SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

J. J. PAYAN
H. AMARA

Extensions non ramifiées non résolubles

Séminaire de théorie des nombres de Grenoble, tome 1 (1971-1972), p. 61-67
<http://www.numdam.org/item?id=STNG_1971-1972__1__61_0>

EXTENSIONS NON RAMIFIEES NON RESOLUBLES

d'après K. UCHIDA

Exposé de J.J. PAYAN le 5 février 1972
Rédigé par H. AMARA

On va démontrer les théorèmes suivants :

Théorème I (Uchida 1970 [3]).

Soit n un entier naturel supérieur ou égal à 3 . Il existe une infinité de corps K quadratiques sur Q pour lesquels existe L avec L/K non ramifiée et Gal $L/K \simeq A_n$.

Théorème II (Fröhlich 1962 [1]).

Soit G un groupe fini de degré n , il existe une infinité d'extensions de corps de nombres, L/K avec L/K non ramifiée Gal $L/K \simeq G$ et $[K:Q] \leq 2(n-1)!$

Pour la démonstration de ces deux théorèmes nous allons suivre Uchida [3] et commencer par la

Proposition I.

k désigne un corps de nombres, a et b deux entiers de k . On note L le corps de rupture du polynôme $f(X) = X^n - aX + b$ et D le discriminant de f(X) . Si (n-1)a et nb sont premiers entre eux $L/k(\sqrt{D})$ est non ramifiée.

Démonstration : Soit $\mathfrak{P}$ un idéal premier de L , posons $\mathfrak{p} = \mathfrak{P} \cap k$ et $G = \text{Gal } L/k$. G est un sous-groupe de $S\{\alpha_1, \ldots, \alpha_n\}$ où $(\alpha_1, \ldots \alpha_n)$ sont des racines de f(X) . $k(\sqrt{D})$ est le corps des invariants du sous-groupe H de G formé des permutations paires. L'égalité $Xf'(X) - nf(X) = (n-1)aX - nb$ montre, compte tenu de $((n-1)a, nb) = 1$, que $(n-1)aX - nb$ est le P.G.C.D. de f(X) et f'(X) mod $\mathfrak{p}$, il en résulte que la décomposition de f(X) mod $\mathfrak{p}$ s'écrit :

$$f(X) = \bar{g}_1(X)\bar{g}_2(X)\ldots\bar{g}_r(X) \quad \text{avec les } \bar{g}_i(X)$$

premiers entre eux deux à deux et les $\bar{g}_i(X)$ irréductibles pour $i \geq 2$ et $g_1(X) = ((n-1)aX-nb)^2$ qui sera irréductible suivant que $(n-1)a \in \mathfrak{p}$ ou non. On én déduit d'après le lemme de Hensel une décomposition de $f(X)$ de la forme suivante sur le corps local $k_\mathfrak{p}$

$$f(X) = g_1(X)\ldots g_r(X) \quad \text{avec} \quad \bar{g}_i(X) = \text{image de } g_i(X) \text{ module } \mathfrak{p} .$$

Remarquons que $L_\mathfrak{P}$ s'obtient en adjoignant à $k_\mathfrak{p}$ les racines de $f(X)$. Les polynômes $g_i(X)$ étant irréductibles mod $\mathfrak{p}$ est premier entre eux deux à deux pour $i \geq 2$ l'extension L''_β obtenue par adjonction de leurs racines à $k_\mathfrak{p}$ et non ramifiée sur $k_\mathfrak{p}$. L'extension L'_β par adjonction des racines de $g_1(X)$ à $k_\mathfrak{p}$ est ramifiée ou non suivant que $g_1(X)$ a une racine double ou non mod $\mathfrak{p}$. Dans tous les cas L'_β et L''_β sont linéairement disjoints sur $k_\mathfrak{p}$. Il est clair que le groupe d'inertie G_{T_β} de β dans Gal $L_\beta/k_\mathfrak{p}$ s'identifie à Gal L_β/L''_β donc à Gal $L'_\beta/k_\mathfrak{p}$ et au groupe formé de l'identité et de la permutation des racines de $g_1(X)$ dans le cas où $L_\beta/k_\mathfrak{p}$ est non ramifiée. Il en résulte que $G_{T_\beta} \cap H = \{1\}$ pour tout β .

Remarque : Si $k = Q$, il existe toujours un nombre premier qui se ramifie dans L , donc Gal(L/Q) contient toujours une transposition.

Prenons maintenant $k = Q$.

Proposition II.

n un entier fixé $(n \geq 3)$ *, il existe deux entiers* a , b *tels que* $L/Q(\sqrt{\bar{D}})$ *soit une extension galoisienne non ramifiée et* $\text{Gal}(L/Q(\sqrt{\bar{D}}) \simeq A_n$

Démonstration :

a) n premier : on prend deux entiers a , b tels que : $((n-1)a, nb) = 1$ et $f(X) = X^n - aX + b$ soit irréductible sur Q . $L/Q(\sqrt{\bar{D}})$ est non ramifiée d'après la proposition 1. $G = \text{Gal}(L/Q)$ est un groupe de permutation transitif ($f(X)$ étant irréductible sur Q) il contient une transposition donc $G \simeq S_n$ d'après les 2 lemmes suivants :

Lemme 1. ([5] théorème 8-3)

Un groupe de permutation transitif de degré premier est primitif.

Lemme 2. ([5] théorème 13-3)

Si un groupe de permutation primitif contient une transposition il est égal à S_n .

et ainsi $Gal(L/Q(\sqrt{D}) \simeq A_n$.

b) n quelconque : soit ℓ un nombre premier congru à un (mod n-1) si on choisit $b \equiv 0 \pmod{\ell}$ on aura la décomposition :

$$X^n - aX + b \equiv X(X^{n-1}-a) \pmod{\ell}$$

puisque $Z/\ell Z$ contient les racines (n-1)-ième de l'unité pour avoir $X^{n-1}-a$ irréductible mod ℓ il suffit de choisir a générateur de $(Z/\ell Z)^*$. Ces choix entraînent que f(X) est réductible sur Q , il se décompose en deux facteurs l'un du premier degré et l'autre de degré n-1 , autrement dit f(X) admettra une racine sur Q . Cette racine est un diviseur de b . b étant fixé ainsi que la classe mod ℓ de a , on peut toujours choisir a assez grand pour que f(X) n'admette pas une racine sur Q , f(X) est alors irréductible. La factorisation sur $Z/\ell Z$ montre qu'il est transitif et contient un cycle d'ordre n-1 (voir [3] chap. VII pour une justification) et une transposition d'où on en déduit : $G \simeq S_n$ grâce au lemme suivant :

Lemme 3.([4], chap. VII, 61)

Tout groupe de permutation transitif qui contient une transposition et un (n-1) cycle est S_n .

Si de plus on choisit $((n-1)a, nb) = 1$ on aura $L/Q(\sqrt{D})$ galoisienne non ramifiée et $Gal(L/Q(\sqrt{D}) \simeq A_n$

Théorème I.

$n \geq 3$, A_n désigne comme d'habitude le groupe alterné de degré n . Il existe une infinité de corps quadratiques $K = Q(\sqrt{D})$ qui admettent une extension L galoisienne non ramifiée et $Gal(L/Q(\sqrt{D}) \simeq A_n$.

Démonstration : Nous garderons toutes les conditions imposées à a et b au cours de la démonstration de la proposition II qui prouve l'existence de tels corps quadratiques. Soit p un nombre premier tel : $(p, \ell n(n-1)) = 1$ si on réussit à trouver a,b tel que : $D = D(a,b) = pD'$ avec $(p,D') = 1$, on aura

démontré l'existence d'une infinité de corps quadratiques vérifiant les conditions du théorème 1.

$$D = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (n\alpha_i - a)$$

$$= (-1)^{\frac{n(n-1)}{2}} (n^n b^{n-1} - (n-1)^{n-1} a^n)$$

choisissons $b \equiv n-1 \pmod p$ avec $(b, n-1) = 1$. Puisque $(p,n) = 1$, choisissons a , suffisamment grand et $a_1 \equiv n \pmod p$ tout en prenant le soin que a_1 soit générateur de $(Z/\ell Z)^*$ et ainsi $D(a,b)$ est divisible par p , s'il est divisible par p^2 on remplace a_1 par $a = a_1 + nb\ell p$ et $D(a,b)$ sera divisible par p et non par p^2 .

Exemples.

Dans tous les exemples du tableau suivant les $f(X)$ sont irréductibles sur Q et engendrent des extensions galoisiennes non ramifiées avec des groupes de Galois isomorphes à A_n .

n	a	b	D
5	1	1	2869 = 19 × 151
5	-2	1	11317 = (premier)
6	1	1	-43531 = -101 × 431
6	1	-1	49781 = 67 × 743
7	1	1	-776887 = (premier)
7	-1	1	-870199 = -11 × 239 × 331
8	1	-1	-17600759 = -11 × 1600069
9	1	1	370643273 = 7 × 11 × 13 × 43 × 79 × 109
9	-1	1	404197705 = 5 × 197 × 410353
10	1	1	-9612579511 = -29 × 4127 × 80317
10	1	-1	10387420489 = 173 × 60042893

On va faire l'étude détaillée pour : $n = 6$, $a = 1$, $b = 1$ dans les autres cas ça se fait de la même manière : $f(X) = X^6 - X + 1$ il est irréductible mod 2 , donc sur Q . D'autre part :

$$X^6-X+1 = (X-2)(X^5+2X^4+3X^3+X^2+2X+3) \pmod 7$$

le dernier facteur est irréductible mod 7 ; car tous les polynômes de degré 1 ou 2 qui apparaissent dans la décomposition de $X^6 - X + 1$ mod 7 en facteurs irréductibles sont des diviseurs de $X^{7^2} - X = X^{49} - X$ et que le dernier n'a que $X - 2$ comme facteur commun avec $X^6 - X + 1$ par cette décomposition le groupe de Galois de $f(X)$ sur Q va contenir un (6-1)cycle avec une transposition déjà. C'est S_6 en entier.

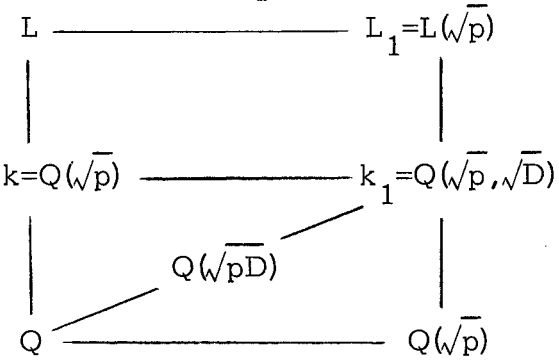
Corollaire II.

Soit p un nombre premier congru à un mod 4 tel que $(p,D) = 1$ si $L/Q(\sqrt{D})$ est galoisienne non ramifiée à groupe de Galois A_n , $L(\sqrt{p})/Q(\sqrt{pD})$ est galoisienne non ramifiée et son groupe de Galois est S_n .

Démonstration : On note $k = Q(\sqrt{D})$, $L_1 = L(\sqrt{p})$, $k_1 = k(\sqrt{p}) = Q(\sqrt{D},\sqrt{p})$ L/k est non ramifiée donc L_1 est non ramifiée sur k_1 , d'autre part

$$\Delta_{k_1/Q} = \Delta_{k/Q}\cdot\Delta_{Q(\sqrt{pD})/Q}\cdot\Delta_{Q(\sqrt{p})/Q}$$
$$= p^2D^2a$$

avec a égal 1 ou une puissance de 2 .



Les nombres premiers qui se ramifient dans k_1 sont p , les diviseurs premiers de D et éventuellement 2 . L'expression de $\Delta_{Q(\sqrt{pD})/Q}$ montre alors que $k_1/Q(\sqrt{pD})$ est non ramifiée en dehors de 2 . Si $p \equiv 1 \pmod 4$ $Q(\sqrt{p})/Q$ est non ramifiée en 2 . On a donc $k_1/Q(\sqrt{pD})$ non ramifiée et ainsi $L_1/Q(\sqrt{pD})$ est galoisienne non ramifiée à groupe de Galois S_n .

Théorème II.

Soit G un groupe fini de degré n .On peut trouver une infinité de corps de nombres k qui admettent des extensions galoisiennes non ramifiées à groupe de Galois G et tels que $[K:Q] \leq 2(n-1)!$.

Démonstration : Soient L une extension de Q tel que $L/Q(\sqrt{D})$ est galoisienne non ramifiée à groupe de Galois A_n et p un nombre premier tel que $(p,D) = 1$ et $p \equiv 1 \pmod 4$ on sait d'après le corollaire II que $L(\sqrt{p})$ est non ramifiée sur $Q(\sqrt{pD})$ et son groupe de Galois est S_n . G étant isomorphe à un sous-groupe de S_n l'extension k de Q qui correspond à ce sous-groupe répond à la question. L'existence d'une infinité est une conséquence immédiate du théorème I.

Théorème III.

Il existe une infinité de corps quadratiques réels tels que leur nombre de classes est divisible par 3.

Démonstration : On considère l'équation $f(X) = X^3-aX+b = 0$, a et b deux entiers tels que $(2a,3b) = 1$ et $Gal(L/Q) \simeq S_3$. Ceci entraîne que $L/Q(\sqrt{D})$ est cyclique non ramifiée de degré 3 donc le nombre de classes de $Q(\sqrt{D})$ est divisible par 3 . $D = 4a^3-27b^2$ est le discriminant de f(X) , démontrons qu'il y a une infinité de $Q(\sqrt{D})$ avec $D > 0$. Choisissons $b = 1$, $a \geq 2$ et $a \equiv 1 \pmod 3$, X^3-aX+1 est alors irréductible et satisfait aux conditions avec $D > 0$. Le groupe de Galois de l'équation X^3-aX+1 est S_n (car il est transitif, de degré premier et contient une transposition). Soit p un nombre premier distinct de 2 et 3 . Une condition nécessaire pour que p divise $D = 4a^3-27$ est que 4 soit reste cubique modulo p . Réciproquement, si 4 est reste cubique modulo un tel p on peut trouver a tel que $4a^3-27$ soit divisible par p . En effet, choisissons $p \equiv 2 \pmod 3$, alors l'élévation au cube est un automorphisme sur $(Z/pZ)^*$ et 4 est reste cubique modulo p ; on peut trouver $a_1 > 2$ tel que p divise $4a_1^3 - 27$. Comme l'équation $a_1+rp \equiv 1 \ (3)$ a des solutions avec $r \in Z$ on peut supposer $a_1 \equiv 1 \ (3)$. Si $4a_1^3 - 27$ est divisible par p^2 , on remplace a_1 par a_1+3p on a ainsi un $D = 4a^3-27$ divisible par p et non par p^2 , ainsi p est ramifié dans $Q(\sqrt{D})/Q$. Il est clair qu'on peut trouver une infinité de ces p . (voir pour des exemples de corps quadratiques réels à nombre de classes divisible par 3 [2]).

Exemple :

p	a	b	D	h
5	7	1	5 x 269	6
"	22	1	5 x 8513	6
"	37	1	5 x 40517	
17	46	1	17 x 22901	
"	97	1	17 x 214735	
23	70	1	23 x 59651	

Remarque : On trouvera une autre démonstration du théorème III dans un article de Taira Honda "On real quadratic fields whose class numbers are multiple of 3" (J. de Crelle 233 (1968) p. 101 et 102).

BIBLIOGRAPHIE

[1] - A. FRÖLICH - "On non-ramified extensions with prescribed Galois group". Mathematika 9 (1962).

[2] - G. GRAS - "Thèse de 3e cycle", Faculté des Sciences de Grenoble, (1970).

[3] - K. UCHIDA - "Unramified extensions of Quadratic numbers fields I et II". Tôhku Math. Jal 22 (1970).

[4] - B.L. VAN DER WAERDEN - "Modern Algebra". Bd 1. Springer. Volume I.

[5] - H. WIELANDT - "Finite permutation group". Academic Press (1964).