La cohomologie galoisienne–cinq pièces faciles

Philippe Caldero

Journée d'équipe

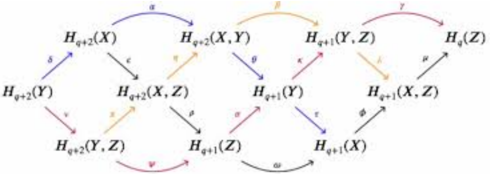
19/01/2018

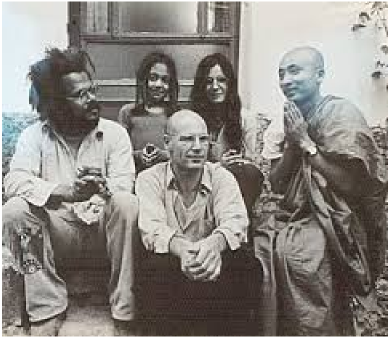
Présentation

Présentation

Présentation

Présentation





Présentation

Définition

Soit G un groupe et M un G-module (un groupe abélien muni d'une action de G compatible) notée m^g. On définit le complexe de cochaînes :

$$C^n(G, M) := \{f,\ G^n \to M\},\ \ C^0 = M$$

$$\delta_n\ :\ C^n(G, M) \to C^{n+1}(G, M)$$

$$\delta_n(f)(g_1, g_2, \cdots, g_{n+1}) =$$

$$-f(g_2, \cdots, g_{n+1})^{g_1} + \sum_{i=1}^{n}(-1)^{i-1} f(g_1, \cdots, g_i g_{i+1}, \cdots, g_{n+1}) + (-1)^n f(g_1, \cdots, g_n).$$

$$\delta_n(f)(g_1, g_2, \cdots, g_{n+1}) =$$

$$-f(g_2, \cdots, g_{n+1})^{g_1} + \sum_{i=1}^{n}(-1)^{i-1} f(g_1, \cdots, g_i g_{i+1}, \cdots, g_{n+1}) + (-1)^n f(g_1, \cdots, g_n).$$

En particulier :

$$\delta_0(m)(g) = -m^g + m,\ \delta_1(f)(g_1, g_2) = -f(g_2)^{g_1} + f(g_1 g_2) - f(g_1)$$

Tout i-cobord est un i-cocycle : $\mathrm{Im}(\delta_{i-1}) \subset \ker(\delta_i)$.

Tout i-cobord est un i-cocycle : $\operatorname{Im}(\delta_{i-1}) \subset \ker(\delta_i)$.
On définit les groupes de cohomologie

$$H^i(G, M) := \ker(\delta_i)/\operatorname{Im}(\delta_{i-1}).$$

Tout i-cobord est un i-cocycle : $\mathrm{Im}(\delta_{i-1}) \subset \ker(\delta_i)$.
On définit les groupes de cohomologie

$$H^i(G, M) := \ker(\delta_i)/\mathrm{Im}(\delta_{i-1}).$$

Pour commencer :

$$H^0(G, M) = M^G.$$

Tout i-cobord est un i-cocycle : $\mathrm{Im}(\delta_{i-1}) \subset \ker(\delta_i)$.
On définit les groupes de cohomologie

$$H^i(G, M) := \ker(\delta_i)/\,\mathrm{Im}(\delta_{i-1}).$$

Pour commencer :

$$H^0(G, M) = M^G.$$

Deux résultats fondamentaux en théorie de Galois : pour toute extension galoisienne L de K :

Tout i-cobord est un i-cocycle : $\mathrm{Im}(\delta_{i-1}) \subset \ker(\delta_i)$.
On définit les groupes de cohomologie

$$H^i(G, M) := \ker(\delta_i)/\,\mathrm{Im}(\delta_{i-1}).$$

Pour commencer :

$$H^0(G, M) = M^G.$$

Deux résultats fondamentaux en théorie de Galois : pour toute extension galoisienne L de K :

$$H^0\big(\mathrm{Gal}(L/K), L^*\big) = K^*,$$

Tout i-cobord est un i-cocycle : $\operatorname{Im}(\delta_{i-1}) \subset \ker(\delta_i)$.
On définit les groupes de cohomologie

$$H^i(G, M) := \ker(\delta_i)/\operatorname{Im}(\delta_{i-1}).$$

Pour commencer :

$$H^0(G, M) = M^G.$$

Deux résultats fondamentaux en théorie de Galois : pour toute extension galoisienne L de K :

$$H^0\big(\operatorname{Gal}(L/K), L^*\big) = K^*,\ H^1\big(\operatorname{Gal}(L/K), L^*\big) = 1$$

Tout i-cobord est un i-cocycle : $\operatorname{Im}(\delta_{i-1}) \subset \ker(\delta_i)$.
On définit les groupes de cohomologie

$$H^i(G, M) := \ker(\delta_i)/\operatorname{Im}(\delta_{i-1}).$$

Pour commencer :

$$H^0(G, M) = M^G.$$

Deux résultats fondamentaux en théorie de Galois : pour toute extension galoisienne L de K :

$$H^0\big(\operatorname{Gal}(L/K), L^*\big) = K^*,\ H^1\big(\operatorname{Gal}(L/K), L^*\big) = 1$$

La seconde égalité est Hilbert '90, revue par Chevalley.

Le résultat initial de Hilbert concerne le cas où $\mathrm{Gal}(L/K)$ est un groupe cyclique d'ordre n et engendré par g.

Le résultat initial de Hilbert concerne le cas où $\mathrm{Gal}(L/K)$ est un groupe cyclique d'ordre n et engendré par g.
Dans ce cas, si f est dans $\ker(\delta_1)$, on voit par récurrence que

$$f(g^k) = 1 \cdot f(g) \cdots f(g)^{g^{k-1}}.$$

Le résultat initial de Hilbert concerne le cas où $\mathrm{Gal}(L/K)$ est un groupe cyclique d'ordre n et engendré par g.
Dans ce cas, si f est dans $\ker(\delta_1)$, on voit par récurrence que

$$f(g^k) = 1 \cdot f(g) \cdots f(g)^{g^{k-1}}.$$

En particulier,

$$1 = f(e) = f(g^n) = 1 \cdot f(g) \cdots f(g)^{g^{n-1}}.$$

$$\ker(\delta_1) \simeq \{z \in L^*,\ N_{L/K}(z) = 1\}.$$

Le résultat initial de Hilbert concerne le cas où $\mathrm{Gal}(L/K)$ est un groupe cyclique d'ordre n et engendré par g.
Dans ce cas, si f est dans $\ker(\delta_1)$, on voit par récurrence que

$$f(g^k) = 1 \cdot f(g) \cdots f(g)^{g^{k-1}}.$$

En particulier,

$$1 = f(e) = f(g^n) = 1 \cdot f(g) \cdots f(g)^{g^{n-1}}.$$

$$\ker(\delta_1) \simeq \{z \in L^*,\ N_{L/K}(z) = 1\}.$$

Hilbert '90 s'interprète en :

Le résultat initial de Hilbert concerne le cas où $\mathrm{Gal}(L/K)$ est un groupe cyclique d'ordre n et engendré par g.
Dans ce cas, si f est dans $\ker(\delta_1)$, on voit par récurrence que

$$f(g^k) = 1 \cdot f(g) \cdots f(g)^{g^{k-1}}.$$

En particulier,

$$1 = f(e) = f(g^n) = 1 \cdot f(g) \cdots f(g)^{g^{n-1}}.$$

$$\ker(\delta_1) \simeq \{z \in L^*,\ N_{L/K}(z) = 1\}.$$

Hilbert '90 s'interprète en :

$$N_{L/K}(z) = 1 \Longleftrightarrow z = z_0(z_0^g)^{-1}, \text{pour un } z_0 \text{ de } L^*.$$

Serre :

Serre : « La cohomologie, c'est la différence entre ce que l'on veut et ce que l'on peut. »

Serre : « La cohomologie, c'est la différence entre ce que l'on veut et ce que l'on peut. »

Corollaire

Serre : « La cohomologie, c'est la différence entre ce que l'on veut et ce que l'on peut. »

Corollaire

$$H^i = 1 \Longrightarrow$$

Serre : « La cohomologie, c'est la différence entre ce que l'on veut et ce que l'on peut. »

Corollaire

$$H^i = 1 \Longrightarrow$$ 

Le but ici est d'interpréter des résultats connus par la cohomologie :

Le but ici est d'interpréter des résultats connus par la cohomologie :

- La paramétrisation rationnelle du cercle.

Le but ici est d'interpréter des résultats connus par la cohomologie :

- La paramétrisation rationnelle du cercle.
- Le problème des canards.

Le but ici est d'interpréter des résultats connus par la cohomologie :

- La paramétrisation rationnelle du cercle.
- Le problème des canards.
- Deux matrices réelles $\mathbb{C}$-semblables sont $\mathbb{R}$-semblables (même question pour une extension galoisienne L de K).

Le but ici est d'interpréter des résultats connus par la cohomologie :

• La paramétrisation rationnelle du cercle.

• Le problème des canards.

• Deux matrices réelles $\mathbb{C}$-semblables sont $\mathbb{R}$-semblables (même question pour une extension galoisienne L de K).

• Le théorème de Sylvester (signature d'une matrice symétrique réelle)

Le but ici est d'interpréter des résultats connus par la cohomologie :

• La paramétrisation rationnelle du cercle.

• Le problème des canards.

• Deux matrices réelles $\mathbb{C}$-semblables sont $\mathbb{R}$-semblables (même question pour une extension galoisienne L de K).

• Le théorème de Sylvester (signature d'une matrice symétrique réelle)

• Question : si une représentation $\rho : H \to \mathrm{GL}_n(L)$ vérifie $\mathrm{tr}\,\big(\rho(h)\big) \in K$ pour tout g, peut-on réaliser la représentation sur K ?

Paramétrisation rationnelle du cercle

On applique Hilbert '90 à l'action de Gal$(\mathbb{C}/\mathbb{R})$ sur $\mathbb{C}^*$.

Paramétrisation rationnelle du cercle

On applique Hilbert '90 à l'action de Gal($\mathbb{C}/\mathbb{R}$) sur $\mathbb{C}^*$.

$$z\overline{z} = 1 \Longleftrightarrow z = \frac{z_0}{\overline{z}_0}$$

Paramétrisation rationnelle du cercle

On applique Hilbert '90 à l'action de $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ sur $\mathbb{C}^*$.

$$z\overline{z} = 1 \Longleftrightarrow z = \frac{z_0}{\overline{z}_0}$$

En posant $z_0 := x_0 + iy_0$, il vient

$$z = \frac{x_0^2 - y_0^2}{x_0^2 + y_0^2} + \frac{2x_0y_0}{x_0^2 + y_0^2}i = \frac{1-t^2}{1+t^2} + \frac{2t}{1+t^2}i,\ t \in \mathbb{P}^1(\mathbb{R})$$

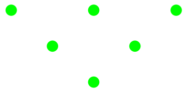
Le problème des canards

Le problème des canards

Une patrouille de canards vole en formation triangulaire. Un chasseur tire sur la patrouille, ce qui a pour effet de diviser la patrouille en deux formations triangulaires égales. Combien y a-t-il de canards ? (on sait qu'il y en a plus que 6)

Le problème des canards

Une patrouille de canards vole en formation triangulaire. Un chasseur tire sur la patrouille, ce qui a pour effet de diviser la patrouille en deux formations triangulaires égales. Combien y a-t-il de canards ? (on sait qu'il y en a plus que 6)



Le problème des canards

Une patrouille de canards vole en formation triangulaire. Un chasseur tire sur la patrouille, ce qui a pour effet de diviser la patrouille en deux formations triangulaires égales. Combien y a-t-il de canards ? (on sait qu'il y en a plus que 6)

Le problème des canards

Une patrouille de canards vole en formation triangulaire. Un chasseur tire sur la patrouille, ce qui a pour effet de diviser la patrouille en deux formations triangulaires égales. Combien y a-t-il de canards ? (on sait qu'il y en a plus que 6)

On veut donc résoudre

$$\frac{n(n+1)}{2} = 2\frac{m(m+1)}{2}.$$

Avec le changement de variables $a := 2n + 1$, $b := 2m + 1$

Avec le changement de variables $a := 2n + 1$, $b := 2m + 1$

$$a^2 - 2b^2 = -1$$

Avec le changement de variables $a := 2n+1,\ b := 2m+1$

$$a^2 - 2b^2 = -1$$

$$a + b\sqrt{2} = (1+\sqrt{2})z,\ z \in \mathbb{N}[\sqrt{2}], N(z) = 1$$

Hilbert '90 : $H^1\big(\,\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}), \mathbb{Q}(\sqrt{2})^*\big) = 1.$

Hilbert '90 : $H^1\big(\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}), \mathbb{Q}(\sqrt{2})^*\big) = 1.$

$$z = a + b\sqrt{2} = \frac{s^2+2t^2}{s^2-2t^2} + \frac{2st}{s^2-2t^2}\sqrt{2},\ s, t \in \mathbb{Q}.$$

Hilbert '90 : $H^1\big(\,\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}), \mathbb{Q}(\sqrt{2})^*\big) = 1.$

$$z = a + b\sqrt{2} = \frac{s^2+2t^2}{s^2-2t^2} + \frac{2st}{s^2-2t^2}\sqrt{2},\ s, t \in \mathbb{Q}.$$

On cherche les solutions entières (et positives !) On peut supposer s et t entiers, premiers entre eux.

Hilbert '90 : $H^1\big(\,\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}), \mathbb{Q}(\sqrt{2})^*\big) = 1.$

$$z = a + b\sqrt{2} = \frac{s^2 + 2t^2}{s^2 - 2t^2} + \frac{2st}{s^2 - 2t^2}\sqrt{2},\ s, t \in \mathbb{Q}.$$

On cherche les solutions entières (et positives !) On peut supposer s et t entiers, premiers entre eux.
Si p premier divise $s^2 - 2t^2$, il divise $s^2 + 2t^2$ et $2st$, donc $2s^2$ et $4t^2$: $p = 2$.

Hilbert '90 : $H^1\big(\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}), \mathbb{Q}(\sqrt{2})^*\big) = 1.$

$$z = a + b\sqrt{2} = \frac{s^2 + 2t^2}{s^2 - 2t^2} + \frac{2st}{s^2 - 2t^2}\sqrt{2},\ s, t \in \mathbb{Q}.$$

On cherche les solutions entières (et positives !) On peut supposer s et t entiers, premiers entre eux.
Si p premier divise $s^2 - 2t^2$, il divise $s^2 + 2t^2$ et $2st$, donc $2s^2$ et $4t^2$: $p = 2$.
On veut éliminer ce cas facheux !

Hilbert '90 : $H^1\big(\operatorname{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}), \mathbb{Q}(\sqrt{2})^*\big) = 1.$

$$z = a + b\sqrt{2} = \frac{s^2+2t^2}{s^2-2t^2} + \frac{2st}{s^2-2t^2}\sqrt{2},\ s, t \in \mathbb{Q}.$$

On cherche les solutions entières (et positives !) On peut supposer s et t entiers, premiers entre eux.
Si p premier divise $s^2 - 2t^2$, il divise $s^2 + 2t^2$ et $2st$, donc $2s^2$ et $4t^2$: $p = 2$.
On veut éliminer ce cas facheux ! Si 2 divise $s^2 - 2t^2$, s est pair, donc t impair.

Hilbert '90 : $H^1\big(\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}), \mathbb{Q}(\sqrt{2})^*\big) = 1.$

$$z = a + b\sqrt{2} = \frac{s^2+2t^2}{s^2-2t^2} + \frac{2st}{s^2-2t^2}\sqrt{2},\ s, t \in \mathbb{Q}.$$

On cherche les solutions entières (et positives !) On peut supposer s et t entiers, premiers entre eux.
Si p premier divise s^2-2t^2, il divise s^2+2t^2 et $2st$, donc $2s^2$ et $4t^2$: $p=2$.
On veut éliminer ce cas facheux ! Si 2 divise s^2-2t^2, s est pair, donc t impair. On a un nouveau changement de variables qui nous amène à

$$\pm z = (s^2+2t^2) + 2st\sqrt{2},\ s^2-2t^2 = \pm 1$$

Par récurrence :

$$z = (1 + \sqrt{2})^k,\ k \text{ impair}$$

Par récurrence :

$$z = (1+\sqrt{2})^k,\ k \text{ impair}$$

$$k = 5,\ n = 20,\ m = 14,\ \frac{n(n+1)}{2} = 210$$

Par récurrence :

$$z = (1+\sqrt{2})^k,\ k \text{ impair}$$

$$k = 5,\ n = 20,\ m = 14,\ \frac{n(n+1)}{2} = 210$$

$$\mathbb{Q}$$

Par récurrence :

$$z = (1+\sqrt{2})^k,\ k \text{ impair}$$

$$k = 5,\ n = 20,\ m = 14,\ \frac{n(n+1)}{2} = 210$$

$$\mathbb{Q} \rightsquigarrow \mathbb{Z}[\frac{1}{2}]$$

Par récurrence :

$$z = (1+\sqrt{2})^k,\ k \text{ impair}$$

$$k = 5,\ n = 20,\ m = 14,\ \frac{n(n+1)}{2} = 210$$

$$\mathbb{Q} \rightsquigarrow \mathbb{Z}[\frac{1}{2}] \dashrightarrow \mathbb{Z}$$

Obstruction de descente- Matrices semblables

Obstruction de descente- Matrices semblables

Soit L une extension galoisienne de K et $G = \mathrm{Gal}(L/K)$.

Obstruction de descente- Matrices semblables

Soit L une extension galoisienne de K et $G = \mathrm{Gal}(L/K)$.
En particulier, G agit sur $\mathcal{M}_n(L)$.

Obstruction de descente- Matrices semblables

Soit L une extension galoisienne de K et $G = \mathrm{Gal}(L/K)$.
En particulier, G agit sur $\mathcal{M}_n(L)$.

Soit $A, B \in \mathcal{M}_n(K)$, $\mathrm{GL}_n(L)$-semblables.

A-t-on A et B $\mathrm{GL}_n(K)$-semblables ?

Obstruction de descente- Matrices semblables

Soit L une extension galoisienne de K et $G = \mathrm{Gal}(L/K)$.
En particulier, G agit sur $\mathcal{M}_n(L)$.

Soit $A, B \in \mathcal{M}_n(K)$, $\mathrm{GL}_n(L)$-semblables.

A-t-on A et B $\mathrm{GL}_n(K)$-semblables ?

On fait agir $\mathrm{GL}_n(L)$ sur A par conjugaison. Il existe $P \in \mathrm{GL}_n(L)$, $P \cdot A := P^{-1}AP = B$.

Obstruction de descente- Matrices semblables

Soit L une extension galoisienne de K et $G = \mathrm{Gal}(L/K)$.
En particulier, G agit sur $\mathcal{M}_n(L)$.

Soit $A, B \in \mathcal{M}_n(K)$, $\mathrm{GL}_n(L)$-semblables.

A-t-on A et B $\mathrm{GL}_n(K)$-semblables ?

On fait agir $\mathrm{GL}_n(L)$ sur A par conjugaison. Il existe $P \in \mathrm{GL}_n(L)$, $P \cdot A := P^{-1}AP = B$. Peut-on trouver P dans $\mathcal{M}_n(K)$?

Obstruction de descente- Matrices semblables

Soit L une extension galoisienne de K et $G = \mathrm{Gal}(L/K)$.
En particulier, G agit sur $\mathcal{M}_n(L)$.

Soit $A, B \in \mathcal{M}_n(K)$, $\mathrm{GL}_n(L)$-semblables.

A-t-on A et B $\mathrm{GL}_n(K)$-semblables ?

On fait agir $\mathrm{GL}_n(L)$ sur A par conjugaison. Il existe $P \in \mathrm{GL}_n(L)$, $P \cdot A := P^{-1}AP = B$. Peut-on trouver P dans $\mathcal{M}_n(K)$?
La matrice P est unique modulo Z_A (le centralisateur de A dans $\mathrm{GL}_n(L)$).

But : Trouver $C \in Z_A$ telle que $CP \in \mathrm{GL}_n(K)$.

But : Trouver $C \in Z_A$ telle que $CP \in \mathrm{GL}_n(K)$.

Condition : $\exists C \in Z_A$, $(PC)^g = PC$, $\forall g \in G$

But : Trouver $C \in Z_A$ telle que $CP \in \mathrm{GL}_n(K)$.

Condition : $\exists C \in Z_A$, $(PC)^g = PC$, $\forall g \in G$,

$$i.e. \;\; P(P^g)^{-1} = C(C^g)^{-1}$$

But : Trouver $C \in Z_A$ telle que $CP \in \mathrm{GL}_n(K)$.

Condition : $\exists C \in Z_A$, $(PC)^g = PC$, $\forall g \in G$,

$$i.e.\ \ P(P^g)^{-1} = C(C^g)^{-1} \in Z_A.$$

But : Trouver $C \in Z_A$ telle que $CP \in \mathrm{GL}_n(K)$.

Condition : $\exists C \in Z_A$, $(PC)^g = PC$, $\forall g \in G$,

$$i.e.\ \ P(P^g)^{-1} = C(C^g)^{-1} \in Z_A.$$

(comme $A \in \mathcal{M}_n(K)$, G agit sur Z_A).

Condition nécessaire : $P(P^g)^{-1} \in Z_A$. Clair, car $A, B \in \mathcal{M}_n(K)$.

Condition nécessaire : $P(P^g)^{-1} \in Z_A$. Clair, car $A, B \in \mathcal{M}_n(K)$.

Réciproquement, $P(P^g)^{-1} \in Z_A$ pour tout g implique $P \cdot A \in \mathcal{M}_n(K)$.

Condition nécessaire : $P(P^g)^{-1} \in Z_A$. Clair, car $A, B \in \mathcal{M}_n(K)$.

Réciproquement, $P(P^g)^{-1} \in Z_A$ pour tout g implique $P \cdot A \in \mathcal{M}_n(K)$.

On considère $f_P : G \to Z_A$, $f_P(g) = P(P^g)^{-1}$, $f_P \in C^1(G, Z_A)$.

Condition nécessaire : $P(P^g)^{-1} \in Z_A$. Clair, car $A, B \in \mathcal{M}_n(K)$.

Réciproquement, $P(P^g)^{-1} \in Z_A$ pour tout g implique $P \cdot A \in \mathcal{M}_n(K)$.

On considère $f_P : G \to Z_A$, $f_P(g) = P(P^g)^{-1}$, $f_P \in C^1(G, Z_A)$.

On voit que $f_P \in \ker(\delta_1)$, on voudrait $f_P \in \mathrm{Im}(\delta_0)$.

Condition nécessaire : $P(P^g)^{-1} \in Z_A$. Clair, car $A, B \in \mathcal{M}_n(K)$.

Réciproquement, $P(P^g)^{-1} \in Z_A$ pour tout g implique $P \cdot A \in \mathcal{M}_n(K)$.

On considère $f_P : G \to Z_A$, $f_P(g) = P(P^g)^{-1}$, $f_P \in C^1(G, Z_A)$.

On voit que $f_P \in \ker(\delta_1)$, on voudrait $f_P \in \mathrm{Im}(\delta_0)$.

Obstruction cohomologique :

$$H^1(G, Z_A) = 1 \Longrightarrow$$

Condition nécessaire : $P(P^g)^{-1} \in Z_A$. Clair, car $A, B \in \mathcal{M}_n(K)$.

Réciproquement, $P(P^g)^{-1} \in Z_A$ pour tout g implique $P \cdot A \in \mathcal{M}_n(K)$.

On considère $f_P : G \to Z_A$, $f_P(g) = P(P^g)^{-1}$, $f_P \in C^1(G, Z_A)$.

On voit que $f_P \in \ker(\delta_1)$, on voudrait $f_P \in \mathrm{Im}(\delta_0)$.

Obstruction cohomologique :

$$H^1(G, Z_A) = 1 \Longrightarrow$$

Obstruction de descente- Matrices congruentes

Obstruction de descente- Matrices congruentes

Avec les mêmes hypothèses sur L et K :

Soit $A, B \in \mathcal{S}_n(K)$, $\mathrm{GL}_n(L)$-congruentes.

A-t-on A et B $\mathrm{GL}_n(K)$-congruentes ?

Obstruction de descente- Matrices congruentes

Avec les mêmes hypothèses sur L et K :

Soit $A, B \in \mathcal{S}_n(K)$, $\mathrm{GL}_n(L)$-congruentes.

A-t-on A et B $\mathrm{GL}_n(K)$-congruentes ?

Le problème est le même, en remplaçant juste Z_A par le groupe orthogonal :

$$O_A := \{Q \in \mathrm{GL}_n(L),\ {}^tQAQ = A\}.$$

Ce changement ne se fait pas sans sacrifice. Le groupe O_A n'est plus abélien !

Ce changement ne se fait pas sans sacrifice. Le groupe O_A n'est plus abélien ! Les δ_i ne sont plus des morphismes.

Ce changement ne se fait pas sans sacrifice. Le groupe O_A n'est plus abélien ! Les δ_i ne sont plus des morphismes.
On doit remplacer le groupe quotient

Ce changement ne se fait pas sans sacrifice. Le groupe O_A n'est plus abélien ! Les δ_i ne sont plus des morphismes.
On doit remplacer le groupe quotient

$$H^1(G, H) = \ker \delta_1 / \operatorname{Im}(\delta_0) = \{[f],\ f \in \ker \delta_1\},\ [f] :\ g \mapsto f(g)h(h^g)^{-1}$$

Ce changement ne se fait pas sans sacrifice. Le groupe O_A n'est plus abélien ! Les δ_i ne sont plus des morphismes.
On doit remplacer le groupe quotient

$$H^1(G, H) = \ker \delta_1 / \operatorname{Im}(\delta_0) = \{[f],\ f \in \ker \delta_1\},\ [f] :\ g \mapsto f(g)h(h^g)^{-1}$$

par l'*ensemble* quotient

$$H^1(G, H) = \ker \delta_1 / H = \{[f],\ f \in \ker \delta_1\},\ [f] :\ g \mapsto hf(g)(h^g)^{-1}$$

On considère l'application

On considère l'application
$\{{}^tPAP,\ P \in \mathrm{GL}_n(L)\} \cap \mathrm{GL}_n(K) \to H^1(G, O_A)$,

On considère l'application
$\{{}^tPAP,\ P \in \mathrm{GL}_n(L)\} \cap \mathrm{GL}_n(K) \to H^1(G, O_A),\ {}^tPAP \mapsto [f_P]$.

On considère l'application
$\{{}^tPAP,\ P \in \mathrm{GL}_n(L)\} \cap \mathrm{GL}_n(K) \to H^1(G, O_A),\ {}^tPAP \mapsto [f_P]$.

Cette application fournit une bijection

$$\left(\mathrm{GL}_n(L) \cdot A \cap \mathrm{GL}_n(K)\right) / \mathrm{GL}_n(K) \simeq H^1(G, O_A).$$

On considère l'application
$\{{}^tPAP,\ P \in \mathrm{GL}_n(L)\} \cap \mathrm{GL}_n(K) \to H^1(G, O_A),\ {}^tPAP \mapsto [f_P]$.

Cette application fournit une bijection

$$\left(\mathrm{GL}_n(L) \cdot A \cap \mathrm{GL}_n(K)\right) / \mathrm{GL}_n(K) \simeq H^1(G, O_A).$$

Idée de la preuve : bien défini et injectif, c'est direct. La surjectivité demande :

On considère l'application
$\{{}^tPAP,\ P \in \mathrm{GL}_n(L)\} \cap \mathrm{GL}_n(K) \to H^1(G, O_A),\ {}^tPAP \mapsto [f_P]$.

Cette application fournit une bijection

$$\big(\mathrm{GL}_n(L) \cdot A \cap \mathrm{GL}_n(K)\big)/\,\mathrm{GL}_n(K) \simeq H^1(G, O_A).$$

Idée de la preuve : bien défini et injectif, c'est direct. La surjectivité demande :

Théorème (Hilbert '90 version ultime)

$$H^1\big(\mathrm{Gal}(L/K), \mathrm{GL}_n(L)\big) = 1.$$

Cas particulier : si $K = \mathbb{R}$, $L = \mathbb{C}$, $A = \mathrm{I}_n$.

Cas particulier : si $K = \mathbb{R}$, $L = \mathbb{C}$, $A = \mathrm{I}_n$. Ici, $H^1(\mathbb{Z}/2\mathbb{Z}, \mathrm{O}_n(\mathbb{C}))$ est l'ensemble des signatures de matrices symétriques réelles inversibles.

Cas particulier : si $K = \mathbb{R}$, $L = \mathbb{C}$, $A = \mathrm{I}_n$. Ici, $H^1(\mathbb{Z}/2\mathbb{Z}, \mathrm{O}_n(\mathbb{C}))$ est l'ensemble des signatures de matrices symétriques réelles inversibles.

$$H^1(\mathbb{Z}/2\mathbb{Z}, \mathrm{O}_n(\mathbb{C})) = \{1, -1\}^n / \mathfrak{S}_n$$

Obstruction de descente-théorie des représentations

Obstruction de descente-théorie des représentations

Avec les mêmes hypothèses sur L et K :

Soit H un groupe fini, $\rho : H \to \mathrm{GL}_n(L)$ une représentation. Cette représentation se réalise-t-elle sur K ?

Obstruction de descente-théorie des représentations

Avec les mêmes hypothèses sur L et K :

Soit H un groupe fini, $\rho : H \to \mathrm{GL}_n(L)$ une représentation. Cette représentation se réalise-t-elle sur K ?

On cherche une matrice B de $\mathrm{GL}_n(L)$ telle que

$$B^{-1}\rho B \, : \, H \to \mathrm{GL}_n(K).$$

Obstruction de descente-théorie des représentations

Avec les mêmes hypothèses sur L et K :

Soit H un groupe fini, $\rho : H \to \mathrm{GL}_n(L)$ une représentation. Cette représentation se réalise-t-elle sur K ?

On cherche une matrice B de $\mathrm{GL}_n(L)$ telle que

$$B^{-1}\rho B \,:\, H \to \mathrm{GL}_n(K).$$

Condition nécessaire : $\mathrm{tr}\left(\rho(h)\right) \in K$ pour tout h de H. Est-ce suffisant ?

Obstruction de descente-théorie des représentations

Avec les mêmes hypothèses sur L et K :

Soit H un groupe fini, $\rho : H \to \mathrm{GL}_n(L)$ une représentation. Cette représentation se réalise-t-elle sur K ?

On cherche une matrice B de $\mathrm{GL}_n(L)$ telle que

$$B^{-1}\rho B \; : \; H \to \mathrm{GL}_n(K).$$

Condition nécessaire : $\mathrm{tr}\left(\rho(h)\right) \in K$ pour tout h de H. Est-ce suffisant ?
Supposons $\mathrm{tr}\left(\rho(h)\right) \in K$ pour tout h de H et ρ absolument simple. Cela implique (lemme de Schur) que le commutant de $\mathrm{Im}(\rho)$ est constitué des homothéties de $\mathrm{GL}_n(L)$.

On définit ρ^g par $\rho^g(h) = (\rho)(h)^g$.

On définit ρ^g par $\rho^g(h) = (\rho)(h)^g$.

- Première constatation :

On définit ρ^g par $\rho^g(h) = (\rho)(h)^g$.

- Première constatation : $\mathrm{tr}(\rho^g(h)) = \mathrm{tr}\left(\rho(h)\right)^g = \mathrm{tr}(\rho(h))$.

On définit ρ^g par $\rho^g(h) = (\rho)(h)^g$.

• Première constatation : $\mathrm{tr}(\rho^g(h)) = \mathrm{tr}\left(\rho(h)\right)^g = \mathrm{tr}(\rho(h))$.
Comme le caractère caractérise, ρ^g et ρ sont deux représentations isomorphes :

On définit ρ^g par $\rho^g(h) = (\rho)(h)^g$.

• Première constatation : $\mathrm{tr}(\rho^g(h)) = \mathrm{tr}\left(\rho(h)\right)^g = \mathrm{tr}(\rho(h))$.
Comme le caractère caractérise, ρ^g et ρ sont deux représentations isomorphes :

$$\exists A_g \in \mathrm{GL}_n(L),\ A_g \cdot \rho := A_g^{-1} \rho A_g = \rho^g$$

On définit ρ^g par $\rho^g(h) = (\rho)(h)^g$.

• Première constatation : $\mathrm{tr}(\rho^g(h)) = \mathrm{tr}\left(\rho(h)\right)^g = \mathrm{tr}(\rho(h))$.
Comme le caractère caractérise, ρ^g et ρ sont deux représentations isomorphes :

$$\exists A_g \in \mathrm{GL}_n(L),\ A_g \cdot \rho := A_g^{-1} \rho A_g = \rho^g$$

Si on savait que $g \mapsto A_g$ est un 1-cocycle, alors $A_g = (B^g)^{-1}B$ par Hilbert '90

On définit ρ^g par $\rho^g(h) = (\rho)(h)^g$.

• Première constatation : $\mathrm{tr}(\rho^g(h)) = \mathrm{tr}\left(\rho(h)\right)^g = \mathrm{tr}(\rho(h))$.
Comme le caractère caractérise, ρ^g et ρ sont deux représentations isomorphes :

$$\exists A_g \in \mathrm{GL}_n(L),\ A_g \cdot \rho := A_g^{-1} \rho A_g = \rho^g$$

Si on savait que $g \mapsto A_g$ est un 1-cocycle, alors $A_g = (B^g)^{-1} B$ par Hilbert '90 et donc, $B^g \cdot \rho^g = B \cdot \rho$ pour tout g.

On définit ρ^g par $\rho^g(h) = (\rho)(h)^g$.

• Première constatation : $\mathrm{tr}(\rho^g(h)) = \mathrm{tr}\left(\rho(h)\right)^g = \mathrm{tr}(\rho(h))$.
Comme le caractère caractérise, ρ^g et ρ sont deux représentations isomorphes :

$$\exists A_g \in \mathrm{GL}_n(L),\ A_g \cdot \rho := A_g^{-1} \rho A_g = \rho^g$$

Si on savait que $g \mapsto A_g$ est un 1-cocycle, alors $A_g = (B^g)^{-1}B$ par Hilbert '90 et donc, $B^g \cdot \rho^g = B \cdot \rho$ pour tout g. On aurait donc bien $B^{-1}\rho B$ dans $\mathrm{GL}_n(K)$.

- Deuxième constatation :

- Deuxième constatation :

$$A_{gg'} \cdot \rho = \rho^{gg'} = \left(A_{g'} \cdot \rho\right)^{g} = \left(A_{g'^g} A_g\right) \cdot \rho$$

- Deuxième constatation :

$$A_{gg'} \cdot \rho = \rho^{gg'} = \left(A_{g'} \cdot \rho\right)^g = \left(A_{g'^g} A_g\right) \cdot \rho$$

Si on avait $A_{gg'} = \left(A_{g'}^g A_g\right)$, alors, $g \mapsto A_g$ serait un 1-cocycle

- Deuxième constatation :

$$A_{gg'} \cdot \rho = \rho^{gg'} = \left(A_{g'} \cdot \rho\right)^{g} = \left(A_{g'^{g}} A_{g}\right) \cdot \rho$$

Si on avait $A_{gg'} = \left(A_{g'}^{g} A_{g}\right)$, alors, $g \mapsto A_g$ serait un 1-cocycle
Or, ils diffèrent d'une homothétie. On note donc

$$a_{g,g'} := \left(A_{g'}^{g}\right)^{-1} A_{gg'} A_{g}^{-1} \in L^{*}$$

- Deuxième constatation :

$$A_{gg'} \cdot \rho = \rho^{gg'} = \left(A_{g'} \cdot \rho\right)^g = \left(A_{g'^g} A_g\right) \cdot \rho$$

Si on avait $A_{gg'} = \left(A_{g'}^g A_g\right)$, alors, $g \mapsto A_g$ serait un 1-cocycle
Or, ils diffèrent d'une homothétie. On note donc

$$a_{g,g'} := \left(A_{g'}^g\right)^{-1} A_{gg'} A_g^{-1} \in L^*$$

- Troisième constatation :

$$a : \; G^2 \to L^*, \; (g, g') \to a_{g,g'}$$

est dans $\ker \delta_2$.

Supposons que $H^2(G, L^*) = 1$.

Supposons que $H^2(G, L^*) = 1$.
Dans ce cas, la réponse est positive :

Supposons que $H^2(G, L^*) = 1$.
Dans ce cas, la réponse est positive : l'élément $[a_{g,g'}]$ provient de b_g, puis $b_g^{-1}A_g$ est un 1-cocycle à valeurs dans $\mathrm{GL}_n(L)$,

Supposons que $H^2(G, L^*) = 1$.
Dans ce cas, la réponse est positive : l'élément $[a_{g,g'}]$ provient de b_g, puis $b_g^{-1}A_g$ est un 1-cocycle à valeurs dans $\mathrm{GL}_n(L)$, donc, par Hilbert '90, on obtient la matrice B cherchée : $b_g^{-1}A_g = (B^g)^{-1}B$.

Supposons que $H^2(G, L^*) = 1$.
Dans ce cas, la réponse est positive : l'élément $[a_{g,g'}]$ provient de b_g, puis $b_g^{-1}A_g$ est un 1-cocycle à valeurs dans $\mathrm{GL}_n(L)$, donc, par Hilbert '90, on obtient la matrice B cherchée : $b_g^{-1}A_g = (B^g)^{-1}B$.

Exemples

Supposons que $H^2(G, L^*) = 1$.
Dans ce cas, la réponse est positive : l'élément $[a_{g,g'}]$ provient de b_g, puis $b_g^{-1}A_g$ est un 1-cocycle à valeurs dans $\mathrm{GL}_n(L)$, donc, par Hilbert '90, on obtient la matrice B cherchée : $b_g^{-1}A_g = (B^g)^{-1}B$.

Exemples

- $H^2(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^*) = 1$.

Supposons que $H^2(G, L^*) = 1$.
Dans ce cas, la réponse est positive : l'élément $[a_{g,g'}]$ provient de b_g, puis $b_g^{-1}A_g$ est un 1-cocycle à valeurs dans $\mathrm{GL}_n(L)$, donc, par Hilbert '90, on obtient la matrice B cherchée : $b_g^{-1}A_g = (B^g)^{-1}B$.

Exemples

- $H^2(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^*) = 1$.
- $H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^*) = \{1, -1\}$. (Il n'y a pas de Hilbert '91 !)

Epilogue

Epilogue

• Problème de descente galoisienne. On peut considérer ces problèmes de descente en termes d'un foncteur F qui associe à une extension de K un groupe-anneau-corps-algèbre... et un schéma en groupe G agissant sur F. Si M et N dans $F(K)$ sont tels que M_L et N_L se trouvent dans la même $G(L)$-orbite, a-t-on M et N dans la même $G(K)$-orbite ?

Epilogue

• Problème de descente galoisienne. On peut considérer ces problèmes de descente en termes d'un foncteur F qui associe à une extension de K un groupe-anneau-corps-algèbre... et un schéma en groupe G agissant sur F. Si M et N dans $F(K)$ sont tels que M_L et N_L se trouvent dans la même $G(L)$-orbite, a-t-on M et N dans la même $G(K)$-orbite ?

• Y a-t-il une cohomologie qui permette de voir l'obstruction de descente entre le corps de nombres $(\mathbb{Q}(\sqrt{2}))$ et le groupe des unités de l'anneau $(\mathbb{Z}[\sqrt{2}]^*)$?

• On sait qu'une représentation ρ sur $\mathbb{C}$ dont le caractère est réel peut être se réaliser sur $\mathbb{R}$ ou pas selon si

$$\frac{1}{|H|}\sum_{h\in H}\rho(h^2) = \pm 1$$

• On sait qu'une représentation ρ sur $\mathbb{C}$ dont le caractère est réel peut être se réaliser sur $\mathbb{R}$ ou pas selon si

$$\frac{1}{|H|}\sum_{h\in H}\rho(h^2) = \pm 1$$

Y a-t-il, en général, une formule simple qui donne la classe de ρ (sur L, mais dont le caractère est dans K) dans le groupe de Brauer de K ?