Tours de Hilbert

1 Contexte général, notations

Soit K un corps de nombres, ie une extension finie de $\mathbb{Q}$.
$\mathcal{O}_K$ l'anneau des entiers de K.
$Pl(K)$ l'ensemble des places de K, qu'on décompose en places infinies $Pl_\infty(K)$ et places finies $Pl_0(K)$. $Pl_\infty(K)$ est composée de $r_1(K)$ places réelles $Pl_\mathbb{R}(K)$ et $r_2(K)$ places complexes $Pl_\mathbb{C}(K)$.
Soit $\mathfrak{p}$ une place de K, $L|K$ une extension finie galoisienne. On regarde le comportement de $\mathfrak{p}$ prolongé à L.

- Premier cas: $\mathfrak{p} \in Pl_\infty(K)$. Si $\mathfrak{p}$ est complexe, alors $\mathfrak{p}$ reste complexe (inerte).
  Si $\mathfrak{p}$ est réelle, alors $\mathfrak{p}$ peut soit se complexifier (on dit alors qu'elle se ramifie), soit rester réelle (inerte).
- Second cas: $\mathfrak{p} \in Pl_0(K)$. Alors $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^e ... \mathfrak{P}_g^e$. On dit que $\mathfrak{p}$ est non ramifié si $e = 1$.

On s'intéresse à l'extension de K **abélienne** non ramifiée partout en $Pl(K)$ maximale.

1.1 Définition:

On appelle **corps de Hilbert** de K, noté H(K), l'extension de K **abélienne** non ramifiée partout en $Pl(K)$ maximale.

1.2 Exemples:

1)Sur $\mathbb{Q}$, si $K \neq \mathbb{Q}$, alors $|d_K| \neq 1$ (car $|d_K|^{1/2} \geq \frac{n^n}{n!}(\frac{\pi}{4})^{n/2}$) donc par la théorie algébrique des nombres, pour toute extension non triviale de $\mathbb{Q}$ il existe une place (finie) de $\mathbb{Q}$ qui ramifie, de sorte que $H(\mathbb{Q}) = \mathbb{Q}$.
2)Si $K = \mathbb{Q}(\sqrt{-31})$ alors $H(K) = K(\vartheta)$ avec ϑ racine de $X^3 + X - 1$.

2 Théorie du corps de classes

L'explication des exemples ci dessus nous est donnée par la théorie du corps de classes.
Cette théorie essaie de (et arrive à) décrire toutes les extensions abéliennes K en termes d'arithmétique de K, et de décrire la ramification des places dans de telles extensions.

2.1 Définitions:

Un **module** $\mathfrak{M}$ est un produit formel

$$\mathfrak{M} = \prod_{\mathfrak{p} \in Pl(K)} \mathfrak{p}^{m(\mathfrak{p})}$$

où

- $m(\mathfrak{p}) \in \mathbb{N} \ \ \forall \mathfrak{p}, \ \ m(\mathfrak{p}) = 0$ pour presque tout $\mathfrak{p}$.
- $m(\mathfrak{p}) = 0$ ou 1 si $\mathfrak{p} \in Pl_{\mathbb{R}}(K)$.
- $m(\mathfrak{p}) = 0$ si $\mathfrak{p} \in Pl_{\mathbb{C}}(K)$.

On dit que $\mathfrak{p} \in Pl(K)$ divise $\mathfrak{M}$ si $m(\mathfrak{p}) > 0$.
On note $S(\mathfrak{M})$ l'ensemble des places de K divisant $\mathfrak{M}$.
Etant donné un module $\mathfrak{M}$ on pose

$K_{\mathfrak{M}} = \{a \in^{\times} |ord_{\mathfrak{p}}(a - 1) \geq m(\mathfrak{p})$ si $\mathfrak{p}$ divise $\mathfrak{M}$, $\mathfrak{p}$ finie, $a_{\mathfrak{p}} > 0$ si $\mathfrak{p}$ est réelle divisant $\mathfrak{M}\}$.

Si $a \in K_{\mathfrak{M}}$, on a (a) (=l'idéal engendré par a) $\in I^{S(\mathfrak{M})}$ ={idéaux premiers aux idéaux de $S(\mathfrak{M})$}.
On appelle **groupe des classes de rayons modulo** $\mathfrak{M}$ le groupe

$$C_{\mathfrak{M}} = I^{S(\mathfrak{M})} / \iota(K_{\mathfrak{M}}).$$

2.2 Théorèmes: (Loi de réciprocité, existence)

Soit $L|K$ une extension abélienne finie de K et soit S l'ensemble des premiers de K qui ramifient dans L. Alors il existe un module $\mathfrak{M}$ avec $S = S(\mathfrak{M})$, tel que l'**application d'Artin** $\psi : I^S \to Gal(L|K)$ définit par passage au quotient un isomorphisme

$$I^S \Big/ \iota(K_{\mathfrak{M}}).Nm_{L|K}(I_L^{S(\mathfrak{M})}) \simeq Gal(L|K).$$

Réciproquement, étant donné un module $\mathfrak{M}$, pour tout sous-groupe $\iota(K_{\mathfrak{M}}) \subset H \subset I^{S(\mathfrak{M})}$ il existe une extension abélienne $L|K$ telle que $H = \iota(K_{\mathfrak{M}}) Nm_{L|K} I_L^{S(\mathfrak{M})}$.

2.3 Remarque:

Par construction de l'application d'Artin, le degré résiduel $f(\mathfrak{P}|p) = ordre(\mathfrak{p})$ dans $I^{S(\mathfrak{M})}/H$.
En particulier, $\mathfrak{p}$ est totalement décomposé si et seulement si $f(\mathfrak{P}|\mathfrak{p}) = 1 \iff \mathfrak{p} \in H = Ker(Artin)$.

2.4 Exemple:

$\mathfrak{M} = 1 \Rightarrow C_{\mathfrak{M}} = Cl(K)$ et $H = \iota(K_{\mathfrak{M}}) \Rightarrow L|K = H(K)$.

2.5 Théorème: (Idéal principal)

Tout idéal de K devient principal dans $H(K)$.

En effet, on a le diagramme commutatif suivant (on a posé $K_1 = H(K)$ et $K_2 = H(H(K))$).

$$\begin{tikzcd} C_K \arrow[r, "\sim"] \arrow[d, "can"'] & Gal(K_1|K) \arrow[d, "V"] \\ C_{K_1} \arrow[r, "\sim"'] & Gal(K_2|K_1) \end{tikzcd}$$

Or on peut montrer que V est le transfert et que $V : G^{ab} \to H^{ab} = [G,G]^{ab} = 0$. Attention, cela ne signifie pas que $Cl(K_1) = 0$.

3 Position du problème

On pose $K_0 = K,\ K_1 = H(K), ..., K_n = H(K_{n-1})$.

3.1 Question:

Existe-t'il des corps K pour lesquels (K_n) est une suite infinie?

3.2 Exemples:

- Pour $K = \mathbb{Q}$ la suite stationne.
- Pour $K = \mathbb{Q}(i)$ la suite stationne.

3.3 Remarque:

Pour des raisons pratiques, on ne va pas étudier $H(K)$ mais $H_p(K)$ qui est la p-extension abélienne non ramifiée maximale de K.

4 Rappels de cohomologie galoisienne

4.1 Définitions:

Soit p un nombre premier, et G un groupe profini, disons pro-p de type fini.
On appelle **p-dimension cohomologique** de G et on note $cd_p(G)$ la borne inférieure des entiers n vérifiant "Pour tout G-module discret de torsion A, et pour tout $q > n$, $H^q(G, A) = 0$".
On appelle **p-dimension cohomologique stricte** de G et on note $scd_p(G)$ la borne inférieure des entiers n vérifiant "Pour tout G-module discret A, et pour tout $q > n$, $H^q(G, A) = 0$".
Par dévissage et décalage de dimension, on peut se ramener au cas où A est un G-module discret simple annulé par p et $q = n + 1$. Or

4.2 Lemme:

Un tel module est isomorphe à $\mathbb{Z}/p$ avec action triviale.

En effet, on commence par montrer la finitude d'un tel module:$\{ga, a \in G\}$ est fini pour tout $a \in A$ puisque $a \in A^U$ pour un certain sous groupe ouvert distingué U de G de sorte que $|\{ga\}| \leq |G/U|$: fini.
Dès lors par finitude, $A = A^U \neq 0$. pour un certain sous-groupe ouvert distingué U de G. On a donc $H^0(G/U, A^U) = A^G \neq 0$ puisqu'un p-groupe agit sans points fixes sur un module non trivial. Par simplicité, $A^G = A$, puis encore par simplicité, $A = \mathbb{Z}/p$.

Bref, $cd_p(G) \leq n \iff H^{n+1}(G, \mathbb{Z}/p) = 0$.

4.3 Notations:

On posera

$$H^n(G) = H^n(G, \mathbb{Z}/p)$$

et

$$G^* = G/G^p[G;G] :$$

le plus grand quotient abélien d'exposant p de G, de sorte que

$$H^1(G) = Hom(F, \mathbb{Z}/p) = Hom(G^*, \mathbb{Q}/\mathbb{Z}).$$

4.4 Définition:

Un **système générateur** $S \subset G$ est un ensemble qui engendre topologiquement le groupe G.

4.5 Proposition:

$S \subset G$ engendre $G \iff \overline{S}$ (ensemble des classes des éléments de S modulo $G^p[G,G]$) engendre G^*.
S est minimal (en tant que générateur de G) $\iff \overline{S}$ est minimal (en tant que générateur de G^*).
Tout système minimal de générateurs de G a pour cardinal $d(G) = \dim_p H^1(G)$.

En effet, soit $H = \overline{< S >}$. On a $H \hookrightarrow G$ est surjective $\iff H^1(G) \to H^1(H)$ est injectif $\iff H^* \to G^*$ est surjectif.

4.6 Définition:

$N \lhd G$. Un système de générateurs de N en tant que sous-groupe normal de G est un sous ensemble $S \subset N$ tel que $\overline{<< S >>} = N$.

4.7 Exemple:

Si $N = G$ alors on sait par le théorème précédent que S engendre G en tant que sous groupe normal si et seulement si S engendre G.

4.8 Proposition:

Soit $N \lhd G$ et $S \subset N$ et $H = \overline{< S >}$.
Alors $res : H^1(N)^G \to H^1(H)$ est injectif $\iff N = \overline{<< S >>}$.

4.9 Corollaire:

Soit $N \lhd G$ et $S \subset N$. Alors $\overline{<< S >>} = N \iff \overline{S}$ (ensemble des classes de S modulo $N^p[G, N]$) engendre $N/N^p[G, N]$.
En particulier, S est minimale $\iff \overline{S}$ l'est et dans ce cas, $|S| = \dim_p H^1(N)^G$.

En effet, on pose $H = \overline{< S >} \subset N$. On a

$H^1(N)^G = Hom(N, \mathbb{Z}/p)^G = Hom(N/N^p[G, N], \mathbb{Z}/p) = Hom(N/N^p[G, N], Q_p/\mathbb{Z}_p)$

de sorte que

$H \hookrightarrow N$ surjectif $\iff H^1(N)^G \to H^1(H)$ injectif $\iff H^* \to N/N^p[G, N]$ surjectif .

4.10 Définition:

Soit S un système de générateur de G, $F = F_S$ le pro-p-groupe groupe libre sur S. On a une suite exacte

$$1 \to R \to F \to G \to 1.$$

Un **système de relations** de G relativement à S est un ensemble $\mathcal{R}$ de générateurs de R en tant que sous-groupe normal de F.

4.11 Proposition:

Soit S un système de générateurs de G.
Alors un système fini de relations R relativement à S existe $\iff H^2(G)$ est fini et alors $|S| - |\mathcal{R}| = \dim_p H^1(G) - \dim_p H^2(G)$.

En effet, par la proposition précédente, $|\mathcal{R}| = \dim_p H^1(R)^F = \dim_p H^1(R)^G$. Le résultat découle facilement de la suite exacte

$$0 \to H^1(G) \to H^1(F) \to H^1(R)^G \to H^2(G) \to H^2(F) = 0.$$

En particulier, le cardinal d'un système minimal de relations dépend seulement de $|S|$ et si S est minimal, $|\mathcal{R}|$ s'appelle le nombre de relations de G, noté $r(G) = \dim H^2(G)$.

5 Inégalité de Golod-Shafarevitch

5.1 Lemme:

Soit $L|K$ une extension galoisienne non ramifiée dont le groupe G est un p-groupe fini. On suppose que L n'a aucune extension cyclique non ramifiée de degré p.
Alors $r(G) - n(G) \leq r_1(K) + r_2(K)$.

En effet, par la théorie du corps de classes, les hypothèses se traduisent par le fait que L a un groupe de classes d'idéaux dont la p-partie est triviale. Donc $\hat{H}^q(G, Cl(L)) = 0$ pour $q > 0$. De plus, puisque $L|K$ est non ramifiée, le sous-groupe U_L des idèles unités de L est cohomologiquement triviale, et donc $\hat{H}^q(G, U_L) = 0$ si $q > 0$. En appliquant les suites exactes de cohomologie associées à $0 \to U_L/E_K \to C_L \to Cl(L) \to 0$ et $0 \to E_L \to U_L \to U_L/E_L \to 0$ on en déduit que $\hat{H}^q(G, C_L) = \hat{H}^{q+1}(G, E_K)$.
D'autre part, par la théorie du corps de classes, $\hat{H}^q(G, C_L) = \hat{H}^{q-2}(G, \mathbb{Z})$. On en déduit, en prenant $q = -1$:

$$\hat{H}^{-3}(G, \mathbb{Z}) \simeq E_K/Nm(E_L).$$

Or $\hat{H}^{-3}(G, \mathbb{Z})$ est le dual de $H^3(G, \mathbb{Z})$ de sorte que leur rang est identique.
Par le théorème de Dirichlet, on a $Rg(H^3(G, \mathbb{Z})) \leq r_1(K) + r_2(K)$.
En utilisant la suite longue de cohomologie associée à $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/p \to 0$ il n'est pas difficile de voir que $Rg(H^3(G, \mathbb{Z})) = r(G) - n(G)$.

5.2 Corollaire:

Si pour la différence $r(G) - n(G)$ tend vers l'infini avec $n(G)$, alors il existe un corps de nombres K et $L|K$ non ramifiée dont le groupe de galois est un pro-p-groupe infini.
En particulier, sous l'hypothèse, le problème des tours infinies de Hilbert a une réponse positive.

En effet, soit $K(p)$ la plus grande extension galoisienne non ramifiée de K dont le groupe de galois G est un pro-p-groupe. On suppose G fini. Alors on a

$$r(G) - n(G) \leq r_1(K) + r_2(K) \leq [K : \mathbb{Q}].$$

Or $n(G)$ est, par la théorie du corps de classes, le rang de la p-composante de $Cl(K)$. On peut construire des corps K de degré bornés sur K tels que $n(G) \to \infty$, contredisant l'hypothèse faite $r(G) - n(G) \to \infty$.

5.3 Exemple:

Si $K = \mathbb{Q}(\sqrt{-p_1 ... p_N})$ avec les p_i congrus à 1 modulo 4, alors on a $r_1(K) + r_2(K) = 1$ et il est facile de voir que les extensions quadratiques engendrées par les $\sqrt{p_i}$ sont indépendantes et non ramifiées sur K de sorte que $n(G) \geq N$ et $r(G) - n(G) \leq 1$.

5.4 Théorème: (Inégalité de Golod-Shafarevitch)

Pour tout p-groupe fini G, on a

$$r(G) > n(G)^2/4.$$

On commence par montrer que si $\Lambda = \mathbb{F}_p[G]$ alors pour tout G-module fini A tel que $pA = 0$, il existe une résolution

$$0 \longrightarrow A \xrightarrow{\partial} \Lambda^{b_0} \xrightarrow{\partial} \Lambda^{b_1} \xrightarrow{\partial} \Lambda^{b_2} \longrightarrow \cdots$$

avec $b_n = \dim_p H^n(G,A)$ et $\partial((\Lambda^{b_n})^G) = 0$.
$L^{2\prime} isomorphisme A^G \mapsto (\Lambda^{b_0})^G = \mathbb{F}_p^{b_0}$ s'étend en un G-morphisme $j : A \to \Lambda^{b_0}$ puisque de la suite exacte

$$0 \to Hom(A/A^G, \Lambda^{b_0}) \to Hom(A, \Lambda^{b_0}) \to Hom(A^G, \Lambda^{b_0})$$

on tire, en prenant la G-cohomologie:

$$Hom_G(A, \lambda^{b_0}) \to Hom_G(A^G, \lambda^{b_0}) \to H^1(G, Hom(A/A^G, \Lambda^{b_0})) = 0.$$

De plus, le morphisme j est injectif car $Ker(j)^G = 0$ et donc $Ker(j) = 0$ (un p-groupe agit sans point fixe). De la suite $0 \to A \to \Lambda^{b_0} \to B \to 0$ on obtient, pour $i > 0$: $H^i(G,B) = H^{i+1}(G,A)$. De plus dans $A^G \to (\Lambda^{b_0})^G \to B^G \to H^1(G,A) \to 0$ la premiere flèche est une égalité de sorte qu'on a aussi $H^0(G,B) = H^1(G,A)$. En remplaçant A par B et en procédant de même, remarquant que $\dim_p H^0(G,B) = \dim_p H^1(G,A) = b_1$ on obtient une suite exacte $0 \to B \to \Lambda^{b_1} \to C \to 0$ avec un isomorphisme $B^G \to (\Lambda^{b_1})^G$ de sorte que l'on peut définir ∂ comme le composé $\Lambda^{b_0} \to B \to \Lambda^{b_1}$.
Le résultat s'ensuit par récurrence.

Revenons à la démonstration de Golod-Shafarevitch à proprement parler: Pour un G-module fini A tel que $pA = 0$ on définit

$$A = A_0 \subset A_1 \subset \ldots \subset A_m = A$$

par $A_0 = 0$, $A_1 = A^G$, et $A_{n+1}/A_n = (A/A_n)^G$. Puisqu'un p-groupe agit sans point fixe, on a $A_n \neq A_{n+1}$ sauf si $A_n = A$. De plus, on montre facilement que si $h : A \hookrightarrow B$, alors $A_n = h^{-1}B_n$.
On pose

$$c_n(A) = \dim_p A_{n+1}/A_n$$

et on définit le polynôme de Poincaré de A par

$$P_A(t) = \sum_{n \geq 0} c_n(A) t^n.$$

De sorte que $P_A(T)\frac{1}{1-t} = \sum_{n\geq 0} s_n(A)t^n$ avec $s_n(A) = \sum_0^n c_i(A) = \dim_p(A_{n+1})$. On applique le résultat précédent à $A = \mathbb{F}_p = \Lambda^G = \Lambda_1$. On trouve une suite exacte $0 \to E \to D \to R$ avec $E = \Lambda/\Lambda_1, D = \Lambda^d(G), R = \Lambda^r(G)$. On a par le lemme, $\partial(D_1) = R_0 = 0$. Par récurrence, on montrerait que $\partial(D_n) \subset R_{n-1}$, pour obtenir les suites exactes

$$(*) \quad 0 \to E_n \to D_n \to R_{n-1} \quad (n \geq 1).$$

On a les relations

$$P_E(t) = \frac{P_\Lambda(t) - 1}{t}, P_D(t) = d(G)P_\Lambda(t), P_R(t) = r(G)P_\Lambda(t).$$

De plus, les suites exactes (*) entrainent

$$s_n(D) \leq s_n(E) + s_{n-1}(R)$$

(on a posé $s_{-1}(R) = 0$). On a donc, pour tout $t \in]0,1[$:

$$P_D(t)\frac{1}{1-t} \leq P_E(t)\frac{1}{1-t} + P_R(t)\frac{1}{1-t}$$

Soit, si $0 < t < 1$:

$$1 \leq P_\Lambda(t)(r(G)t^2 - d(G)t + 1$$

Or $P_\Lambda(t)$ a des coefficients positifs de sorte que pour tout $t \in]0,1[$:

$$r(G)t^2 - d(G)t + 1 > 0.$$

Il suffit d'évaluer en $t = d(G)/2r(G)$.

En particulier, si $N > 7$ dans l'exemple ci-dessus, alors K possède une tour de Hilbert infinie.