Calcul de groupes de ramifications globaux

B. Allombert

IMB
CNRS/Université Bordeaux 1

06/12/2010

Lignes directrices

Présentation du problème

On se donne

- $K/\mathbb{Q}$ un extension galoisienne de $\mathbb{Q}$.
- $G = \mathrm{Gal}(K/\mathbb{Q})$ son groupe de Galois.
- $\mathfrak{p}$ un idéal premier de K au-dessus de $p \in \mathbb{Z}$.

On souhaite identifier explicitement comme sous-groupe de G :

- Le groupe de décomposition $G_{-1}(\mathfrak{p}) = D_{\mathfrak{p}}$.
- Le groupe d'inertie $G_0(\mathfrak{p}) = I_{\mathfrak{p}}$.
- Les groupes de ramification $G_i(\mathfrak{p}), i \geq 0$.

De plus si $\mathfrak{p}$ n'est pas ramifié, on souhaite identifier l'élément de Frobenius $\left(\frac{\mathfrak{p}}{K/\mathbb{Q}}\right)$ dans G.

Définition des groupes de ramification

Si $\mathfrak{p}$ n'est pas ramifié, l'élément de Frobenius $\left(\frac{\mathfrak{p}}{K/\mathbb{Q}}\right)$ est l'unique $\phi \in G$ qui vérifie $\forall x \in \mathcal{O}_K \quad \phi(x) \equiv x^p \pmod{\mathfrak{p}}$.

$$\begin{aligned} D_{\mathfrak{p}} &= \{\phi \in G | \phi(\mathfrak{p}) = \mathfrak{p}\} \\ I_{\mathfrak{p}} &= \{\phi \in D_{\mathfrak{p}} | \forall x \in \mathcal{O}_K \quad \phi(x) \equiv x \pmod{\mathfrak{p}}\} \\ G_i(\mathfrak{p}) &= \{\phi \in D_{\mathfrak{p}} | \forall x \in \mathcal{O}_K \quad \phi(x) \equiv x \pmod{\mathfrak{p}^{i+1}}\} \end{aligned}$$

On remarque que $G_{-1}(\mathfrak{p}) = D_{\mathfrak{p}}$ et $G_0(\mathfrak{p}) = I_{\mathfrak{p}}$.

Définition des groupes de ramification

- Localement nous avons $D_\mathfrak{p} \cong \mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$ mais nous nous intéressons aux automorphismes globaux.
- Les sous-groupes $G_i(\mathfrak{p})$ sont tous distingués dans $D_\mathfrak{p}$ (mais pas dans G en général).
- Soit f le degré résiduel et e l'indice de ramification de $\mathfrak{p}$. Soit $e' = ep^{-v_p e}$. Nous avons $D_\mathfrak{p}/I_\mathfrak{p} \cong \mathbb{Z}/f\mathbb{Z}$ et $I_\mathfrak{p}/G_1(\mathfrak{p}) \cong \mathbb{Z}/e'\mathbb{Z}$.
- Si $i \geq 1$ le groupe $G_i(\mathfrak{p})$ est un p-groupe.

Bibliographie : Jean-Pierre Serre, *Corps locaux*, 3e édition, Hermann, Paris (1968).

Groupe de Galois explicite

Il est nécessaire que le groupe de Galois soit donné explicitement. Nous choisirons la définition suivante.

Définition

Un groupe de Galois explicite pour $K/\mathbb{Q}$ est la donnée d'un sous-groupe transitif H de $\mathfrak{S}_n$ où $n = [K : \mathbb{Q}]$ et d'une action par automorphismes de H sur K effectivement calculable.

Ce modèle permet de calculer dans le groupe G avec une complexité qui ne dépend que de n et pas du corps K ou du modèle choisi pour K. Les sous-groupes de G s'identifient naturellement aux sous-groupes de H, en particulier il suffira de donner l'image des groupes $G_i(\mathfrak{p})$ dans H.

Idéal premier explicite

Pour $\mathfrak{p}$ un ideal premier de K au-dessus de p, on suppose connu :

- une uniformisante locale $\pi \in \mathfrak{p}$ tel que $\mathfrak{p} = p\mathcal{O}_K + \pi\mathcal{O}_K$ et $v_{\mathfrak{p}}(\pi) = 1$.
- un générateur local $x_{\mathfrak{p}} \in \mathcal{O}_K$ tel que $x_{\mathfrak{p}} \mod \mathfrak{p}$ engendre le corps résiduel $\mathcal{O}_K/\mathfrak{p}$ sur $\mathbb{F}_p$.

La donnée de (p, π) identifie uniquement $\mathfrak{p}$.

Cas non-ramifié

Ici on suppose $\mathfrak{p}$ non-ramifié de degré résiduel f.

Algorithme

- *Pour tout $\sigma \in G$ d'ordre f on teste si $v_{\mathfrak{p}}(\sigma(\pi)) = 1$.*
- *Si c'est le cas, σ engendre $D_{\mathfrak{p}}$. On calcule k tel que tel que $\sigma(x_{\mathfrak{p}}) \equiv x_{\mathfrak{p}}^{p^k} \pmod{\mathfrak{p}}$.*
- *On calcule u telque $uk \equiv 1 \pmod{f}$.*
- *On retourne $\left(\frac{\mathfrak{p}}{K/\mathbb{Q}}\right) = \sigma^u$.*

Cas modéré

Ici on suppose $\mathfrak{p}$ modérément ramifié de degré résiduel f et d'indice de ramification e.

Algorithme

- *Pour tout $\sigma \in G$ d'ordre e on teste si $v_{\mathfrak{p}}(\sigma(\pi)) = 1$.*
- *Si c'est le cas, on teste si $\sigma(x_{\mathfrak{p}}) \equiv x_{\mathfrak{p}} \pmod{\mathfrak{p}}$.*
- *Si c'est le cas, σ engendre $I_{\mathfrak{p}}$. Si $f = 1$ on retourne $D_{\mathfrak{p}} = I_{\mathfrak{p}} = \langle\sigma\rangle$.*
- *Pour tout $\tau \in G$ d'ordre f modulo $I_{\mathfrak{p}}$, on teste si $v_{\mathfrak{p}}(\sigma(\pi)) = 1$.*
- *Si c'est le cas, on retourne $D_{\mathfrak{p}} = \langle\tau, \sigma\rangle$ et $I_{\mathfrak{p}} = \langle\sigma\rangle$.*

Cas sauvage

On suppose $\mathfrak{p}$ sauvagement ramifié.
Pour $\sigma \in G$ on note $\iota_{\mathfrak{p}}(\sigma)$ le plus petit $k \geq -1$ tel que $\sigma \notin G_k(\mathfrak{p})$.
La connaissance de la fonction d'ordre $\iota_{\mathfrak{p}}$ détermine entièrement la filtration : $G_i(\mathfrak{p}) = \{\sigma \in G | \iota_{\mathfrak{p}}(\sigma) \geq i+1\}$.

Théorème

Soit $\sigma \in G$. On pose $v = v_{\mathfrak{p}}(\sigma(\pi) - \pi)$.

- *$\sigma \in D_{\mathfrak{p}}$ si et seulement si $v \geq 1$.*
- *Si $\sigma \in I_{\mathfrak{p}}$ alors $v = \iota_{\mathfrak{p}}(\sigma)$.*

Calcul de la fonction d'ordre

L'algorithme suivant calcule $\iota_{\mathfrak{p}}(\sigma)$.

- On calcule $v = v_{\mathfrak{p}}(\sigma(\pi) - \pi)$.
- Si $v = 0$ then $\iota_{\mathfrak{p}}(\sigma) = -1$.
- Sinon si $x_{\mathfrak{p}} \not\equiv \sigma(x_{\mathfrak{p}}) \mod \mathfrak{p}$ alors $\iota_{\mathfrak{p}}(\sigma) = 0$.
- Sinon. $\iota_{\mathfrak{p}}(\sigma) = v$.

Une fois connues quelque valeurs de ι_D, il est possible d'en déterminer d'autres :

- Si $(\sigma, \tau) \in G \times D$ alors $\iota_{\mathfrak{p}}(\tau^{-1}\sigma\tau) = \iota_{\mathfrak{p}}(\sigma)$.
- Si $\sigma \in G$ est d'ordre s, alors pour tout a premier à s, $\iota_D(\sigma^a) = \iota_D(\sigma)$.

Évaluation des automorphismes

L'étape la plus couteuse est l'évaluation d'un automorphisme, à cause de la taille des objets mis en jeux.
La méthode qui semble préférable pour limiter ce problème est la suivante :

- Soit K donné par $\mathbb{Q}[X]/(P)$ avec $P \in \mathbb{Z}[X]$ unitaire.
- On suppose connu une base d'entier (LLL-réduite) B de $\mathcal{O}_K$ en terme d'éléments de $\mathbb{Q}[X]/(P)$.
- On suppose connu la table de multiplication M de B.

Évaluation des automorphismes

- Pour $\sigma \in G$, on précalcule le vecteur S des coordonnées de $\sigma(X \pmod P)$ dans la base B.
- En général $\sigma(X \pmod P)$ aura des gros coéfficients mais S sera raisonnable.
- Pour un élément $a = A \pmod P$ de $\mathcal{O}_K$, on calcule $\sigma(a)$ en évaluant A sur S en utilisant la méthode de Horner (ou Brent & Kung) et la table de multiplication B.

Implantation dans PARI/GP

La fonction GP idealfrobenius calcule l'élément de Frobenius.

```
? nf=nfinit(polcyclo(31));
? gal=galoisinit(nf);
? pr=idealprimedec(nf,101)[1];
? g=idealfrobenius(nf,gal,pr)
%4 = Vecsmall([13, 14, 29, 27, 19, 30, 10, 21, 17,
1, 16, 18, 3, 6, 2, 15, 23, 28])
? galoispermtopol(gal,g)
%5 = x^8
```

fonction idealramgroups

La fonction GP idealramgroups calcule les groupes de ramification.

```
? nf=nfinit(x^6+108);
? gal=galoisinit(nf);
? pr=idealprimedec(nf,2)[1];
? iso=idealramgroups(nf,gal,pr)[2]
%4 = [[Vecsmall([2, 3, 1, 5, 6, 4])], Vecsmall([3])]
? nfdisc(galoisfixedfield(gal,iso,1))
%5 = -3
```