Internat. J. Math. & Math. Sci.
VOL. 20 NO. 1 (1997) 43-46

COMPUTATION OF HILBERT SEQUENCE FOR COMPOSITE QUADRATIC EXTENSIONS USING DIFFERENT TYPE OF PRIMES IN Q

M. HAGHIGHI and J. MILLER
Department of Computer Science
Bradley University
Peoria, IL 61625 USA

(Received April 3, 1995 and in revised form July 3, 1995)

ABSTRACT. First, we will give all necessary definitions and theorems. Then the definition of a Hilbert sequence by using a Galois group is introduced. Then by using the Hilbert sequence, we will build tower fields for extension K/k, where $K = k(\sqrt{d_1}, \sqrt{d_2})$ and $k = Q$ for different primes in Q.

KEY WORDS AND PHRASES: Composite quadratic extension, Hilbert sequence
1991 AMS SUBJECT CLASSIFICATION CODES: 12A65.

1. INTRODUCTION

Let K/k be an extension of degree n. We consider the tower of fields and a tower of integer rings for this extension

$$\begin{array}{c} K \supseteq \ldots \supseteq L \ldots \supseteq k \\ O_K \supseteq \ldots \supseteq O_L \ldots \supseteq O_k \end{array} \tag{1.1}$$

A prime ideal P in K determines a prime $P_L$in each field of the tower, where each P_L is divisible by P. Let p be a rational prime that is divisible by all these prime ideals P_L. Then we have:

$$P_L = P_k \cap O_L, \quad p = P_L \cup Z.$$

If the prime ideal p in k does not split into n distinct factors of P in K, how far can we go in terms of an intermediate field where splitting occurs? This will be answered later.

First we define what is meant by order and degree

DEFINITION 1.1.

(a) Order $P/p = e = P^e | p,\ p^{e+1} \nmid P$

(b) Degree $P/p = f = N_{k/k}P = p^f$

LEMMA 1.2. Both order and degree are multiplicative

Order P/p = order P/P_L • order P_L/p

Degree P/p = degree P/P_L • degree P_L/p

Let us assume here that K/k for $[K;k] = n$ is a normal extension. This makes K/L normal for each L in the tower but not in L/k. Let p have factors $P_L^{(j)}$ in L for $j = 1, 2, 3, \ldots, g$,

$$p = \bigcap_{i=1}^{g} P_L^{(j)e},\ N\left(P_L^{(j)}\right)^f = N(p)^f \tag{1.2a}$$

$$n = e.f.g. \tag{1 2b}$$

Let order $K/k\,P = e$ and degree $K/k\,P = f$. Then for $P = p$, we have order p = degree $p = 1$ from k to k.

Thus from k to K the order has grown from 1 to e and the degree has grown from 1 to f and the number of factors in (1.2a) and (1.2b) has grown from 1 to g. We arrange the tower fields in 1.1 in such a way that will separate the growths for K/k normal.

Let K_Z be a maximal L in $\{L : K \supseteq L \supseteq k\}$. K_Z is called the "splitting" field of P in K/L and is such that.

$$\begin{aligned} &\text{degree } P_L/p = 1 \\ &\text{order } \ P_L/p = 1 \end{aligned}$$

Let us assume that K_T is a maximal L in $\{L : K \supseteq L \supseteq k\}$. K_T is called the "inertial" field of P in $K/_L$ and is such that

$$\begin{aligned} &\text{degree } P_L/p = f_L \geq 1 \\ &\text{order } \ P_L/p = 1. \end{aligned}$$

This maximality process can be performed again for all L such that:

$$\begin{aligned} &\text{degree } P_L/p = f_L \geq 1 \\ &\text{order } \ P_L/p = e_L \ \text{ for } \ (e_L, p) = 1. \end{aligned}$$

The maximal field here is called the "first ramification" field K_{v_1}.

For this field, $F_L = f$ and e_L is a part of e prime to p. This part is called "tame ramification " If order e is divisible by p, the ramification is called "wild." Thus we have the new tower fields for extension K/k:

$$K \supseteq \ldots \supseteq K_{v_1} \supseteq K_T \supseteq K_Z \supseteq k \tag{1 2c}$$

It is easier to define 1.2c by the Galois group methods.

DEFINITION 1.2. Let K/k be a normal extension. The Hilbert sequence for an ideal P in K is given by the subgroups of $G = Gal(K/k)$ as follows:

$$\begin{aligned} K \supseteq \ldots \supseteq K_{v_1} \supseteq K_T \supseteq K_Z \supseteq k \\ 1 \subseteq \ldots \subseteq G_{v_1} \subseteq G_T \subseteq G_Z \subseteq G \end{aligned} \tag{1.3a}$$

$$k_Z \overset{G}{\leftrightarrow} \{u \in G : P^u = P \text{ or } A \equiv 0 = A^u \equiv 0 \bmod p\} = G_Z \tag{1.3b}$$

$$k_T \overset{G}{\leftrightarrow} \{u \in G : P^u \equiv A \bmod p\} = (G_{v_0}) \tag{1.3c}$$

$$k_{V_r} \overset{G}{\leftrightarrow} \left\{u \in G : A^u \equiv A \bmod p^{r+1}\right\} = G_{v_r}, \quad (r \geq 0)\,. \tag{1.3d}$$

Where A is an arbitrary integer in O_k. Since G_Z fixes P, then G_T, G_v, and so on are invariant subgroups of G_Z. Since G_Z preserves P, it is one of g conjugates,

$$|G/G_Z| = g\,, \tag{1.3e}$$

also, since G_T preserves each residue class mod P,

$$|G_Z/G_T| = |(O_K/_P)/(O_k/_p)| = |c(f)| = f\,, \tag{1.3f}$$

which refer to the cyclic Galois group of an extension of a finite field. Furthermore

$$|G_T| = e\,. \tag{1 3g}$$

If $r = e_0 p^w$, where $(e_0, p) = 1$, then there is a cyclic quotient,

$$|G_T/G_{v_0}| = e_0 \tag{1.3h}$$

followed by future quotient groups of type $C(p) \times C(p) \times \ldots \times C(p)$, with

$$G_{v_r}/G_{v_{r+1}} = p^{w_r} (w_r \geq 0,\ \Sigma w_r = w)\,. \tag{1.3i}$$

Here there is only a finite number $w_r > 0$, indeed $p^w | n$ More general details of the above can be found in [1], [2], [3], [4], [5], [6], [7]

2. COMPUTING HILBERT SEQUENCE FOR $K = k(\sqrt{d1}, \sqrt{d2})$, FOR $k = Q$.

Computing Hilbert sequence for $K = k(\sqrt{d})$, $k = Q$, is contained in [1, p 89]. So we process to $K \supseteq k_i = Q(\sqrt{d_i})$ for $i = 1, 2, 3$. Let $d_3 = d_1 \cdot d_2/t^2$ which means d_3 is square factor free, where d_i is the discriminant of k_i.

Let $G = \{1, u_1, u_2, u_3)$, where $u_i : \sqrt{d_i} \to \sqrt{d_i}$, $\sqrt{d_j} \to -\sqrt{d_j}$ for $i \neq j$, then we have

$$k_i = Q(\sqrt{d_i}) \overset{G}{\Leftrightarrow} G_i = \{1, u_i\}\,.$$

Here we will build a tower of fields $K \supseteq \ldots \supseteq K_{v_1} \supseteq K_T \supseteq K_Z \supseteq Q$ by using the Hilbert sequence in Definition 1.2 for different types of primes p in Q.

a Let $p = P_1 P_2 P_3 P_4$ (unramified) where the P_i's are primes in K for $(d_1/p) = (d_2/p) = (d_3/p) = 1$ where:

$$(a/p) = \begin{cases} 1 \text{ if } x^2 = a \bmod p \text{ solvable for } x \text{ integer}, a|p \\ -1 \text{ if } x^2 \neq a \bmod p \text{ for } x \text{ integer}, a|p \\ 0 \text{ if } a|p. \end{cases}$$

Here $f = e = 1$ then $g = 4$ by 1.1. From $|G/G_Z| = g = 4$ in (1.3e) we get that, $|K_Z/k| = 4$ and $K_Z = K$ and from $|G_Z/G_T| = f = 1$ in (1.3f), $|K_T/K_Z| = 1$ and so $K_T = K$. Since $|G_T| = e = 1$ in (1.3g), and from $|G_T/G_{v_0}| = e_0 = 1$ in (1.3h) and (1.3i) for $r = 0, 1, 2, 3$ then $|G_{v_r}/G_{v_{r+1}}| = |K_{vr+1}/K_{v_r}| = 1$

$$K_{v_1} = K_{v_2} = K_{v_3} = K_{v_4} = K\,.$$

Thus, we have the following field tower for K/k :

$$k = Q \subseteq K_Z \subseteq K_T \subseteq K_{v_1} \subseteq K_{v_2} \subseteq K_{v_3} \subseteq K_{v_4} \subseteq K$$

$$Q \subseteq K = K = K = K = K = K = K = K\,.$$

b Let $p = P_1 P_2$ (unramified) for $-(d_1/p) = -(d_2/p) = (d_3/p) = 1$. Here $e_1 = e_2 = 1$, $f_1 = f_2 = 2$ and $g = 2$. Again from $|G/G_Z| = g = 2$, we have: $|K_Z/k| = 2$ and by (1.3b) $K_Z = k_3 = Q(\sqrt{d_3})$. From $|G_Z/G_T| = f = 1$ then $|K_Z/K_T| = 2$ and then $K_T = K$ Using the same proof as above: $K_{v_1} = K_{v_2} = K_{v_3} = K_{v_4} = K$. This produces the following tower fields for K/k :

$$k = Q \subseteq K_Z \subseteq K_T \subseteq K_{v_1} \subseteq K_{v_2} \subseteq K_{v_3} \subseteq K_{v_4} \subseteq K$$

$$Q \subseteq k_3 \subseteq K = K = K = K = K = K\,.$$

c $p = P_1^2 \cdot P_2^2$, where p is odd and $p|d_1$, $p|d_2$, $p|d_3$ and $(d_3/p) = 1$. Here $e_1 = e_2 = 2$ and $f_1 = f_2 = 1$ and so $g = 2$ Since again $|G/G_Z| = g = 2$ then $|K_Z/k| = 2$ and by (1 3b) $K_Z = k_3 = Q(\sqrt{d_3})$. From $|G_Z/G_T| = f = 1$ then $K_T = K_Z = k_3 = Q(\sqrt{d_3})$ From $|G_T| = e = 2 = e_0 \cdot p^w = 1 \cdot 2^1$ then by (1.3i) $|G_{v_r}/G_{v_{r+1}}| = p^w r = 2^1$ and from here for $r = 0$:

$|G_{r_0}/G_{v_1}| = |K_{v_1}/K_T| = 2$ and thus $K_{v_1} = K$ and also $K_{v_2} = K_{v_3} = K_{v_4} = K$, because $|G_{v_r}/G_{v_{r+1}}| = |K_{v_{r+1}}/k_{v_r}| = 2^0 = 1$ which produces the following tower fields for K/k

$$k = Q \subseteq k_Z \subseteq k_T \subseteq k_{v_1} \subseteq k_{v_2} \subseteq k_{v_3} \subseteq k_{v_4} \subseteq K$$

$$Q \subseteq K_3 = k_3 \subseteq K = K = K = K = K .$$

d. $p = P_1^2$ for p odd, $p|d_1$, $p|d_2$, $p|d_3$, $(d3/p) = -1$ with the same proof as above, the following tower fields are produced.

$$K_Z = Q,\ K_T = k_3, \text{ and } K_{v_1} = K_{v_2} = K_{v_3} = K_{v_4} = K .$$

e. $P = p_1^2 p_2^2$, and $d_1 \equiv d_2 \equiv 1^2 \pmod{16}$, $d_3 \equiv 1 \pmod 8$ produces the tower

$$k = Q \subseteq k_Z \subseteq k_T \subseteq K_{v_1} \subseteq K_{v_2} \subseteq K_{v_3} \subseteq K_{v_4} \subseteq K$$

$$Q = Q \subseteq k_3 \subseteq K = K = K = K = K .$$

f. $p = p_1^2$ for $d_1 \equiv d_2 \equiv 12 \pmod{16}$, $d_3 \equiv 5 \pmod 8$. Here $e = 2$ and $g = 1$ then $f = 2$. From $|G/G_Z| = g = |K_Z/Q| = 1$, $K_Z = Q$ and by $|G_Z/G_T| = f = |K_T/K_Z| = 2$, K_T is a quadratic extension over Q, then by (1.3c) $K_T = k_3$, $e = 2 = e^0 \cdot p^w = 1.2^w$ and $|G_{v_r}/G_{v_{r+1}}| = 2^{w_r}$ where $\Sigma\ w_r = w$ and $w_r \geq 0$. From $|G_{v_0}/G_{v_1}| = |K_{v_1}/K_T| = 2^0 = 1$, $K_{v_1} = k_3$. $|G_{v_2}/G_{v_1}| = 2^1 = |K_{v_2}/G_{v_1}| = 2$, then $K_{v_2} = K$, and with some proof $K_{v_2} = K_{v_3} = K_{v_4} = K$ producing

$$k = Q \subseteq K_Z \subseteq K_T \subseteq K_{v_1} \subseteq K_{v_2} \subseteq K_{v_3} \subseteq K_{v_4} \subseteq K$$

$$Q = Q \subseteq k_3 = k_3 \subseteq K = K = K = K .$$

g. $p = p_1^2 p_2^2$ for $d_1 \equiv d_2 \equiv 8 \pmod{16}$, $d_3 \equiv 1 \pmod 8$ has the same tower fields as e.

h. $p = p_1^2$, for $d_1 \equiv d_2 \equiv 8 \pmod{16}$, $d_3 \equiv 5 \pmod 8$ also has the same Hilbert sequence as f.

i. $p = p_1^4$ for $d_1 \equiv d_2 \equiv 8 \pmod{16}$, $d_3 \equiv 12 \pmod 8$ has the following tower fields

$$k = Q \subseteq k_Z \subseteq K_T \subseteq K_{v_1} \subseteq K_{v_2} \subseteq K_{v_3} \subseteq K_{v_4} \subseteq K$$

$$Q = Q = Q = Q \subseteq k_3 = k_3 \subseteq K = K .$$

We showed in the above cases, if the prime ideal p of k does not split into n distinct prime factors of K, how we can build intermediate fields K_Z, K_T, K_{v_0}, ... where splitting of prime p occurs.

ACKNOWLEDGMENT. Thanks to the referees for many valuable suggestions for improving the content of the paper.

REFERENCES

[1] COHN, H., *Introduction to the Construction of Class Fields*, Cambridge University Press, 1985

[2] HILBERT, D., Die theorie der algebraischen Zahlkörper, *Jahrsber. Deutsch. Math.* **4** (1897), 173-546.

[3] HILBERT, D., Über die theorie des relativ quadratischen Zahlkörpers, *Math. Ann.* **51** (1899), 1-27.

[4] HECKE, E., Vorlesungenüber die theorie der algebraischen, *Zahlem. Leipzig: Teubner*, 1923.

[5] HASSE, H., Klassenkörper theorie, Original Lecture Notes, Marbug, 1933.

[6] HAGHIGHI, M., Relative Integral Bases for Algebraic Number Fields, Ph.D. Dissertation, Dept of Mathematics, CUNY, 1982.

[7] McCARTHY, P. J., *Algebraic Extensions of Fields*, Blaisedell Publishing Company, 1966.

Mathematical Problems in Engineering

Special Issue on Space Dynamics

Call for Papers

Space dynamics is a very general title that can accommodate a long list of activities. This kind of research started with the study of the motion of the stars and the planets back to the origin of astronomy, and nowadays it has a large list of topics. It is possible to make a division in two main categories: astronomy and astrodynamics. By astronomy, we can relate topics that deal with the motion of the planets, natural satellites, comets, and so forth. Many important topics of research nowadays are related to those subjects. By astrodynamics, we mean topics related to spaceflight dynamics.

It means topics where a satellite, a rocket, or any kind of man-made object is travelling in space governed by the gravitational forces of celestial bodies and/or forces generated by propulsion systems that are available in those objects. Many topics are related to orbit determination, propagation, and orbital maneuvers related to those spacecrafts. Several other topics that are related to this subject are numerical methods, nonlinear dynamics, chaos, and control.

The main objective of this Special Issue is to publish topics that are under study in one of those lines. The idea is to get the most recent researches and published them in a very short time, so we can give a step in order to help scientists and engineers that work in this field to be aware of actual research. All the published papers have to be peer reviewed, but in a fast and accurate way so that the topics are not outdated by the large speed that the information flows nowadays.

Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://www.hindawi.com/journals/mpe/guidelines.html. Prospective authors should submit an electronic copy of their complete manuscript through the journal Manuscript Tracking System at http://mts.hindawi.com/ according to the following timetable:

Manuscript Due	July 1, 2009
First Round of Reviews	October 1, 2009
Publication Date	January 1, 2010

Lead Guest Editor

Antonio F. Bertachini A. Prado, Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 12227-010 São Paulo, Brazil; prado@dem.inpe.br

Guest Editors

Maria Cecilia Zanardi, São Paulo State University (UNESP), Guaratinguetá, 12516-410 São Paulo, Brazil; cecilia@feg.unesp.br

Tadashi Yokoyama, Universidade Estadual Paulista (UNESP), Rio Claro, 13506-900 São Paulo, Brazil; tadashi@rc.unesp.br

Silvia Maria Giuliatti Winter, São Paulo State University (UNESP), Guaratinguetá, 12516-410 São Paulo, Brazil; silvia@feg.unesp.br