Une famille infinie d'extensions faiblement ramifiées.

Stéphane Vinatier

27 Juin 2000

A2X
Université Bordeaux I

Définition et exemples

Soit N une extension finie galoisienne de $\mathbb{Q}$ de groupe de Galois G.

Définition 1

*$N/\mathbb{Q}$ est **faiblement ramifiée** si, pour tout premier $\wp$ de N, le second groupe de ramification $G_2(\wp)$ est trivial.*

où

$$G_0(\wp) \triangleright G_1(\wp) \triangleright G_2(\wp) \triangleright \dots$$

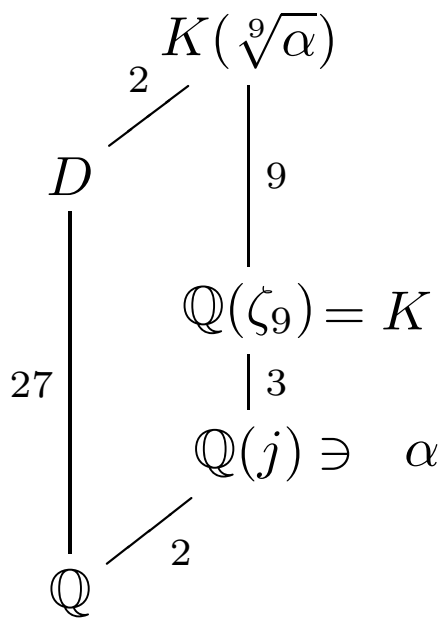
est la suite des groupes de ramification en $\wp$:

$$G_i(\wp) = \{g \in G(\wp),\ \forall x \in \mathcal{O}_N,\ g(x) \equiv x\ (\wp^{i+1})\}$$

Exemples :

- les extensions modérées
- le compositum $\mathbb{Q}(\sqrt{-3})$ par $\mathbb{Q}(\sqrt[3]{2})$
- les extensions cycliques de $\mathbb{Q}$ de degré premier impair.

Construction d'extensions galoisiennes de groupe $C_9 \rtimes C_3$.



On choisit $\alpha = (t+j)^8(t+j^2)$. D'après des résultats d'**Eichenlaub** (*thèse*, 1996), pour toutes les valeurs de t sauf un nombre fini :

- $K(\sqrt[9]{\alpha})/\mathbb{Q}$ est galoisienne de groupe :

$$\mathcal{G} \simeq C_9 \rtimes C_6$$

- $\mathcal{G}$ contient un unique 2-Sylow H (d'ordre 2).

On pose :

$$D = K(\sqrt[9]{\alpha})^H$$

Proposition 1

Pour toutes les valeurs de t sauf un nombre fini, $D/\mathbb{Q}$ est galoisienne de groupe de Galois

$$G \simeq C_9 \rtimes C_3$$

On détermine une équation paramétrée de D sur $\mathbb{Q}$. On pose $v = t^2 - t + 1$:

$$P_t(x) = x^9 - 9vx^7 + 27v^2x^5 - 30v^3x^3 + 9v^4x -$$
$$(2t-1)(t^6 - 3t^5 - 12t^4 + 29t^3 - 3t^2 - 12t + 1)v$$

Théorème 1

Pour toutes les valeurs de t congrues à 5 modulo 9, le corps de décomposition D du polynôme P_t est faiblement ramifié sur $\mathbb{Q}$.

On suppose désormais que t **est congru à 5 modulo 9** et on écrit :

$$t = 5 + 9u$$

Comportement de $\wp$ dans $K(\sqrt[3]{\alpha})/K$.

On note $\wp$ l'idéal premier de K au-dessus de 3. On remplace α par :

$$\alpha = \frac{(t+j)^8(t+j^2)}{(1-j)^9}$$

de sorte que $\alpha \notin \wp$. On dispose alors du **critère de Hecke** :

Proposition 2

Pour $\xi \in K$, on considère les congruences :

$$(i)\ \alpha \equiv \xi^3 \bmod \wp^9 \quad et \quad (ii)\ \alpha \equiv \xi^3 \bmod \wp^{10}$$

Alors, dans $K(\sqrt[3]{\alpha})/K$:

- *$\wp$ est ramifié si (i) n'a pas de solution*
- *$\wp$ est inerte si (i) a des solutions et si (ii) n'en a pas*
- *$\wp$ est décomposé si (ii) a des solutions*

$$t = 5 + 9u.$$

Lemme 1

$$v_\wp(\alpha - 1) = \begin{cases} 9 & si \quad u \equiv 0 \ ou \ 2 \bmod 3 \\ 15 & si \quad u \equiv 1 \ ou \ 7 \bmod 9 \\ 18 & si \quad u \equiv 4 \bmod 9 \end{cases}$$

Corollaire 1

Si $u \equiv 1 \bmod 3$, $\wp$ *se décompose dans* $K(\sqrt[3]{\alpha})/K$.

Proposition 3

Si $u \equiv 0$ ou $2 \bmod 3$, $\wp$ *est inerte dans* $K(\sqrt[3]{\alpha})/K$.

Comportement de $\wp$ dans $K(\sqrt[9]{\alpha})/K$.

On utilise des résultats de **Greither** (*Manuscripta Math.*, 1989). Soit k un corps local de caractéristique 0 et caractéristique résiduelle p, d'anneau d'entiers R contenant une racine primitive p^n-ième de l'unité ζ. Il décrit l'ensemble :

$$E_n(R) = \{x \in R,\ k(\sqrt[p^n]{x})/k \text{ est non ramifiée}\}$$

On note $\pi = 1 - \zeta$ et

$$U_{n,+} = \{x \in R^*,\ x-1 \text{ est divisible par } p^n \pi^{p^{n-1}}\}$$

Théorème 2 (Greither)
$U_{n,+} \subset E_n(R)$.

Application : $p = 3$, $n = 2$, $\zeta = \zeta_9$ et $k = \mathbb{Q}_3(\zeta_9)$.

Corollaire 2
Si $u \equiv 1 \bmod 3$, alors $K(\sqrt[9]{\alpha})/K$ est non ramifiée en $\wp$.

On pose $D_n(R) = E_n(R)/U_{n,+}$ et $\zeta_{p^i} = \zeta^{p^{n-i}}$.

Théorème 3 (Greither)
Il existe des polynômes explicites $f_i \in \mathbb{Z}[\zeta_{p^i}][X]$ $(2 \leq i \leq n)$, *définis modulo* $p^n(1-\zeta_p)$, *tels que :*

$$D_n(R) = \left\{ r^{p^n} \prod_{i=2}^{n} f_i(r_i)^{p^{n-i}} \mod^{\times} U_{n,+}, \quad r \in R^*,\ r_i \in R \right\}$$

On revient à $p = 3$, $n = 2$, $\zeta = \zeta_9$ et $k = \mathbb{Q}_3(\zeta)$.

$$f_2(X) \equiv 1 + 9\pi(1+\pi/2)X + (9\pi(1+\pi/2) + 3\pi^3(1+\pi^3/8))X^3 \mod \wp^{15}$$

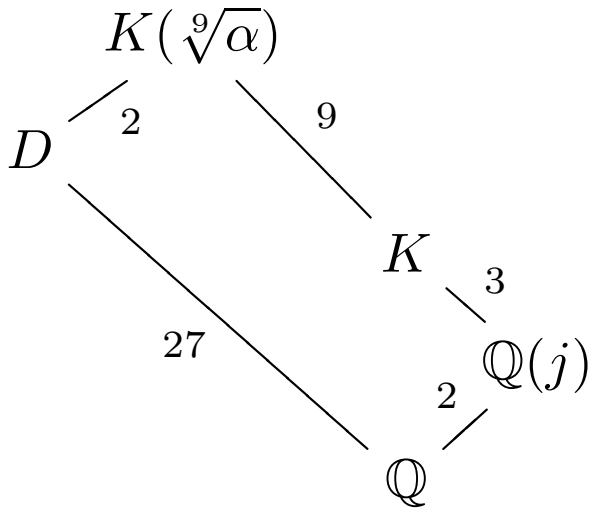
Proposition 4
Si u *est congru à 0 ou 2 modulo 3,* α *n'appartient pas à* $E_2(\mathbb{Z}_3[\zeta_9])$, *c'est-à-dire l'extension* $K(\sqrt[9]{\alpha})/K$ *est* ***ramifiée*** *en* $\wp$.

Récapitulatif.

Soient e, f et g les indices de ramification, d'inertie et de décomposition de $\wp$ dans $K(\sqrt[9]{\alpha})/K$. On a montré :

- si $u \equiv 1 \bmod 3$, alors $e = 1$ et soit $g = 9$, soit $f = g = 3$.
- si $u \equiv 0$ ou $2 \bmod 3$, $e = f = 3$ et $g = 1$.

Remarque : f et g sont aussi les indices d'inertie et de décomposition de 3 dans $D/\mathbb{Q}$.



Calculs de discriminants.

Lemme 2

$$2v_3(d_D) + fg = 81 + v_3(\mathrm{N}_{K/\mathbb{Q}}(d_{K(\sqrt[9]{\alpha})/K}))$$

Soit s la valuation de la différente $\mathcal{D}_D$ en les idéaux premiers de D au-dessus de 3. Alors :

$$2s + 1 = \frac{81 + v_3(\mathrm{N}_{K/\mathbb{Q}}(d_{K(\sqrt[9]{\alpha})/K}))}{fg}$$

Corollaire 3

Si $K(\sqrt[9]{\alpha})/K$ est non ramifiée en $\wp$, alors $D/\mathbb{Q}$ est faiblement ramifiée.

en utilisant la **formule de Hilbert** :

$$s = \sum_{i \geq 0} |G_i| - 1$$

Fin de la preuve.

On suppose que $K(\sqrt[9]{\alpha})/K$ est ramifiée en $\wp$, alors $f = 3$, $g = 1$ et

$$e(K(\sqrt[9]{\alpha})/K(\sqrt[3]{\alpha}), 3) = 3$$

Soit $\mathfrak{q}$ l'idéal premier de $K(\sqrt[3]{\alpha})$ au-dessus de 3. On note $\gamma = \sqrt[9]{\alpha}$.

Lemme 3
$\mathcal{O}_{K(\sqrt[3]{\alpha})}[\gamma]$ n'est pas un ordre $\mathfrak{q}$-maximal de $\mathcal{O}_{K(\sqrt[9]{\alpha})}$.

On en déduit :

$$v_{\mathfrak{q}}(d_{K(\sqrt[9]{\alpha})/K(\sqrt[3]{\alpha})}) < v_{\mathfrak{q}}(\mathrm{disc}(1, \gamma, \gamma^2)) = 18$$

Corollaire 4
Si $K(\sqrt[9]{\alpha})/K$ est ramifiée en $\wp$, alors $D/\mathbb{Q}$ est faiblement ramifiée.

Racine carrée de la Codifférente.

$N/\mathbb{Q}$ extension finie galoisienne de groupe G, de **degré impair**.

$$v_{\wp}(\mathcal{D}_N) = \sum_{i \geq 0} |G_i(\wp)| - 1$$

On définit $\mathcal{A}_N$, l'idéal **racine carrée de la codifférente** par la relation :

$$\mathcal{A}_N^2 = \mathcal{D}_N^{-1}$$

C'est un idéal fractionnaire *stable* sous l'action de $G \longrightarrow \mathbb{Z}[G]$-module

Théorème 4 (Erez *Math. Z.* (1991)**)**
$\mathcal{A}_N$ est un $\mathbb{Z}[G]$-module ***localement libre*** $\Leftrightarrow$ *$N/\mathbb{Q}$ est* ***faiblement ramifiée.***

Le réseau associé à $\mathcal{A}_N$.

$N/\mathbb{Q}$ faiblement ramifiée de degré impair. On munit N de la **forme trace** :

$$\mathrm{Tr} \ : \ (x,y) \in N^2 \mapsto \mathrm{Tr}_{N/\mathbb{Q}}(xy) \ \in \mathbb{Q}$$

Le dual d'un idéal I de N est $I^{-1}\mathcal{D}_N^{-1}$.

$\mathcal{A}_N$ est **auto-dual** pour l'action de Tr
$\longrightarrow$ réseau entier unimodulaire $(\mathcal{A}_N, \mathrm{Tr})$.

On munit $\mathbb{Z}[G]$ de la forme quadratique q pour laquelle les éléments de G forment une base orthonormale
$\longrightarrow$ réseau entier unimodulaire $(\mathbb{Z}[G], q)$.

Ces deux réseaux sont-ils G-isométriques ?

Résultats théoriques.

Si $N/\mathbb{Q}$ est abélienne (Erez 1987) :

- $(\mathcal{A}_N, \mathrm{Tr})$ est isométrique à $(\mathbb{Z}[G], q)$.

Si $N/\mathbb{Q}$ est modérée :

- $\mathcal{A}_N$ est un $\mathbb{Z}[G]$-module libre (Erez 1991)
- $(\mathcal{A}_N, \mathrm{Tr})$ stablement isométrique à $(\mathbb{Z}[G], q)$ (Erez-Taylor 1992).

Si $N/\mathbb{Q}$ est faiblement ramifiée :

- $\mathcal{A}_N$ est libre sur tout ordre maximal de $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$ (Erez 1991)
- si les groupes de décomposition aux places sauvages sont abéliens, $\mathcal{A}_N$ est un $\mathbb{Z}[G]$-module libre.
- $(\mathcal{A}_N, \mathrm{Tr}) \ldots$?

Calculs sur les exemples.

Proposition 5

Pour $t \in \{5, 14, 23, 41\}$, $D/\mathbb{Q}$ *est une extension galoisienne faiblement ramifiée avec* $G \simeq C_9 \rtimes C_3$.

(i) Pour $t \in \{14, 41\}$, $(\mathcal{A}_D, \mathrm{Tr})$ *est* ***isométrique*** *à* $(\mathbb{Z}[G], q)$.

(ii) Pour $t \in \{5, 23\}$, $(\mathcal{A}_D, \mathrm{Tr})$ *est un réseau unimodulaire de rang 27 de* ***minimum 3*** *bien déterminé.*

Remarque :

(i) correspond à u congru à 1 modulo 3 : le groupe de décomposition en 3 est d'ordre 3 ou 9 donc abélien.

(ii) correspond à u congru à 0 et 2 modulo 3 : le groupe de décomposition en 3 est égal à G.

Plus d'exemples.

On considère le polynôme paramétré $Q_t(X)$:

$$X^9-3^3v\,X^7-2^1 3^3(t-1)v\,X^6+2^5 3^4 wv\,X^5+2^4 3^4(6t-13)wv\,X^4$$
$$-2^4 3^3(175t^2-495t+1629)wv\,X^3-2^5 3^5(33t-103)w^2v\,X^2$$
$$+2^6 3^5(7t^2+54t+51)w^2v\,X-2^7 3^3(3t^3+73t^2-75t+1791)w^2v$$

où $v=12t^2-30t+109$ et $w=t^2-3t+9$.

On note D le corps de décomposition de Q_t pour une valeur entière de t.

Proposition 6 (Eichenlaub)
Pour presque tout t, $D/\mathbb{Q}$ est une extension galoisienne de groupe de Galois G isomorphe à $C_9 \rtimes C_3$.

Proposition 7

Pour toutes les valeurs de t *considérées,* $D/\mathbb{Q}$ *est une extension galoisienne* ***faiblement ramifiée*** *avec* $G \simeq C_9 \rtimes C_3$.

(i) pour $t \in \{12, 21, 30\}$, $D/\mathbb{Q}$ *est modérée et* $(\mathcal{A}_D, \mathrm{Tr})$ *est* ***isométrique*** *à* $(\mathbb{Z}[G], q)$.

(ii) pour $t = 24$, *le groupe de décomposition en* 3 *est abélien et* $(\mathcal{A}_D, \mathrm{Tr})$ *est* ***isométrique*** *à* $(\mathbb{Z}[G], q)$.

(iii) pour $t \in \{9, 18, 27\}$, *le groupe de décomposition en* 3 *est non abélien et* $(\mathcal{A}_D, \mathrm{Tr})$ *est un réseau de* ***minimum 3***.

(iv) pour $t \in \{15, 33\}$, *le groupe de décomposition en* 3 *est abélien et* $(\mathcal{A}_D, \mathrm{Tr})$ *est un réseau de* ***minimum*** 2.

Remarque : dans tous les cas considérés, certains vecteurs de norme 3 ou 5 du réseau $(\mathcal{A}_D, \mathrm{Tr})$ engendrent des bases normales de $\mathcal{A}_D$.

Eichenlaub Y., *Problèmes effectifs de théorie de Galois en degrés 8 à 11*, Thèse de Doctorat, Université Bordeaux 1 (1996).

Greither C., Unramified Kummer extensions of prime power degree, *Manuscripta Math.*, **64** (1989), *no. 3*, 261-290.

Erez B., The Galois structure of the square root of the inverse different, *Math. Z.*, **208** (1991), 239-255.

Erez B., Taylor M. J., Hermitian modules in Galois extensions of number fields and Adams operations, *Ann. of Math.*, **135** (1992), *no. 2*, 271–296.

Hecke E., *Lectures on the theory of algebraic numbers*, Graduate texts in maths. **77**, Springer-Verlag, New York-Berlin (1981).

Vinatier S., Structure galoisienne dans les extensions faiblement ramifiées, *en préparation*.