$

$k(\sqrt{2d}) = k(\sqrt{2})$

(ici d=1).

Le 13.12.93

4

Rque : $(a)(b) = 0 \iff \langle a,b\rangle \simeq \langle 1, ab\rangle$.

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 $\boxed{4}$ sur $k(\sqrt{2})$.

Donc $\langle c,c,c,c\rangle \simeq \langle 1,1,1,1\rangle$ sur $k(\sqrt{2})$.

Ainsi sur $k(\sqrt{2})$ $q \simeq \langle 1,1,1,1,1,1\rangle$ 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. $w_1(Q) = 0$; $w_2(Q) = (-1)(-1) + (a)(b)$
2. $\exists c \in k^*$ tq $Q \simeq \langle 1\rangle \oplus \langle c\rangle q_{a,b}$

Preuve :

2 => 1 : c'est du calcul.

1 => 2 : On regarde $Q_6 := \langle -1\rangle \oplus Q$. Cette forme a les mêmes w_1 et w_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 $w_1(Q_4)=0$ et $w_2(Q_4) = (-1)(-1) + (a)(b)$. 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 w_1 et w_2].

Ici, $a=b=-1$. La proposition nous dit que si $w_1(Q) = w_2(Q) = 0$, alors $Q = \langle 1,c,c,c,c\rangle$, $c \in h^*$.

E ; q_E.

La condition triviale dit que q représente 1.

Donc $q = \langle 1\rangle \oplus Q$ avec $\mathrm{rg}\, Q = 5$.
$Q \simeq \langle 1,c,c,c,c\rangle$, $c \in k^*$ grâce à la proposition précédente. On a donc bien
1 $q_E = \langle 1,1,c,c,c,c\rangle$.

On veut maintenant modifier c pour qu'il vérifie 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 donc 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 $Q_4 \simeq \langle y,y,y,y\rangle$.

On choisit $c = y$.

$2 = x^2 + c$ implique $(2)(c) = 0$. C'est 2.

($(2)(c) = 0 \iff c = X^2 - 2Y^2$. De ce fait on a $(2)(-c) = 0$. Mais $(2)(-1) = 0$.
On en déduit $(2)(c) = 0$.).

Reste à prouver 3, i.e. $q_E \simeq \langle 1,\dots,1\rangle$ 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 $k(\sqrt{2})$

Donc $q_E \simeq \langle 1,1\rangle \oplus Q_4$ avec Q_4 représente 1.

Autrement dit $Q_4 = \langle 1,\dots,1\rangle$.

Ainsi $\langle c,c,c,c\rangle \simeq \langle 1,1,1,1\rangle$ 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 $w_1 = w_2 = 0$ on a $q_E \simeq \langle 1,1,\dots,1\rangle$.

Vu le thm,

$O_6 \iff$ Pour tout $c \in k^*$

$$\left.\begin{array}{l} 2c = 0 \\ c = \boxed{4} \text{ dans } k(\sqrt{2}) \end{array}\right) \Rightarrow c = \boxed{4} \text{ dans } k.$$

On va regarder quels corps ont cette propriété.

Déjà :

1) Si $(-1)(-1) = 0$ dans $H^2(k)$, O_6 est vraie car tout élément est $\boxed{4}$

2) En part., si car $k \neq 0$, O_6 est vraie.

3) De m̂, si -1 est u carré, ______

4) ___, -2 ______, ______

5) Si k est u corps de nombre (ou u corps local, ā c.v. fini), O_6 est vraie.

(En effet, il faut simplement vérifier $\langle -c,1,1,1,1\rangle$ 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 u peu plus tard).

Dc il faut chercher u contre exple sur des variétés qui ne sont pas rationnelles.

Pb : Y a-t-il ue courbe elliptique $C/\mathbb{Q}$ dt le corps de fctos ne vérifie pas O_6?

De façon plus gale :

Pb 2 : Quel est le deg. de tr $/\mathbb{Q}$ minimum d'u corps k ne vérifiant pas O_6?

Un exple de corps ne satisfaisant pas à C_6.

$\mathbb{Q}$ quadrique $X_1^2+X_2^2+X_3^2+X_4^2+X_5^2+7=0$.
[$\varphi = \langle 1,1,1,1,1,7\rangle$. $X = Q(\varphi)$ quadrique projective définie par $\varphi = 0$.]
$k = \mathbb{Q}(X) = \mathbb{Q}(x_1, x_2, x_3, x_4, \sqrt{-7-x_1^2-\dots-x_4^2})$.
Sur ce corps, $c=-1$ convient.

Preuve:
On doit vérifier:
(2) $(2)(c) = (2)(-1) = 0$.
(3) $c = \boxed{4}$ dans $k(\sqrt{2})$.

On va utiliser $7 = \boxed{3}$ sur $\mathbb{Q}(\sqrt{2})$
$\neq \boxed{3}$ sur $\mathbb{Q}$.

Sur $k(\sqrt{2})$ $X_1^2+X_2^2+\dots+X_5^2+\alpha_1^2+\alpha_2^2+\alpha_3^2=0$.
Dc la forme $\langle 1,\dots,1\rangle$ de rg 8 représente 0: elle est hyperbolique, et $\langle 1,1,1,1\rangle \simeq \langle -1,-1,-1,-1\rangle$
D'où $-1 = \boxed{4}$ sur $k(\sqrt{2})$.

Supposons maintenant $-1 = \boxed{4}$ sur $k = \mathbb{Q}(\varphi)$
C'est équivalent à $\psi = \langle 1,\dots,1\rangle$ de rg 8 est hyperbolique sur $\mathbb{Q}(\varphi)$.

Le 13.12.93

X - 10

Mais (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. ψ anisotrope, et ψ hyperbolique sur $k_0(\varphi)$, alors $\psi \supset \varphi$.

Grâce à ce résultat, on obtient
$\langle 1, \ldots, 1 \rangle = \langle 1,1,1,1,1,7 \rangle \oplus \langle \alpha, \beta \rangle$.
Thm de simplification de Witt :
$\langle 1,1,1 \rangle \simeq \langle 7, \alpha, \beta \rangle$ 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 $\mathrm{res}(e_c) = 0$ (ds $H^2(k)$).

Rqe : Si K complet, on a alors
$e_c \in H^3(k) \subset H^3(K)$.
$(0 \to H^i(k) \to H^i(K) \xrightarrow{\text{rés}} H^{i-1}(k) \to 0)$.

Preuve:

On peut supposer K complet, car le résidu ne change pas qd on complète.

a) Si $v(c) \equiv 0 \bmod. 2$ $c = \alpha^2 u$ u unité $v(u) = 0$.
Dc $e_c = (-1)(-1)(u) \in H^3(k)$
$(= (-1)(-1)(\tilde{u})$ où $\tilde{u}$ est la réduct° de $u)$.

b) Si $v(c) \equiv 1 \bmod. 2$ $c = \alpha^2 \pi$ π unif.
Dc $(2)(c) = (2)(\pi)$ et
résidu $(2)(\pi) = (2) \in H^1(k)$.
Dc $(2) = 0$ dans $H^1(k)$ (car $(2)(c) = 0$).
i.e. 2 carré dans k^*
D'où 2 ———— K^*.
Ds ce cas $c = \boxed{4}$ ds $K(\sqrt{2})$
$\Rightarrow c = \boxed{4}$ ds K. D'où $e_c = 0$.

On peut maintenant démontrer 6)

k a la propriété $O_6 \Rightarrow k(T)$ aussi.

Notons $K = k(T)$.

$c \in K^*$ tq $(2)(c) = 0$ et $(-1)(-1)(c) = 0$ dans $H^3(K(\sqrt{2}))$.

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 cte, i.e. $e_c \in H^3(k)$

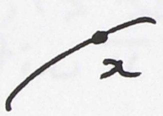
$(0 \to H^i(k) \to H^i(K))$.

Reste à voir que c'est 0.

Pour cela, on spécialise.

k de car 0. Donc k ∞.

$\mathbb{P}_1$



On peut donc choisir un point rationnel $x \in \mathbb{P}_1(k)$

tq $c(x) \neq 0, \infty$.

Alors $c(x) = \tilde{c} \in k^*$.

$$e_c(x) = (-1)(-1)(\tilde{c})$$
$$= e_c$$

Dc 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_0)

$(-1)(-1)(\tilde{c}) = 0$.

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 ctre exples. (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 versel (en car. 0)
Alors K n'est pas une ext. pure de $\mathbb{Q}$.

Exples de tels ss gpes : (pas de torseurs versels rationnels sur $\mathbb{Q}$)

2 Sylow $\simeq Q_{16}$ (quat.)
$\tilde{A}_6 = 2.A_6$; $\tilde{A}_7 = 2.A_7$; $SL_2(\mathbb{F}_7)$.

[$PSL_2(\mathbb{F}_7) \simeq SL_3(\mathbb{F}_2) \hookrightarrow A_7$

$$\begin{tikzcd} \underset{168}{PSL_2(\mathbb{F}_7)} \arrow[r, phantom, "\simeq"] & SL_3(\mathbb{F}_2) \arrow[r, hook] & A_7 \\ SL_2(\mathbb{F}_7) \arrow[u] \arrow[rr] & & 2.A_7 \arrow[u] \end{tikzcd}$$]

Démonstration :

Soit K de caract. 0 tel qu'il existe un G torseur versel sur K.
Le corps K n'a pas la propriété Q_6.
(En effet, s'il l'avait, tout corps de car 0 l'aurait aussi).
G torseur $L/k \longmapsto a(L) \in H^3(k)$.
($G \subset 2.A_7$

$\downarrow$

$A_7 \subset S_7$

De $L \mapsto E_L$ alg. ét. de rg 7.
$q_{E_L} \simeq \langle 1 \rangle \oplus q'$ $\quad q'$ forme trace de rg 6.
$G \subset 2.A_7 \Rightarrow \left\{ \begin{array}{l} w_1 \\ w_2 \end{array} \right.$ sont nuls $\left\{ \begin{array}{l} \text{pour } q \\ \text{—— } q' \end{array} \right.$

D'où $a(q') = (-1)(-1)(c) \in H^3(k)$.).

Dc si K vérifiait O6, l'inv. serait nul $\forall k$, de car 0, et $\forall$ G torseur sur k.

Or on va construire un contre exple :

Soit k un corps ne vérifiant pas O6.
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 $\boxed{k}$
i.e. $a(q_E) \neq 0$.
Une telle alg. correspond à $\varphi : \Gamma_k \to A_6$.
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 $\tilde{\varphi} : \Gamma_k \to 2.A_6 \subset 2.A_7$.
L'image de $\tilde{\varphi}$ est contenue dans un 2 Sylow de $2.A_7$, donc dans G.

D'où un G torseur, avec $a \neq 0$.

contradiction.

FIN DU COURS