Théorème de Hilbert 90

BENSAID Mohamed

December 7, 2024

Boîte à outils

Lemma 1 (de Dedekind)**.** *Soit $\sigma_1, ..., \sigma_n$ des automorphismes distincts sur un corps E, alors*

$$\sum_{i=1}^{n} \lambda_i \sigma_i = 0 \Longrightarrow \lambda_i = 0$$

Proof. On raisonne par l'absurde, supposons qu'il existe des λ_i qui ne sont pas nuls, quitte à réordonner, r l'entier minimal tel que $\lambda_1, ..., \lambda_r$ non nuls.

Prenons $z \in E$ tel que $\sigma_1(z) \neq \sigma_2(z)$, alors par hypothèse pour tout $x \in E$ on a

$$\sum_{i=1}^{r} \lambda_i \sigma_i(x) = 0$$

et donc

$$\sum_{i=1}^{r} \lambda_i \sigma_i(xz) = \sum_{i}^{r} \lambda_i \sigma_i(x)\sigma_i(z) = 0$$

Ansi

$$\sum_{i=2}^{r} \lambda_i (\sigma_i(z) - \sigma_1(z))\sigma_i(x) = 0$$

Ce qui contredit la minimalité de r. □

Definition 2 (Extention normale)**.** *On dit que l'extention $K \subset E$ est normale (ou encore quasi-galoisienne) si elle est algébrique et pour tout $x \in E$, le polynôme minimal de x a toutes ses racines dans E.*

Definition 3 (Extention séparable)**.** *On dit qu' un élément $x \in E$ est séparable si son polynôme minimal (sur K) n'a que des racines simples.*

Dans la suite, on suppose que l'extention E/K est finie

Definition 4. *On dit que E/K est une extention galoissiene si elle est séparable et normale*

Theorem 5. *Si E/K est une extention finie galoissiene on a $\#Gal(E/K) = [E, K]$*

Une petite introduction de la Cohomologie de Groupe

Dans cette courte section on discutera seulement de la définition de la cohomologie de groupe, mais nous interessant just a la premier cohomologie.

Definition 6. *Soit G un groupe, un G-module M est un groupe abelien avec l'action de G sur M. Notons $g \cdot m$ notre action.*

Remark 1. *Les axioms de l'action de G sur M dépendent de loi de groupes choisie. En effet, notons $(G, *)$ et $(M, \times)$*

$$1 \cdot m = m$$

$$(g_1 * g_2) \cdot m = g_1 \cdot (g_2 \cdot m)$$

$$g \cdot (m \times n) = (g \cdot m) \times (g \cdot n)$$

Pour donner une définition générale des groupes de cohomologie d'un groupe fini $(G, *)$. On considère un groupe commutatif M, noté multiplicativement, muni d'une action de G (c'est-à-dire, un G–module M)

La cohomologie de G à coefficents dans M est définie à l'aide des cochaines complexes;

$$C^0(G, M) = M$$

et pour tout $n \geq 1$

$$C^n(G, M) = \{f : G \times ... \times G \longrightarrow M\}$$

Definition 7. *La formule*

$$d_n f(g_1, ...g_{n+1}) = (g_1 \cdot f(g_2, ..., g_{n+1})) \prod_{i=1}^{n} f^{(-1)^i}(g_1, ..., g_i * g_{i+1}, ...g_{n+1}) f^{(-1)^{n+1}}(g_1, ..., g_n)$$

définit un morphisme $d_n : C^n \longrightarrow C^{n+1}$

Proposition 8. *On a pour tout $n \geq 2$,*

$$d_n \circ d_{n-1} = 0$$

Proof. Laissée au lecteur, c'est un calcul sophistiqué □

Definition 9 (n-cocycle)**.** *Soit M un G-module, un n-cocycle est un élément de $Z^n(G, M) := Ker(d_n)$*

Definition 10 (n-Cobord)**.** *Un n-cobord de G sur M est un élément de $B^n(G, M) := Im(d_{n-1})$*

Remark 2. *Par la proposition 8, on en déduit que $B^n \subset Z^n$*

Definition 11. *On definit le n-ieme groupe de cohomologie par*

$$H^n(G, M) = Z^n(G, M)/B^n(G, M)$$

Pour $n = 0$, $H^0(G, M) = Ker(d_0) = \{m \in M | g \cdot m = m\} = M^G$.

Example 12. *Pour $n = 1$, on obtient*

$$Z^1(G, M) = \{f : G \longrightarrow M | f(g_1 * g_2) = (g_1 \cdot f(g_2)) f(g_1)\}$$

$$B^1(G, M) = \{f : G \longrightarrow M | \exists m \in M, f(g) = (g \cdot m)m^{-1}, \forall g \in G\}$$

Autour des Traces et Normes

Definition 13. *Soit E/K une extention de corps, donc E peut-être vue comme un K-espace vectoriel. Soit alors $a \in E$, on définit l'application linéaire L_a par $L_a(x) = ax$ pour tout $x \in E$.*

Norme *La norme de a pour cette extention est $N_{E/K}(a) = \det(\mathrm{L_a})$*

Trace *La trace de a pour cette extention est $Tr_{E/K}(a) = \mathrm{Tr}(L_a)$*

Example 14. *Pour bien comprendre ces notation nous donnrons un exemple sur les extentions quadratiques de corpe de nombres. Soit d un rationnel qui n'est pas un carrée parfait dans $\mathbb{Q}$. On sait que $\{1, \sqrt{d}\}$ est une base de $\mathbb{Q}(\sqrt{d})$.*

Calcoulons la norme et la trace de $z = a + b\sqrt{d}$ pour cette extention.

On souhaite trouver une représentation matricielle de l'application linéaire. L_z.

$L_z(1) = z = a + b\sqrt{d}$ et $L_z(\sqrt{d}) = \sqrt{d}z = \sqrt{d}a + db$

Donc la matrice de L_z dans la base canonique est

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix}$$

Donc la trace $Tr(L_z) = 2a$ et la norme est $det(L_z) = a^2 - db^2$.

Theorem 15. *Soit E/K une extention galoissiene (finie) de groupe de galois G alors*

$$N_{E/K}(x) = \prod_{\sigma \in G} \sigma(x)$$

et

$$Tr_{E/K}(x) = \sum_{\sigma \in G} \sigma(x)$$

Proof. Admis. □

Théorème de Hilbert 90

Dans cette section, on va travailler sur les deux groupes $(Gal(E/K), \circ)$ et $(E^\times, \cdot)$ où E/K est une extention galoissiene finie. ($E^\times$ a une strecture de $Gal(E/K)$-module)

Theorem 16 (Hilbert (Noether))**.** *Soit E/K une extention galoissiene finie alors*

$$H^1(Gal(E/K), E^\times) = 1$$

Proof. Il suffit de prouver que $Z^1(Gal(E/K), E^\times) \subset B^1(Gal(E/K), E^\times)$. Notons $G := Gal(E/K)$.

Soit $\phi \in Z^1(G, E^\times)$, considerons l'application

$$\sum_{\mu \in G} \phi(\mu)\mu : E \longrightarrow E$$

l'application est bien definie, de plus elle est non nulle par le lemme 1

Il existe alors $x \in E$ tel que

$$y := \sum_{\mu \in G} \phi(\mu)\mu(x) \neq 0$$

Soit $\sigma \in G$

$$\begin{aligned}\sigma(y) &= \sum_{\mu \in G} \sigma(\phi(\mu))\sigma\mu(x) \\ &= \sum_{\mu \in G} \phi^{-1}(\sigma)\phi(\sigma\mu)\sigma\mu(x) \\ &= \phi^{-1}(\sigma)y\end{aligned}$$

Ce qui se traduit par $\phi(\sigma) = \sigma(b)b^{-1}$ où $b = y^{-1}$ □

Theorem 17 (Hilbert original)**.** *Soit E/K une extension finie galoissiene et son groupe de galois G est cyclique de degré n, de générateur σ. Soit N la norme de E sur K, alors pour tout $x \in E$,*

$$N(y) = 1 \Longleftrightarrow \exists x \in E \ y = x\sigma^{-1}(x)$$

Proof. On pourrait prouver ce théorème directement en utilisant le lemme de Dedekind mais nous nous focalisons sur sa preuve par le biais du théorème précedent.

Il est évidant de ramarquee que E a une structure de G-module.

On souhiate reformuler le théorème 19 afin d'appliquer le théorème 17. Pour cela introduisons le **sous-groupe** $F = \{x\sigma^{-1}(x) | x \in K^\times\}$ de $K^\times$

Et nous rappelons que la norme de l'extention E/K est difine dans ce cas par

$$N(x) = \prod_{i=1}^{i-1} \sigma^i(x)$$

Reformulation du théorème le théorème est vrai si $F \subset Ker(N)$ et $Ker(N)/F = H^1(G, E^\times)$ (donc par le théorème 17 on a le résultat souhaité).

Vérification $F \subset Ker(N)$. Soit $x \in E^\times$

$$N(x\sigma^{-1}(x)) = \prod_{i=0}^{n-1} \sigma^i(x) \prod_{i=0}^{n-1} \sigma^{i-1}(x) = 1$$

Vérification de $Ker(N)/F = H^1(G, E^\times)$. Soit $g \in Z^1(G, E^\times)$, puisque G est cyclique d'ordre n alors

$$g(\sigma^k) = \prod_{i=0}^{n-1} \sigma^i(g(\sigma))$$

$$\begin{aligned} \psi : Ker(N) &\longrightarrow Z^1(G, E^\times) \\ a &\longrightarrow g_a(\sigma^i) = \prod_{i=0}^{n-1} \sigma^i(g(\sigma)) \end{aligned}$$

cette application est un isomorphisme grâce au fait qu'un élément de $Z^1(G, E^\times)$ est complétement detreminé par son image par σ. On peut également prouver que $\psi(F) = B^1(G, E^\times)$ ce qui affirme le résultat.

□

Application : Soit K un corps et n un entier premier à sa caracteristique.

On suppose que K contient une racine primitive n-ième de l'unité. Alors

Soit E une extension galoissiene finie et son groupe de galois G cyclique d'ordre n alors $\exists x \in E$ tel que $E = K(x)$ est que x est une racine de $X^n - a$ pour certain $a \in E$.

Soit y une racine primitive n-ième de l'unité dans K, et on pose par hypothèse que $G =< \sigma >$, par la formule de trace on obtient $N(y^{-1}) = y^{-n} = 1$ donc par le théorème de Hilbert précédent on en déduit qu'il existe $x \in K$ tel que $\sigma(x) = yx$. Comme $x \in K$,$\sigma(x) = y^i x$. Ainsi les éléments $y^i x$ sont n-conjugués distincts de x sur K, d'où $[K(x), K] = n$. Mais comme $[E, K] = n$ on a donc $E = K(x)$. D'autre part $\sigma(x^n) = x^n$ et donc n est invariant par σ donc par toutes les puissances de σ et est donc un élément de F . Donc $x^n = a \in K$.