MÉMOIRES DE LA S. M. F.

PIERRE DAMEY

Extensions quaternioniennes d'un corps de nombres

Mémoires de la S. M. F., tome 37 (1974), p. 35-38
<http://www.numdam.org/item?id=MSMF_1974__37__35_0>

Journées arithmétiques [1973, Grenoble]
Bull. Soc. math. France,
Mémoire 37, 1974, p. 35-38

EXTENSIONS QUATERNIONIENNES D'UN CORPS DE NOMBRES

par

Pierre DAMEY
(Travail fait en commun avec J. MARTINET)

-:-:-:-

I. - GROUPES QUATERNIONIENS. EXTENSIONS QUATERNIONIENNES.

Soient g un groupe cyclique d'ordre 2, τ son générateur et C_n un groupe cyclique d'ordre n (n entier positif). On fait opérer g sur C_n par

$$(\tau, x) \to \tau x = x^{-1} \qquad (x \in C_n)$$

et on cherche les groupes E extensions de C_n par g pour cette opération.

Si n est impair, à isomorphisme près, il n'y a qu'une solution, le groupe diédral D_n donné par les générateurs et les relations :

$$\tau^2 = 1 \; ; \; \sigma^n = 1 \quad \text{et} \quad \tau\sigma\tau^{-1} = \sigma^{-1} \; .$$

Si n est pair, il y a une autre solution, unique à isomorphisme près : le groupe quaternionien. On notera H_n le groupe quaternionien d'ordre $4n$ défini par les générateurs et les relations suivantes :

$$\sigma^{2n} = 1 \; ; \; \tau^2 = \sigma^n \; , \; \tau\sigma\tau^{-1} = \sigma^{-1} \; .$$

Remarque : Le groupe D_n est produit semi-direct de deux groupes cycliques, l'un étant l'ordre 2, alors que le groupe H_n n'est pas le produit semi-direct de 2 groupes, l'un étant d'ordre 2.

Exemples.
- H_1 est le groupe cyclique d'ordre 4.
- H_2 est le groupe quaternionien usuel (d'ordre 8).

DÉFINITION. - Soient k un corps, k_1 une extension quadratique séparable de k ; on dira que le plongement de k_1 dans une extension quaternionienne (resp. diédrale) de degré $4n$ (resp. $2n$) est possible s'il existe une extension N, cyclique sur k_1, galoisienne sur k et dont le groupe $\mathrm{Gal}(N/k)$ de Galois sur k est isomorphe à H_n (resp. D_n) .

PROPOSITION I. - <u>Si</u> $n = qn_1$ <u>avec</u> n_1 <u>entier impair et</u> $q = 2^r$, <u>puissance de</u> 2, <u>le plongement de</u> k_1 <u>dans une extension quaternionienne de degré</u> $4n$ <u>est possible si et seulement si</u> k_1 <u>se plonge dans une extension diédrale de degré</u> $2n_1$ <u>et dans une extension quaternionienne de degré</u> $4q$. (Il suffit de composer une extension diédrale de degré $2n_1$, cyclique sur k_1 , avec une extension quaternionienne de degré $4q$, cyclique sur k_1).

<u>Remarque</u> : Si k est un corps de nombres, le plongement du corps k_1 dans une extension diédrale est toujours possible, car c'est une extension décomposée.

On va se limiter dans la suite au cas où k est un corps de nombres.

PROPOSITION II. - <u>Si</u> $n = 2^r$ <u>est une puissance de</u> 2 <u>et si le plongement de</u> k_1 <u>dans une extension quaternionienne de degré</u> $4n$ <u>est possible, alors le plongement est possible dans une extension quaternionienne de degré</u> $4nn'$ <u>quel que soit l'entier positif</u> n' .

<u>Indication</u> : En utilisant la proposition I on se ramène au cas où n' est une puissance de 2. Il suffit alors de remarquer que le composé d'une extension quaternionienne de degré $4n$, cyclique sur k_1 , et d'une extension diédrale de degré $4nn'$, cyclique sur k_1 , contient une extension quaternionienne de degré $4nn'$, cyclique sur k_1 .

<u>Conséquence</u> : Soient k un corps de nombres et $k_1 = k(\sqrt{m})$ une extension quadratique de k . <u>Si</u> k_1 <u>se plonge dans une extension quaternionienne, il existe un plus petit entier</u> n <u>tel que ce plongement soit possible en degré</u> $4n$ <u>et il est alors possible en degré</u> $4nn'$ <u>quel que soit l'entier</u> n' .

II. - <u>DETERMINATION DE L'ENTIER</u> n .

1) En complétant le corps k par rapport aux valuations archimédiennes et en remarquant qu'une extension N quaternionienne ne contient qu'une sous-extension N_o tel que $[N : N_o] = 2$ on voit qu'une condition nécessaire pour que $k_1 = k(\sqrt{m})$ se plonge dans une extension quaternionienne est que m soit totalement positif.

2) THEOREME 1. - <u>Soit</u> $k_1 = k(\sqrt{m})$. <u>Pour que</u> m <u>soit somme de</u> 2 <u>carrés dans</u> k <u>il faut et il suffit que</u> k_1 <u>se plonge dans une extension quaternionienne de degré</u> 4. <u>Pour que</u> m <u>soit somme de</u> 3 <u>carrés dans</u> k <u>il faut et il suffit que</u> k_1 <u>se plonge dans une extension quaternionienne de degré</u> 8.

Ces résultats sont connus (pour le deuxième, cf. [4]).

3) THEOREME 2. - <u>Si</u> m <u>est totalement positif, le corps</u> k_1 <u>se plonge dans une extension quaternionienne de degré</u> 32.

THEOREME 3. - <u>Si</u> m <u>est totalement positif, non somme de</u> 3 <u>carrés</u>, k_1 <u>se plonge dans une extension quaternionienne de degré</u> 16 <u>si et seulement si l'une des 2 conditions suivantes est vérifiée</u> :

a) <u>il existe une place</u> v <u>de</u> k <u>telle que</u> $[k_v(\sqrt{-m},\sqrt{2}) : k_v] = 4$;

b) <u>le nombre de places de</u> k <u>où</u> m <u>n'est pas somme de</u> 3 <u>carrés est pair</u>.

<u>Remarque</u> : Dans la deuxième condition, seules les places au-dessus de 2 peuvent intervenir.

<u>Indications sur la démonstration des deux théorèmes</u>.

En utilisant les résultats de [2], le plongement de k_1 dans une extension quaternionienne de degré 32 sur k est possible si et seulement si un certain élément x de k est tel qu'il existe $\alpha \in k(\sqrt{-m},\sqrt{2+\sqrt{2}}) = K_{16}$ avec $N_{K_{16}/k}(\alpha) = x^4$.

Or, en utilisant, par exemple, les résultats de [1] (chapitre VII et exercice 5), on peut montrer que dans une extension abélienne K de degré 8, sur k composée d'une extension de degré 2 et d'une extension cyclique de degré 4, on a $k^4 \subset N_{K/k}(K)$.

Pour le théorème III, dans le cas où la condition a) est vérifiée, on sait que toute norme locale est une norme globale dans $k(\sqrt{-m},\sqrt{2})$ (sur k) , et si la condition a) n'est pas vérifiée, le calcul de la valeur de $\varphi(x)$ où φ désigne la fonction définie dans [1] (exercice 5.2) donne le résultat.

<u>Applications au cas où le corps</u> k <u>est le corps des rationnels</u>.

Soit m un entier positif, sans facteurs carrés ; on notera $n(m)$ le degré de la plus petite extension quaternionienne sur $\mathbb{Q}$, cyclique sur $\mathbb{Q}(\sqrt{m})$; la lettre p désignera un nombre premier positif.

$$n(m) = 4 \Leftrightarrow p \mid m \Rightarrow p \not\equiv -1 \pmod 4$$

$$n(m) = 8 \Leftrightarrow \exists p \mid m : p \equiv -1 \pmod 4 \text{ et } m \not\equiv -1 \pmod 8$$

$$n(m) = 16 \Leftrightarrow m \equiv -1 \pmod 8 \text{ et } \exists p \mid m : p \not\equiv \pm 1 \pmod 8$$

$$n(m) = 32 \Leftrightarrow m \equiv -1 \pmod 8 \text{ et } p \mid m \Rightarrow p \equiv \pm 1 \pmod 8 .$$

Exemples.

$\mathbb{Q}(\sqrt{1973})$ se plonge dans une extension cyclique de degré 4 ;

$\mathbb{Q}(\sqrt{1974})$ se plonge dans une extension quaternionienne de degré 8 ;

$\mathbb{Q}(\sqrt{1975})$ se plonge dans une extension quaternionienne de degré 32 ;

$\mathbb{Q}(\sqrt{1983})$ se plonge dans une extension quaternionienne de degré 16 .

Comme autre application du théorème 3, donnons le théorème suivant :

THEOREME 4. - Soient k un corps de nombres, k_1 une extension quadratique de k qui ne se plonge dans une extension quaternionienne que si son degré est divisible par 32, et soit K une extension de k ne contenant pas k_1 . Alors $K(\sqrt{m})$ se plonge dans une extension quaternionienne de degré 16 sur K si et seulement si le degré $[K : k]$ est pair.

-:-:-:-

BIBLIOGRAPHIE

[1] J.W.S. CASSELS, A. FROHLICH. - Algebraic Number Theory. (Academic Press).

[2] P. DAMEY. - Sur certaines 2-extensions galoisiennes, non-abéliennes d'un corps de caractéristique différente de 2. Thèse, Grenoble (1971).

[3] P. DAMEY, J. MARTINET. - Plongement dans une extension quaternionienne. (à paraître).

[4] P. DAMEY, J.J. PAYAN. - Existence et construction des extensions galoisiennes et non-abéliennes de degré 8. J. reine angew. Math., 244, 1970, p. 37-54.

-:-:-:-

Pierre DAMEY, Jacques MARTINET
U.E.R. de Mathématiques et Informatique
(ERA n° 362)
351, cours de la Libération
33405 TALENCE