EXPLICIT INTEGRAL GALOIS MODULE STRUCTURE FOR LOW DEGREE ABELIAN EXTENSIONS

A THESIS IN MATHEMATICS

Submitted to the University of Madras
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy

by
Manisha V. Kulkarni

DEPARTMENT OF MATHEMATICS
INSTITUTE OF MATHEMATICAL SCIENCES, MADRAS

कां साडेपंधरया रजतवणी। तैशीं स्तुतीचीं बोलणीं।
उगियांचि माथा ठेविजे चरणीं। हेंचि भले ॥

Dedicated

to the memory

of my brother–in–law

Manohar

CERTIFICATE

This is to certify that the Ph.D. thesis titled "*Explicit Integral Galois Module Structure for Low Degree Abelian Extensions*" submitted by Manisha V. Kulkarni is a bonafide research work done under my supervision. The research work presented in this thesis has not formed the basis for the award to the candidate of any Degree, Diploma, Associateship, Fellowship or other similar titles. It is further certified that the thesis represents independent work by the candidate and collaboration was necessitated by the nature and scope of the problems dealt with.

IMSC, MADRAS
11.09.96

R. Balasubramanian
Thesis Supervisor

PROFESSOR
THE INSTITUTE OF MATHEMATICAL SCIENCES
MADRAS-600 113

Acknowledgements

I am deeply indebted to my guide Prof. R. Balasubramanian for several things, tangible and intangible. But for his patient and expert guidance this work would never have seen the light of the day.

I am obliged to Prof. Anupam Srivastava for having suggested the problems that I worked on. I shall remain grateful to him for having steadfastly supported me whenever I needed such support.

My sincere thanks are due to my friend and collaborator Dr. S. Venkataraman. His knowledge and desire for perfection played a key role in shaping my attitude towards Mathematics.

It is difficult to express the extent of my debt to Dr. V. Balaji in whom I found a friend and mentor.

I take this opportunity to thank Kalyan who helped me to get over some really hard times. His love and affection never let me miss my family and home.

I thank Dr. Sukumar Adhikari(Sukuda) and Dr. Viswanath for many invaluable discussions in Mathematics. I also thank Amora for her pleasant and helpful friendship and for the things I learned from her.

I wish to thank the people who have provided me pleasant association, timely help and comfort. Swarup and Raghavan helped me a lot during the preparation of my papers and thesis and otherwise too. Vanaja, as always, was all love and affection. Srinath, Anand, Biswajit, Gulan, Janaki, Radha, Ravindran(Tambi), Surya, and Vimala and many others made my stay in Matscience a memorable one.

I thank Dr. B. Ramkrishnan (Ramki) for pointing out all typographical mistakes of thesis.

I specially thank Prakash Mathews and the Anitas for their friendship.

I sincerely thank Prof. R. Ramachandran, Director of this institute and Prof. H. S. Mani, Director of MRI, Allahabad for their kind support and encouragement.

The Library and Administrative staff deserve special thanks for their help.

Last but not the least, I thank my family for everything.

Manisha

Contents

1 Introduction

Let M be a Galois extension of a number field L with Galois group G. The associated order $A_{M/L}$ of M over L is defined as: $\{x \in L[G] \mid x\mathcal{O}_M \subseteq \mathcal{O}_M\}$, Here $L[G]$ is the usual group algebra. Then the ring of integers $\mathcal{O}_M$ of M is a module over $A_{M/L}$.

We are interested in the explicit Galois module structure problem which is the same as the following problem :

Is it possible to:

1) Describe $A_{M/L}$ explicitly?

2) Determine if O_M is free as an $A_{M/L}$–module, i.e., determine if there exists a $\gamma \in \mathcal{O}_M$ such that $O_M = \gamma.A_{M/L}$?

3) Describe explicitly the generator γ whenever O_M is free over $A_{M/L}$?

It is known that $A_{M/L} = \mathcal{O}_L[G]$ iff M is tame over L. For an extension M over L, by normal basis theorem, there is a $\gamma \in M$, which can be chosen to be in $\mathcal{O}_M$, such that $\{\sigma(\gamma)\}_{\sigma \in G}$ spans M over L. Normal integral basis problem is concerned with the existence of such a $\gamma \in \mathcal{O}_M$. In other words, it concerns with the freeness of $\mathcal{O}_M$ as an $\mathcal{O}_L[G]$ module.

One of the early results is the following due to Hilbert and Speiser: Let $L = Q$ and $M \subset Q(\zeta_n)$ for some squarefree n. Then $\mathcal{O}_M = Tr_{Q(\zeta_n)/M}(1 - \zeta_n)ZG$.

By a Theorem of Noether [16], if $\mathcal{O}_M$ is free over $\mathcal{O}_L[G]$, M/L is necessarily tame. In fact, the squarefree condition on n in the above result ensures that M/L is tame. Thus, in the tame case the Galois module structure problem is just a normal integral basis problem.

The Galois Module structure problem has been completely solved in the case when

$L = Q$ and G is abelian by Leopoldt [13]. A simpler proof is given recently by G. Lettl. [14].

Theorem 1: (Leopoldt) *Let M be a finite abelian extension of Q. Then the ring of integers $\mathcal{O}_M$ of M is a free, rank one module over the associated order $A_{M/Q}$.*

When $L \neq Q$, no general result is known. In the following situations the associated order $A_{M/L}$ has been determined:

(1) (almost) Maximally ramified Kummer extensions [8].

(2) Kummer extensions of Cyclotomic extensions of Q and some complex analogues [23]

(3) Kummer extensions of Lubin– Tate division fields, [22].

In [20], the Galois module structure for relative quadratic extensions was determined. Similar results were obtained independently by Lettl [14]. When M/Q is a dihedral extension of order $2p$, p an odd prime, the associated order and conditions for O_M to be free over $A_{M/Q}$ was given by A. M. Berge [2]. When M/L is an extension of Cyclotomic fields, Chan and Lim [7], have proved that O_M is always free over $A_{M/L}$.

Let k be an imaginary quadratic field and let $k(J)$ denote the ray class field with conductor J for an integral ideal J in O_k. When $M = k(I^*)$, $L = k(I)$ and $I|I^*|I^2$, Schertz [19] has proved freeness.

There are more results on Explicit Galois Module Structure problem in ([2], [3], and [5]) for the local cases and in ([1], [7], [17], and [19]) for the global cases. [6] and [24] have good surveys for the explicit Galois module structure.

In this thesis we have considered the following cases:

(1) M, a bicyclic biquadratic extension of Q and L, quadratic subfield.

(2) M, a cyclic quartic, Galois extension of Q and L, quadratic subfield.

(3) $L = Q(\sqrt{-3})$ and M, its cubic Galois extension.

(4) $L = Q(i)$ and M, a cyclic Galois extension of degree 4 i.e. $M = L(\sqrt[4]{a})$ where a is an integer which is fourth power free.

(5) $L = Q(i)$ and once again M be a cyclic Galois extension of degree 4 but here $M = L(\sqrt[4]{a})$ where a is an element of $Z[i]$ which is fourth power free.

And in each of the above cases we have completely solved the Explicit Galois Module Structure problem.

One can also study the structure of $\mathcal{O}_M$ as a $Z[G]$ module. If M/L is tame, $\mathcal{O}_M$ defines a class in the locally free class group $\mathrm{cl}(Z[G])$. One can describe this class in terms of certain constants associated with the Artin L- functions for the extension M/L. We have Taylor's theorem which implies in particular that $\mathcal{O}_M$ is always free as a $Z[G]$ module when M/L is abelian. For more details [21]. There is no method for constructing a $Z[G]$ basis for $\mathcal{O}_M$ when $\mathcal{O}_M$ is free over $Z[G]$. In this thesis in cases (1) and (2), we have found $Z[G]$ basis of $\mathcal{O}_M$ over L whenever extension is tamely ramified.

This thesis is organised in the following way:

In **chapter 2** of this thesis, we consider a field extension M over L, where M is a quartic galois extension of Q and L, it's quadratic subfield. In this case $G = Z_2 \times Z_2$ or Z_4. We give the explicit structure of the associated order and conditions under which the ring of integers of M will be free over $A_{M/L}$ as a module and whenever it is free, we give a generator of $\mathcal{O}_M$ over $A_{M/L}$. In this chapter we also study the structure of $\mathcal{O}_M$ as a $Z[G]$ module whenever M is tame over L.

In **chapter 3** of this thesis, we have found explicitly the associated order and structure of O_M as an $\Lambda_{M/L}$-module for the following cases:

(1) $L = Q(\omega)$, $G = Z_3$, where ω is a primitive cube root of unity.

(2) $L = Q(i)$, $M = L[\sqrt[4]{a}]$ where $i^2 = -1$ and a is an integer which is fourth power free.

In **chapter 4** of this thesis, we consider the field extension F of K where $K = Q(i)$ and $G = Z_4$. First we find an integral basis of F over K and using this integral basis we find explicit structure of $A_{F/K}$ and of O_F as an $A_{F/K}$ module. In each of the cases we give generator of O_F over $\Lambda_{F/K}$.

2 Galois module structure of quartic Galois extensions

Let M be a quartic Galois extension of Q and let L be it's quadratic subfield. Here $G = Z_2 \times Z_2$ or Z_4. In this chapter, we give the explicit structure of the associated order and conditions under which the ring of integers of M will be free over $A_{M/L}$ as a module and whenever it is free, we give a generator of $\mathcal{O}_M$ over $A_{M/L}$.

In section 1 we will give notations used in this chapter and some known results which we will use in later sections. In section 2 we will give explicit structure of the associated order and structure of $\mathcal{O}_M$ as an $A_{M/L}$ module and in section 3 we will give $Z[G]$ basis of M over L whenever M is tame over L.

1 Preliminaries

Let $m, n \neq 1$ are distinct and squarefree integers such that mn is not a square. $d = (m, n)$, $m' = \frac{m}{d}$ and $n' = \frac{n}{d}$. Let M be a quartic Galois extension over Q and L be the quadratic subfield of M. G denotes the Galois group of M over L, Δ denotes the discriminant of M over L. When $m > 0$ let $\epsilon_0 = r + t\sqrt{m}$ be the fundamental unit of L. When M is cyclic quartic, let $\delta \in Z$ be such that $\delta = 0$ if $r, t \in Z$ and $\delta = 2$ if $r, t \notin Z$. When $\delta = 2$, let $s = \frac{1}{2}(2r + 1)$.

When $\delta = 2$, $\epsilon_0 = \frac{p+q\sqrt{D}}{2}$, ${\epsilon_0}^2 = \frac{j+k\sqrt{D}}{2}$ and ${\epsilon_0}^3 = \frac{l+m\sqrt{D}}{2}$ for some $p, q, j, k, l, m \in Z$.

When M is cyclic quartic, in [10] it is shown that $M = Q\left(\sqrt{A\left(D + B\sqrt{D}\right)}\right)$, with A, B, $C \in Z$, A and D square free, A is odd, B, $C > 0$ and $D = B^2 + C^2$. Clearly

$D \not\equiv 3 \pmod 4$. Moreover $(A, D) = 1$.

We now state a few known results which will be used later in this chapter.

Theorem 2: **(K. S. Williams [27])** *An integral basis of field M over Q where $M = Q(\sqrt{m}, \sqrt{n})$ and m, n are as above, is given as follows.*

$1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m'n'}}{4}$ when $m \equiv n \equiv 1 \pmod 4$

$1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m'n'}}{2}$ when $m \equiv 1, n \not\equiv 1 \pmod 4$

$1, \frac{1+\sqrt{n}}{2}, \sqrt{m}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m'n'}}{2}$ when $n \equiv 1, m \not\equiv 1 \pmod 4$

$1, \frac{1+\sqrt{m'n'}}{2}, \sqrt{n}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m'n'}}{2}$ when $m \equiv n \not\equiv 1, m'n' \equiv 1 \pmod 4$

$1, \sqrt{m}, \sqrt{n}, \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m'n'}}{2}$ when $m \not\equiv 1,\ n \not\equiv 1, m'n' \not\equiv 1 \pmod 4$

Theorem 3: **(Bird - Parry [4])** *The discriminant of $Q(\sqrt{m}, \sqrt{n})$ over $Q(\sqrt{m})$ is*

(i). n' *when* $n \equiv 1 \pmod 4$ *or* $m'n' \equiv 1 \pmod 4$

(ii). $4n'$ *when* $m \equiv 1 \pmod 4$ *and* $n \not\equiv 1 \pmod 4$.

(iii). $2n'$ *otherwise.*

Theorem 4: **(Bird - Parry [4])** *An Integral basis of $Q(\sqrt{m}, \sqrt{n})$ over $Q(\sqrt{m})$ for $m < 0$ is given as follows.*

$m,\ n,\ m'n' \equiv \pmod 4$	*Conditions*	*Integral Basis*
$n \equiv 1$	$d = 1$	$\{1, \frac{1+\sqrt{n}}{2}\}$
$m \equiv 1,\ n \not\equiv 1$	$d = 1$	$\{1, \sqrt{n}\}$
$m \equiv 1,\ n \not\equiv 1$	$d = -m$	$\{1, \sqrt{-n'}\}$
$m \equiv n \equiv 2,\ m'n' \equiv 3$	$d = 2$	$\{1, \frac{\sqrt{m}+\sqrt{2n'}}{2}\}$
$m \equiv m'n' \equiv 2,\ n \equiv 3$	$d = \frac{-m}{2}$	$\{1, \frac{\sqrt{m}+\sqrt{-2n'}}{2}\}$
$n \equiv 1$	$d = -m$	$\{1, \frac{\sqrt{m}+\sqrt{m'n'}}{2}\}$
$m \equiv 3,\ n \equiv m'n' \equiv 2$	$m = -1$	$\{1, \frac{\sqrt{n}+\sqrt{-n}}{2}\}$
$m \equiv n \equiv 3$	$d = -m$	$\{1, \frac{1+\sqrt{m'n'}}{2}\}$
$m \equiv n \equiv 3$	$d = 1$	$\{1, \frac{\sqrt{m}+\sqrt{n}}{2}\}$

Lemma 1.1: **(Bird - Parry [4])** *Let $\epsilon = \epsilon_0$ or ϵ_0^3 be of the form $p + q\sqrt{m}$ where $p, q \in Z$ and let the norm of ϵ be 1. If $m \equiv 1$ or $2 \pmod 4$ then $(p, q) \equiv (1, 0) \pmod 2$ and if $m \equiv 1 \pmod 4$ then $q \equiv 0 \pmod 4$. Furthermore*

$$\sqrt{\epsilon} = s\sqrt{u} + t\sqrt{v} \tag{1}$$

with $(u, v) = 1$ *and* $uv = m$. *If* $m \equiv 3 \pmod 4$ *then either* $q \equiv 0 \pmod 4$ *and equation (1) holds or* $(p, q) \equiv (0, 1) \pmod 2$ *and*

$$\sqrt{\epsilon} = \frac{s\sqrt{2u} + t\sqrt{2v}}{2} \tag{2}$$

with the above conditions on u *and* v.

Theorem 5: (**Bird - Parry [4]**) *An integral basis of* $M = Q(\sqrt{m}, \sqrt{n})$ *over* $Q(\sqrt{m})$ *for* $m > 0$, *when* $d = 1$, m *or* $\frac{m}{2}$ *is as in theorem 3 and in other cases it is as follows. Here, for this table,* $\sqrt{\epsilon} = \frac{s\sqrt{ru} + t\sqrt{rv}}{r}$ *where* $r = 1$ *for all cases except for the last case in which* $r = 2$.

m, n, $m'n' \equiv \pmod 4$	Conditions	Integral Basis
n *or* $m'n' \equiv 1$	$d = u$ *or* v $pn' \equiv 1 \pmod 4$	$\{1, \quad \frac{1+\sqrt{n'\epsilon}}{2}\}$
$m \equiv 1$ $n \not\equiv 1$		$\{1, \quad \sqrt{n'\epsilon}\}$
$m \equiv 2$ n *or* $m'n' \equiv 1$	$d = u$ *or* v $pn' \equiv 3 \pmod 4$	$\{1, \quad \frac{1+\sqrt{m}+\sqrt{n'\epsilon}}{2}\}$
$m \equiv n \equiv 2$ $m'n' \equiv 3$	$d = 2u$ *or* $2v$	$\{1, \quad \frac{\sqrt{m}+\sqrt{2n'\epsilon}}{2}\}$
$m \equiv m'n' \equiv 2$ $n \equiv 3$	$d = \frac{u}{2}$ *or* $\frac{v}{2}$	$\{1, \quad \frac{\sqrt{m}+\sqrt{2n'\epsilon}}{2}\}$
$m \equiv 3$ n *or* $m'n' \equiv 1$	$d = u$ *or* v $pn' \equiv 3 \pmod 4$	$\{1, \quad \frac{\sqrt{m}+\sqrt{n'\epsilon}}{2}\}$
$m \equiv 3$ $n \equiv 2$	$d = u$ *or* v	$\{1, \quad \frac{\sqrt{2n'\epsilon}}{2}\}$

Lemma 1.2: (**Hymo - Parry [11]**) *Let* M *be a cyclic quartic extension of* Q *and* $L = Q(\sqrt{D})$ *be its quadratic subfield. Then* M/L *has an integral basis iff* $M = L(\sqrt{A'\epsilon_0\sqrt{D}})$ *where*

$A' = 2A$ *if* $D \equiv 1 \pmod 4$ *and* $B \equiv 1 \pmod 2$

$A' = A$ *otherwise.*

Theorem 6: (Hymo - Parry [11]) *If D is odd and $M = L(\sqrt{2A\epsilon_0\sqrt{D}})$ then $1, \sqrt{2A\epsilon_0\sqrt{D}})$ is an integral basis for M over L. If $M = L(\sqrt{A\epsilon_0\sqrt{D}})$ then an integral basis of M/L can be given by,*

(1) $1, \frac{1}{2}\left(\frac{1+(-1)^s\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}\right)$ *if* $d \equiv 1 \pmod 4$, $A \equiv 3 \pmod 4$ *and* $\delta = 2$.

(2) $1, \frac{1+\sqrt{A\epsilon_0\sqrt{D}}}{2}$ *if* $D \equiv A + r \equiv 1 \pmod 4$ *and* $\delta = 0$

(3) $1, \sqrt{A\epsilon_0\sqrt{D}}$ *otherwise.*

Theorem 7: (Srivastav - Venkataraman [20]) *Let M/L be a quadratic extension of number fields with Galois group G. Let $Tr(\mathcal{O}_M) = \{tr_L^M(\alpha) | \alpha \in \mathcal{O}_M\}$. Then $\mathcal{O}_M$ is a free $\Lambda_{M/L}$ module if and only if*

1. $Tr(\mathcal{O}_M)$ is a principal ideal of $\mathcal{O}_L$,

2. $\mathcal{O}_M$ is monogenic over $\mathcal{O}_L$, i.e. there exists an $\alpha \in \mathcal{O}_M$ such that $\mathcal{O}_M = \mathcal{O}_L[\alpha]$ and,

3. There exists a generator t of $Tr(\mathcal{O}_M)$ such that $tr(\alpha) \equiv t \pmod{2\mathcal{O}_L}$.

Moreover, if M/L satisfies all the above conditions then,

$\Lambda_{M/L} = \mathcal{O}_L 1_G + t^{-1}\mathcal{O}_L\sigma$, where $\sigma = g_1 + g_2, g_i \in G$ such that g_1 and g_2 are distinct. and $\mathcal{O}_M = \gamma\Lambda_{M/L}$, where $\gamma = \alpha + \frac{t - tr(\alpha)}{2}$.

Lemma 1.3: (Srivastav - Venkataraman [20]) *Let $|G| = 2$. Then $\mathcal{O}_M = \alpha\mathcal{O}_L[G]$ for an $\alpha \in \mathcal{O}_M$ if and only if $\mathcal{O}_M = \mathcal{O}_L[\alpha]$ and $tr(\alpha) \in \mathcal{O}_L^*$.*

2 Structure of $\mathcal{O}_M$

In this section we will determine the structure of $\mathcal{O}_M$ as an $\Lambda_{M/L}$ module.

Theorem 8: *Let $M = Q(\sqrt{m}, \sqrt{n})$ be a bicyclic, biquadratic extension of Q and $L = Q(\sqrt{m})$. The structure of $\mathcal{O}_M$ as an $\Lambda_{M/L}$ module for $m > 0$ can be given as follows. Here p is as in lemma 1.1, and $t = x + y\sqrt{m}$ with $x^2 - y^2 m = \pm 2$ When $d = 1$, m or $\frac{m}{2}$ the structure is given in table II. In other cases it is as in table I.*

Table I

	$m,\ n \equiv \pmod 4$	*Conditions*	$\mathcal{O}_M$
1	$m \equiv n \equiv 1$		$\mathcal{O}_L[G](\frac{1+\sqrt{n'\epsilon}}{2})$
2	n *or* $m'n' \equiv 1$	$pm' \equiv 1 \pmod 4$	$\mathcal{O}_L[G](\frac{1+\sqrt{n'\epsilon}}{2})$

3	$n \equiv 1$ $m \equiv 2$	$pn' \equiv 3 \pmod 4$ $N_{L/K}(\epsilon_0) = 1$	*is not an* $A_{M/L}$ *free module.*
4	$m \equiv 1$ $n \not\equiv 1$		$\left(\mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma\right)(\sqrt{n'\epsilon}+1)$
5	$m \equiv 2$ n *or* $m'n' \equiv 3$	$u = 2$ *or* $v = 2$	$\left(\mathcal{O}_L 1_G + \frac{1}{t}\mathcal{O}_L\sigma\right)\left(\left(\frac{\sqrt{m}+\sqrt{2n'\epsilon}}{2} + \frac{t-\sqrt{m}}{2}\right)\right.$
6	$m \equiv 3$ $n \equiv 2$		$\left(\mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma\right)\left(\frac{\sqrt{2n'\epsilon}+2}{2}\right)$
7	$m \equiv 3$ n *or* $m'n' \equiv 1$	$pn' \equiv 3 \pmod 4$	*is not an* $A_{M/L}$ *free module*

Table II

	$m,\ n \equiv \pmod 4$	*Conditions*	$\mathcal{O}_M$
1	$n \equiv 1$	$d = 1$	$\mathcal{O}_L[G](\frac{1+\sqrt{n'}}{2})$
2	$m \equiv 1$ $n \equiv 1$	$d = m$	$\mathcal{O}_L[G](\frac{1+n'}{2})$
3	$m \equiv 2$ $n \equiv 1$	$d = m$ $u = 2$ *or* $v = 2$	$(\mathcal{O}_L 1_G + \frac{1}{t}\mathcal{O}_L\sigma)(\frac{\sqrt{m}+\sqrt{n}}{2} + \frac{t-\sqrt{m}}{2})$
4	$m \equiv 3$ $n \equiv 1$	$d = m$	*is not an* $\Lambda_{M/L}$ *free module.*
5	$m \equiv 1$ $n \not\equiv 1$	$d = 1$ *or* $d = m$	$(\mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma)(\sqrt{n'}+1)$
6	$m \equiv 2$ $n \equiv 3$	$d = \frac{m}{2}$ $u = 2$ *or* $v = 2$	$(\mathcal{O}_L 1_G + \frac{1}{t}\mathcal{O}_L\sigma)(\frac{m+\sqrt{n'}}{2} + \frac{t-\sqrt{m}}{2})$

Proof. (i) **Proofs of the cases of table I.**

Case 1: $m \equiv n \equiv 1 \pmod 4$

Here $\mathcal{O}_M = \{1, \frac{1+\sqrt{n'\epsilon}}{2}\}$. By Theorem 3, M is tame over L. Now, if we take $\alpha = \frac{1+\sqrt{n'}}{2}$, then α satisfies Lemma 1.3 and hence $\mathcal{O}_M = \mathcal{O}_L[G](\alpha)$. This shows that $\mathcal{O}_M$ is a free $A_{M/L}$ module and $\mathcal{O}_M = \mathcal{O}_L[G](\frac{1+\sqrt{n'\epsilon}}{2})$.

Case 2: $n \equiv 1 \pmod 4$ or $m'n' \equiv 1 \pmod 4$

The proof is similar to that of case 1 above.

Case 3: $n \equiv 1 \pmod 4$ and $m \equiv 2 \pmod 4$

Here $\mathcal{O}_M = \{1, \frac{1+\sqrt{m}+\sqrt{n'\epsilon}}{2}\}$. Let $N_{L/K}(\epsilon_0) = 1$. Again by Theorem 3, M is tame over L. We now have to check if there is any $\alpha \in \mathcal{O}_M$ which satisfies Lemma 1.3. If there is any such α then $\alpha = x + y(\frac{1+\sqrt{m}+\sqrt{n'\epsilon}}{2})$ for some $x, y \in \mathcal{O}_L$. Since α satisfies Lemma 1.3, $\{1, \alpha\}$ is an integral basis of M and therefore the discriminant of α is n'. Hence y is a unit in $\mathcal{O}_L$. We can check easily that every unit in $\mathcal{O}_L$ is of the form $a + b\sqrt{m}$ where a and b are odd and even integers respectively. Therefore, $y = p + q\sqrt{m}$ for some p and q in Z where p is an odd integer and q an even integer. Then

$$\begin{aligned} \mathrm{tr}(\alpha) &= 2x + y + y\sqrt{m} \\ &= 2x + (p + q\sqrt{m}) + (p + q\sqrt{m})\sqrt{m} \\ &= (2x + p + qm) + (p + q)\sqrt{m} \\ &= r + s\sqrt{m} \qquad \text{where, r and s are odd} \end{aligned}$$

This implies that $\mathrm{tr}(\alpha)$ can not be a unit in $\mathcal{O}_L$. Therefore, there does not exist any α which satisfies Lemma 1.3. Hence $\mathcal{O}_M$ is not an $\Lambda_{M/L}$ free module.

Case 4: $m \equiv 1 \pmod 4$ and $n \not\equiv 1 \pmod 4$

Here $\mathcal{O}_M = \{1, \sqrt{n'\epsilon}\}$. So $\mathrm{Tr}(\mathcal{O}_M) = (2)$ and consequently, $\mathrm{Tr}(\mathcal{O}_M)$ is a principal ideal of $\mathcal{O}_L$. Moreover, since $\mathcal{O}_M = \mathcal{O}_L[\sqrt{n'\epsilon}]$, $\alpha = \sqrt{n'\epsilon}$ and so we have $\mathrm{tr}(\alpha) = 0$. Thus $\mathrm{tr}(\alpha) \equiv 2 \pmod 2 \mathcal{O}_L$ and hence, from Theorem 7, we conclude that $\mathcal{O}_M$ is an $\Lambda_{M/L}$ free module. Thus $\Lambda_{M/L} = \mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma$ and $\mathcal{O}_M = \left(\mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma\right)(\sqrt{n'\epsilon} + 1)$.

Case 5: $m \equiv 2 \pmod 4$ and n or $m'n' \equiv 3 \pmod 4$

Here $= \mathcal{O}_M\{1, \frac{\sqrt{m}+\sqrt{2n'\epsilon}}{2}\}$. So $\mathrm{Tr}(\mathcal{O}_M) = (2, \sqrt{m})$. We now need to check whether this ideal is principal in $\mathcal{O}_L$. Denote this ideal by I.

If I is principal then, $I = (2, \sqrt{m}) = x + y\sqrt{m}$ for some x and y in Z. This implies $I^2 = (2) = (x^2 + y^2 m + 2xy\sqrt{m})$. Therefore, $N_{L/K}(I^2) = 4 = (x^2 - y^2 m)^2$ i.e., $x^2 - y^2 m = \pm 2$. One can easily verify that whenever there exist x, y in Z such that $x^2 - y^2 m = \pm 2$, the ideal generated by $x + y\sqrt{m}$ in $\mathcal{O}_L$ is the same as I. Therefore, to show that I is a principal ideal

is equivalent to showing that the equation $x^2 - y^2 m = \pm 2$ has solution in Z. Since m is even, x is even. So this equation can be reduced to $2a^2 - y^2 b = \pm 1$, where $a = \frac{x}{2}$ and $b = \frac{m}{2}$. So clearly I is principal in $\mathcal{O}_L$ iff the equation

$$2a^2 - y^2 b = \pm 1 \qquad (1)$$

admits solutions in Z. From the criterian in D. T. Walker [26] (1) has solutions iff $(a\sqrt{2} + y\sqrt{b})^2 = \epsilon_0$. By Lemma 1.1, $a\sqrt{2}+y\sqrt{b} = s\sqrt{u}+t\sqrt{v}$ from which one can deduce immediately that $u = 2$ or $v = 2$. Now if I is principal then $I = (t) = (2a+b\sqrt{m})$ where b is an odd integer. Therefore $\mathrm{tr}(\alpha) = \sqrt{m} \equiv t \pmod{2\mathcal{O}_L}$ (because $2\mathcal{O}_L = 2r + 2s\sqrt{m}$ for r , $s \in Z$). Hence from Theorem 7, $\mathcal{O}_M$ is an $A_{M/L}$ free module and $\mathcal{O}_M = \mathcal{O}_L 1_G + \frac{1}{t}\mathcal{O}_L\sigma(\frac{\sqrt{m}+\sqrt{2n'\epsilon}}{2} + \frac{t-\sqrt{m}}{2})$.

Case 6: $m \equiv 3 \pmod 4$ and $n \equiv 2 \pmod 4$

Here $\mathcal{O}_M = \{1, \frac{\sqrt{2n'\epsilon}}{2}\}$. So $\mathrm{Tr}(\mathcal{O}_M) = (2)$. Now, as in case 4, we can show that $A_{M/L} = \mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma$ and $\mathcal{O}_M = \mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma(\frac{\sqrt{2n'\epsilon}+2}{2})$.

Case 7: $m \equiv 3 \pmod 4$ and n or $m'n' \equiv 1 \pmod 4$

Here $\mathcal{O}_M = \{1, \frac{\sqrt{m}+\sqrt{n'\epsilon}}{2}\}$ and by Theorem 3 M is tame over L. We now have to check if there is any $\alpha \in \mathcal{O}_M$ which satisfies Lemma 1.3. If there is any such α then $\alpha = x+y(\frac{\sqrt{m}+\sqrt{n'\epsilon}}{2})$ for some $x, y \in \mathcal{O}_L$. Since α satisfies Lemma 1.3, $\{1, \alpha\}$ is an integral basis of M and therefore the discriminant of α is n'. Hence y is a unit in $\mathcal{O}_L$. Now if $\epsilon_0 = p + q\sqrt{m}$, where $p, q \in Z$, is a fundamental unit of $\mathcal{O}_L$, then it can be easily checked from congruence conditions that the norm of ϵ_0 can not be -1. So in this case, the fundamental unit (and therefore all other units) has norm 1. From Lemma 1.1, ϵ_0 or ϵ_0^3 has the form $r_1 + r_2\sqrt{m}$ where r_1 is an odd integer and r_2 is an even integer. But if ϵ_0^3 has this form we can easily show that ϵ_0 also has the same form. From the above we get that every unit in $\mathcal{O}_L$ is of the form $h + j\sqrt{m}$ where h is an odd integer and j even. Therefore $y = r + s\sqrt{m}$, where r and s are as above. Now tr $(\alpha) = 2x + y\sqrt{m} = 2x + sm + r\sqrt{m}$. But $x = x_1 + x_2\sqrt{m}$ where $x_1, x_2 \in Z$. Then tr $(\alpha) = k + l\sqrt{m}$ where $k = 2x_1 + sm$ and $l = 2x_2 + r$. But here k is an even integer and l is odd. Therefore, $\mathrm{tr}(\alpha)$ cannot be a unit in $\mathcal{O}_L$, implying that such an α does not exist. Therefore, $\mathcal{O}_M$ is not an $A_{M/L}$ free module.

(ii) **Proofs of the cases of Table II.**

Since the proofs of the cases 1,3 and 6, 4, 5 of Table II is similar to the proofs of the cases

1, 5, 7, 4 of the Table I respectively, it is enough to prove the case 2.

Case(2) $m \equiv n \equiv 1 \pmod 4$. In this case $\mathcal{O}_M = 1, \frac{\sqrt{m}+\sqrt{n'}}{2}$. So $\mathrm{tr}(\mathcal{O}_M) = (2, \sqrt{m})$. Since m is an odd integer $\mathrm{tr}(\mathcal{O}_M) = (1)$. Therefore in this case the extension is tame. So $A_{M/L} = \mathcal{O}_L[G]$. Now since $\mathrm{tr}(\mathcal{O}_M) = (1)$, there exist x and y in $\mathcal{O}_L$ such that $2x + y\sqrt{m} = 1$. Consider $\alpha = \frac{2x+y\sqrt{m}+\sqrt{n'}}{2}$ then obviously $\mathcal{O}_M = \mathcal{O}_L[\alpha]$ and $\mathrm{tr}(\alpha) = 2x + y\sqrt{m} \in (\mathcal{O}_L)^*$. Therefore by Lemma (1.1) we get $\mathcal{O}_M$ is free over $A_{M/L}$ with $\mathcal{O}_M = \mathcal{O}_L[G](\frac{2x+y\sqrt{m}+\sqrt{n'}}{2})$. This completes the proof. ∎

Theorem 9: *Let $M = Q(\sqrt{m}, \sqrt{n})$ be a bicyclic, biquadratic extension of Q and $L = Q(\sqrt{m})$ where $m < 0$. Then the structure of $\mathcal{O}_M$ as an $A_{M/L}$ module can be given as follows:*

	$m,\ n,\ m'n' \equiv \pmod 4$	*Conditions*		$\mathcal{O}_M = A_{M/L}(\alpha)$
1	$n \equiv 1$	$d = 1$	—	$\mathcal{O}_L[G]\left(\frac{1+\sqrt{n'}}{2}\right)$
2	$m \equiv n \equiv 1$	$d = -m$		$\mathcal{O}_L[G](\frac{1-\sqrt{m'n'}}{2})$
3	$m \equiv 1$ $n \not\equiv 1$	d=1		$\left(\mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma\right)(\sqrt{n'}+1)$
4	$m \equiv 1$ $n \not\equiv 1$	d=-m		$\left(\mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma\right)\left(\sqrt{-n'}+1\right)$
5	$m \equiv n \equiv 2$ $m'n' \equiv 1$	$d = -m$		$\mathcal{O}_L[G]\left(\frac{1+\sqrt{-n'}}{2}\right)$
6	$m \equiv n \equiv 2$ $m'n' \equiv 3$	$d = 2$	$m = -2$	$\left(\mathcal{O}_L 1_G + \frac{1}{\sqrt{-2}}\mathcal{O}_L\sigma\left(\frac{\sqrt{m}+\sqrt{2n'}}{2}\right)\right)$
7	$m \equiv 2$ $n \equiv 3$	$d = \frac{-m}{2}$	$m = -2$ $m'n' = -2$	$\left(\mathcal{O}_L 1_G + \frac{1}{\sqrt{-2}}\mathcal{O}_L\left(\frac{\sqrt{m}+\sqrt{-2n'}}{2}\right)\right)$
8	$m \equiv 3$ $n \equiv 1$	$d = \pm m$	$m \neq -1$	*is not an $A_{M/L}$ free module*

9	$m \equiv 3$ $n \equiv 1$	$d = \pm m$	$m = -1$	$\mathcal{O}_L[G](\frac{\sqrt{m}+\sqrt{m'n'}}{2})$
10	$m \equiv 3$ $n \equiv 2$	$d = 1$	$m = -1$	$\left(\mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma\right)\left(\frac{\sqrt{n}+\sqrt{-n}}{2}\right)$
11	$m \equiv n \equiv 3$	$d = 1$	$m \neq -1$	*is not an $A_{M/L}$ free module*
12	$m \equiv n \equiv 3$	$d = 1$	$m = -1$	$\mathcal{O}_L[G]\left(\frac{\sqrt{m}+\sqrt{n}}{2}\right)$
13	$m \equiv n \equiv 3$	$d = \pm m$		$\mathcal{O}_L[G]\left(\frac{1+\sqrt{m'n'}}{2}\right)$

Proof. **Case 1:** $n \equiv 1 \pmod 4$

By Theorem 3, M is tame over L. This implies $A_{M/L} = \mathcal{O}_L[G]$. Now let $\alpha = \frac{(1+\sqrt{n'})}{2}$. Then $\mathrm{tr}(\alpha) = 1 \in \mathcal{O}_L^*$ and $\mathcal{O}_M = \mathcal{O}_L[\alpha]$. Therefore, α satisfies Lemma 1.3 and hence $\mathcal{O}_M = \mathcal{O}_L[G](\alpha)$.

Cases (2), (5), (9), (12) and (13): In all these cases M is tame over L. So following the same procedure as in case 1 one can show that in each of these cases $\mathcal{O}_M = \mathcal{O}_L[G](\alpha)$ for the corresponding α mentioned in the table.

Case 3: $m \equiv 1 \pmod 4$, $n \not\equiv 1 \pmod 4$ and $d = 1$

Since in this case $\mathcal{O}_M = \{1, \sqrt{n'}\}$, $\mathrm{Tr}(\mathcal{O}_M) = (2)$. Therefore $\mathrm{Tr}(\mathcal{O}_M)$ is the principal ideal of $\mathcal{O}_L$. Moreover, since $\mathcal{O}_M = \mathcal{O}_L(\sqrt{n'})$, $\alpha = \sqrt{n'}$ and so we have $\mathrm{tr}(\alpha) = 0$ and $\mathrm{tr}(\alpha) \equiv 2 \pmod{2\mathcal{O}_L}$. Hence, from Theorem 7, we conclude that $\mathcal{O}_M$ is an $A_{M/L}$ free module. Thus $A_{M/L} = \mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma$ and $\mathcal{O}_M = \left(\mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma\right)(\sqrt{n'}+1)$.

Case 4: $m \equiv 1 \pmod 4$, $n \not\equiv 1 \pmod 4$ and $d = -m$

Similar to case 3.

Case 6: $m \equiv n \equiv 2 \pmod 4$ and $m'n' \equiv 3 \pmod 4$

In this case, $\mathcal{O}_M = \{1, \frac{\sqrt{m}+\sqrt{2n'}}{2}\}$. So $\mathrm{tr}(\mathcal{O}_M) = (2, \sqrt{m})$. We now have to check whether this ideal, denoted as I, is principal in $\mathcal{O}_L$. If I is principal then, $I = (2, \sqrt{m}) = (x + y\sqrt{m})$ for some $x, y \in Z$. Now $(x - y\sqrt{m}) = (2, \sqrt{m}) = I$ so that $(2) = I^2 = (x^2 - y^2 m)$. Thus $x^2 - y^2 m = \pm 2$. Clearly, I is principal if and only if there exist solutions to the equation $x^2 - y^2 m = \pm 2$. Now since $x, y \in Z$, x^2 and y^2 are positive. Moreover $m < 0$. So, this equation has solutions if and only if $m = -2$. When $m = -2$, $I = (\sqrt{-2})$. Then $\mathrm{Tr}(\mathcal{O}_M)$ is a principal ideal of $\mathcal{O}_L$. Now since $\mathcal{O}_M = \mathcal{O}_L[\frac{\sqrt{m}+\sqrt{2n'}}{2}]$, $\alpha = \frac{\sqrt{m}+\sqrt{2n'}}{2}$. So

$\mathrm{tr}(\alpha) = \sqrt{m} \equiv \sqrt{-2} \pmod{2\mathcal{O}_L}$. Hence from Theorem 7, $\mathcal{O}_M$ is an $A_{M/L}$ free module with $\mathcal{O}_M = \left(\mathcal{O}_L 1_G + \frac{1}{\sqrt{-2}}\mathcal{O}_L\sigma\right)\left(\frac{\sqrt{m}+\sqrt{2n'}}{2}\right)$.

Case 7: Since $\mathcal{O}_M$ and $\mathcal{O}_L$ are the same as in the previous case, the proof is identical.

Case 8: $m \equiv 3 \pmod 4$, $n \equiv 1 \pmod 4$ and $m \neq -1$

Since $\mathcal{O}_M = \{1, \frac{\sqrt{m}+\sqrt{m'n'}}{2}\}$, by Theorem 3, M is tame over L. Therefore $A_{M/L} = \mathcal{O}_L[G]$. We now need to see if there exists an $\alpha \in \mathcal{O}_M$ which satisfies Lemma 1.3. If there exists such an α then $\alpha = x + y(\frac{\sqrt{m}+\sqrt{m'n'}}{2})$ for some $x, y \in \mathcal{O}_L$. Since α satisfies Lemma 1.3, $\{1, \alpha\}$ is an integral basis. Thus the discriminant of α is n', implying that y is a unit in L. So $y = \pm 1$. Therefore, $\alpha = x \pm \frac{(\sqrt{m}+\sqrt{m'n'})}{2}$ and $\mathrm{tr}(\alpha) = 2x \pm \sqrt{m} = 2x_1 + 2x_2\sqrt{m} + \sqrt{m}$ where $x_1, x_2 \in Z$. By Lemma 1.1 this cannot be a unit in L. So such an α cannot exist. Thus $\mathcal{O}_M$ is not an $A_{M/L}$ free module.

Case 10: $m \equiv 3 \pmod 4$, $n \equiv 2 \pmod 4$ and $m = -1$

In this case, $\mathcal{O}_M = \{1, \frac{\sqrt{n}+\sqrt{-n}}{2}\}$. So $\mathrm{Tr}(\mathcal{O}_M) = (2)$ and is a principal ideal of $\mathcal{O}_L$. Hence, as in case 4 we can show that $A_{M/L} = \mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma$ and $\mathcal{O}_M = (\mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma)(\frac{\sqrt{n}+\sqrt{-n}+2}{2})$.

Case 11: Here $\mathcal{O}_M = \{1, \frac{\sqrt{m}+\sqrt{n}}{2}\}$ and by Theorem 3, M is tame over L. Following the same procedure as in case 8 above, one can show that $\mathcal{O}_M$ is not an $A_{M/L}$ free module.

∎

Theorem 10: *Let M be a cyclic quartic extension of Q and let L be the quadratic subfield of M. If M over L has an integral basis then the conditions under which $\mathcal{O}_M$ is a free $\Lambda_{M/L}$ module and the corresponding structure of $\mathcal{O}_M$ as an $\Lambda_{M/L}$ module in the form $\Lambda_{M/L}(\alpha)$ are as given in the table below.*

	Conditions	$A_{M/L}$	α
1	$D - odd$, $M = L\left(\sqrt{2A\epsilon_0\sqrt{D}}\right)$	$\mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L(\sigma)$	$\sqrt{2A\epsilon_0\sqrt{D}} + 1$
2	$D \equiv 1 \pmod 4$, $A + r \equiv 1 \pmod 4$	$\mathcal{O}_L[G]$	$\frac{1+\sqrt{A\epsilon_0\sqrt{D}}}{2}$

3	$D \equiv 1 \pmod 4$ $\delta = 2$ *and* $A \equiv 3 \pmod 4$ *s-even* $p \equiv q \pmod 4$	$\mathcal{O}_L[G]$	$\frac{1}{2}\left(\frac{p+q\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}\right)$
4	$D \equiv 1 \pmod 4$ $\delta = 2$ $A \equiv 3 \pmod 4$ *s-even* $p \not\equiv q \pmod 4$	$\mathcal{O}_L[G]$	$\frac{1}{2}\left(\frac{j+k\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}\right)$
5	$D \equiv 1 \pmod 4$ $\delta = 2$ $A \equiv 3 \pmod 4$ *s-odd* $p \not\equiv q \pmod 4$	$\mathcal{O}_L[G]$	$\frac{1}{2}\left(\frac{p+q\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}\right)$
6	$D \equiv 1 \pmod 4$ $\delta = 2$ $A \equiv 3 \pmod 4$ *s-odd* $p \equiv q \pmod 4$	$\mathcal{O}_L[G]$	$\frac{1}{2}\left(\frac{l+m\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}\right)$
7	*in all other cases*	$\mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L(\sigma)$	$\sqrt{A\epsilon_0\sqrt{D}} + 1$

Proof. **Case (1)** Here, $\mathcal{O}_M = \left\{1, \sqrt{2A\epsilon_0\sqrt{D}}\right\}$ over $\mathcal{O}_L$. So, $\mathrm{Tr}(\mathcal{O}_M) = (2)$ and is a principal ideal of $\mathcal{O}_L$. Hence, following the same procedure as in the previous theorem's proof, we get $\mathcal{O}_M$ is free over $A_{M/L}$ with $\mathcal{O}_M = (\mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma)\left(\sqrt{2A\epsilon_0\sqrt{D}} + 1\right)$.

Case (2) In this case, $\mathcal{O}_M = \left\{1, \frac{1+\sqrt{A\epsilon_0\sqrt{D}}}{2}\right\}$ over $\mathcal{O}_L$. Now as $\mathrm{tr}\left(\frac{1+\sqrt{A\epsilon_0\sqrt{D}}}{2}\right) = 1$, $\mathrm{Tr}(\mathcal{O}_M) = \mathcal{O}_L$. Therefore, M is tame over L. So by Lemma 1.3, $A_{M/L} = \mathcal{O}_L[G]$. Moreover, since $\mathcal{O}_M = \mathcal{O}_L\left[\frac{1+\sqrt{A\epsilon_0\sqrt{D}}}{2}\right]$, $\alpha = \frac{1+\sqrt{A\epsilon_0\sqrt{D}}}{2}$. Clearly α satisfies Lemma 1.3. Therefore by Lemma 1.3, $\mathcal{O}_M = \mathcal{O}_L[G]\left(\frac{1+\sqrt{A\epsilon_0\sqrt{D}}}{2}\right)$.

Cases (3), (4), (5) and (6) In all these cases, $\mathcal{O}_M = \left\{1, \frac{1}{2}\left(\frac{1+(-1)^s\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}\right)\right\}$. Here $\mathrm{Tr}(\mathcal{O}_M) = \left(2, \frac{1+(-1)^s\sqrt{D}}{2}\right)$

We have to check if this ideal is principal in $\mathcal{O}_L$. Let us denote this ideal by I. If it is principal in $\mathcal{O}_L$, then there exists an $\alpha \in \mathcal{O}_L$ such that $(\alpha) = \left(2, \frac{1+(-1)^s\sqrt{D}}{2}\right)$. Therefore, $\exists\ x, y \in \mathcal{O}_L$ such that $\alpha x = 2$ and $\alpha y = \frac{1+(1)^s\sqrt{D}}{2}$. Now $N_K^L(\alpha)N_K^L(y) = \frac{1-D}{4}$ which is an odd integer since $D \equiv 5 \pmod 8$. Therefore, $N_K^L(\alpha)$ is an odd integer. Moreover, $N_K^L(\alpha)N_K^L(x) = N_K^L(\alpha x) = N_K^L(2) = 4$. This implies that $N_K^L(\alpha) = 1$. Thus α is a unit in $\mathcal{O}_L$. But then since $I = (\alpha)\mathcal{O}_L = \mathcal{O}_L$, $\mathrm{Tr}(\mathcal{O}_M) = \mathcal{O}_L$. Therefore, M is a tame extension of

L. So by Lemma 1.3, $A_{M/L} = \mathcal{O}_L[G]$. To check if $\mathcal{O}_M$ is an $A_{M/L}$ free module one has to check whether there exists an $\alpha \in \mathcal{O}_M$ such that $\mathcal{O}_M = \mathcal{O}_L[\alpha]$ and $\mathrm{tr}(\alpha)$ is a unit in $\mathcal{O}_L$. Note that as $\delta = 2$, $\epsilon_0 = \frac{p+q\sqrt{D}}{2}$, where p, q are odd integers.

If s is an even integer and $p \equiv q \pmod 4$ then, $\frac{(p-1)+(q-1)\sqrt{D}}{4} \in \mathcal{O}_L$. Let $\alpha = \frac{(p-1)+(q-1)\sqrt{D}}{4} + \frac{1}{2}\left(\frac{1+(-1)^s\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}\right)$. Then it is easy to see that the discriminant of $\{1, \alpha\}$ is $A\epsilon_0\sqrt{D}$ and $\alpha \in \mathcal{O}_M$. So $\mathcal{O}_M = \mathcal{O}_L[\alpha]$. Now $\mathrm{tr}(\alpha) = \frac{p+q\sqrt{D}}{2}$ which is a unit in $\mathcal{O}_L$.

So by Lemma 1.3, $\mathcal{O}_M = \mathcal{O}_L[G]\left(\frac{(p-1)+(q-1)\sqrt{D}}{4} + \frac{1}{2}\left(\frac{1+(-1)^s\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}\right)\right)$.

If s is an even integer and $p \not\equiv q \pmod 4$, then one can check that ${\epsilon_0}^2 = \frac{j+k\sqrt{D}}{2}$, where $j \equiv k \pmod 4$. Therefore, $\frac{(j-1)+(k-1)\sqrt{D}}{4} \in \mathcal{O}_L$. Now let

$$\alpha = \frac{(j-1)+(k-1)\sqrt{D}}{4} + \frac{1}{2}\left(\frac{1+(-1)^s\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}\right).$$

Then, just as above, one can check that $\mathcal{O}_M = \mathcal{O}_L[\alpha]$ and $\mathrm{tr}(\alpha) = {\epsilon_0}^2$ which is a unit in $\mathcal{O}_L$. So by Lemma 1.3, $\mathcal{O}_M = \mathcal{O}_L[G]\left(\frac{(j-1)+(k-1)\sqrt{D}}{4} + \frac{1}{2}\left(\frac{1+(-1)^s\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}\right)\right)$.

If s is an odd integer, $\delta = 2$ and $p \not\equiv q \pmod 4$ then since p, q are odd integers, clearly $(p-1) \equiv (q+1) \pmod 4$. Therefore, $\frac{(p-1)+(q+1)\sqrt{D}}{4} \in \mathcal{O}_L$. Let

$$\alpha = \frac{(p-1)+(q+1)\sqrt{D}}{4} + \frac{1}{2}\left(\frac{1+(-1)^s\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}\right).$$

Then, α satisfies Lemma 1.3 and this gives

$$\mathcal{O}_M = \mathcal{O}_L[G]\left(\frac{(p-1)+(q+1)\sqrt{D}}{4} + \frac{1}{2}\left(\frac{1+(-1)^s\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}\right)\right).$$

If s an odd integer, $\delta = 2$ and $p \equiv q \pmod 4$, then one can check that ${\epsilon_0}^2 = \frac{l+m\sqrt{D}}{2}$ where $l - 1 \equiv m + 1 \pmod 4$. Therefore, $\frac{(l-1)+(m+1)\sqrt{D}}{4} \in \mathcal{O}_L$. Let $\alpha = \frac{(l-1)+(m+1)\sqrt{D}}{4} + \frac{1}{2}\left(\frac{1-\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}\right)$. Then α satisfies Lemma 1.3, giving

$$\mathcal{O}_M = \mathcal{O}_L[G]\left(\frac{(l-1)+(m+1)\sqrt{D}}{4} + \frac{1}{2}\left(\frac{1-\sqrt{D}}{2} + \sqrt{A\epsilon_0\sqrt{D}}\right)\right)$$

Case (7) In this case, $\mathcal{O}_M = \left\{1, \sqrt{A\epsilon_0\sqrt{D}}\right\}$ over $\mathcal{O}_L$. Then $\mathrm{Tr}(\mathcal{O}_M) = (2)$ and consequently $\mathrm{Tr}(\mathcal{O}_M)$ is a principal ideal of $\mathcal{O}_L$. Moreover, since $\mathcal{O}_M = \mathcal{O}_L\left[\sqrt{A\epsilon_0\sqrt{D}}\right]$, $\alpha = \sqrt{A\epsilon_0\sqrt{D}}$ and so we have $\mathrm{tr}(\alpha) = 0 \equiv 2 \pmod{2\mathcal{O}_L}$ and hence from Theorem 7, $\mathcal{O}_M$ is an $A_{M/L}$ free module with $\mathcal{O}_M = (\mathcal{O}_L 1_G + \frac{1}{2}\mathcal{O}_L\sigma)\left(\sqrt{A\epsilon_0\sqrt{D}} + 1\right)$. ∎

3 $Z[G]$ basis of $\mathcal{O}_M$

Theorem 11: *Let $M = Q(\sqrt{m}, \sqrt{n})$ be a bicyclic, biquadratic extension of Q and let $L = Q(\sqrt{m})$. If M/L has an integral basis then a $Z[G]$ basis of $\mathcal{O}_M$ (whenever M is tame over L) can be given as follows:*

	$m,\ n,\ m'n' \equiv \pmod 4$	$\{\alpha, \beta\}$
1	$m \equiv n \equiv 1$	$\{\frac{1+\sqrt{m'n'}}{2},\ \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m'n'}}{4}\}$
2	$n \equiv 1,\ m \not\equiv 1$	$\{\frac{1+\sqrt{n}}{2},\ \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m'n'}}{2}\}$
3	$m'n' \equiv 1,\ m \equiv n \not\equiv 1$	$\{\frac{1+\sqrt{m'n'}}{2},\ \frac{1+\sqrt{m}+\sqrt{n}+\sqrt{m'n'}}{2}\}$

Proof. Let $G = (g_1, g_2)$ where g_1 is the identity map and $g_2 : \sqrt{n} \to -\sqrt{n}$. In each case we show that α and β are generators of $\mathcal{O}_M$ over $Z[G]$ by showing $\mathcal{O}_M = Z\{\alpha, g_2(\alpha), \beta, g_2(\beta)\}$. It suffices to show that generators of $\mathcal{O}_M$ can be written as linear combination of $\alpha, g_2(\alpha), \beta$ and $g_2(\beta)$ over Z, The reverse containment ($Z\{\alpha, \beta, g_2(\alpha), g_2(\beta)\} \subseteq \mathcal{O}_M$) is obvious.

Case 1: $m \equiv n \equiv 1 \pmod 4$

Here $\alpha + g_2(\alpha) = 1$, $\beta + g_2(\beta) = \frac{1+\sqrt{m}}{2}$ and $\beta - g_2(\beta - \alpha) = \frac{1+\sqrt{n}}{2}$.

Case 2: $n \equiv 1,\ m \not\equiv 1$

Here $\alpha + g_2(\alpha) = 1$ and $\beta - \alpha - g_2(\alpha - \beta) = \sqrt{m}$.

Case 3: $m'n' \equiv 1,\ m \equiv n \not\equiv 1$

Here $\alpha + g_2(\alpha) = 1$, $\beta - \alpha + g_2(\beta - \alpha) = \sqrt{m}$ and $\beta - \alpha - g_2(\beta - \alpha) = \sqrt{n}$. Since in each case, we have shown that the generators are linear combinations of $\alpha, g_2(\alpha), \beta$ and $g_2(\beta)$ over Z, we are done. ∎

Theorem 12: *Let M be a cyclic quartic extension of Q with quadratic subfield $L = Q(\sqrt{d})$. If M/L has an integral basis then a $Z[G]$ basis of $\mathcal{O}_M$ (whenever M is tame over L) can be given as follows.*

Conditions	$\{\alpha, \beta\}$
$D \equiv 1 \pmod 4$ $\Lambda + r \equiv 1 \pmod 4$ $\delta = 0$	$\frac{1+\sqrt{\Lambda c_0 \sqrt{D}}}{2}$, $\frac{1+\sqrt{\Lambda c_0 \sqrt{D}+\sqrt{D}+\sqrt{D}\sqrt{\Lambda\sqrt{D}c_0}}}{4}$

$D \equiv 1 \pmod 4$ $A \equiv 3 \pmod 4$ $\delta = 2$	$\frac{1+\sqrt{D}}{2}\left(\frac{1+\sqrt{D}}{2}+\sqrt{A\epsilon_0\sqrt{D}}\right)^{\frac{1}{2}}, \quad \left((\frac{1+\sqrt{D}}{2})^2+1+\sqrt{A\epsilon_0\sqrt{D}}\right)^{\frac{1}{2}}$

Proof. Here g_1 is the identity map and $g_2\sqrt{(A\epsilon_0\sqrt{D})} = -\sqrt{(A\epsilon_0\sqrt{D})}$. Like in the bicyclic biquadratic case we have to find some $\alpha, \beta \in \mathcal{O}_M$ such that $\alpha, \beta, g_2(\alpha)$ and $g_2(\beta)$ generate $\mathcal{O}_M$ over Z. We will follow the same procedure like in bicyclic biquadratic case and show that generators of $\mathcal{O}_M$ can be written as linear combinations of $\alpha, \beta, g_2(\alpha)$ and $g_2(\beta)$ over Z.
Case(1) $\beta = \frac{1+\sqrt{A\epsilon_0\sqrt{D}}+\sqrt{D}+\sqrt{D}\sqrt{A\epsilon_0\sqrt{D}}}{4}$ and $\alpha = \frac{1+\sqrt{A\epsilon_0\sqrt{D}}}{2}$. Then

$$\begin{aligned}\alpha + g_2(\alpha) &= \frac{1+\sqrt{A\epsilon_0\sqrt{D}}}{2} + \frac{1-\sqrt{A\epsilon_0\sqrt{D}}}{2} = 1, \text{ and}\\ \beta + g_2(\beta) &= \beta + \frac{1-\sqrt{A\epsilon_0\sqrt{D}}+\sqrt{D}-\sqrt{D}\sqrt{A\epsilon_0\sqrt{D}}}{4}\\ &= \tfrac{1+\sqrt{D}}{2}\end{aligned}$$

Therefore $\{\alpha, \beta\}$ form a $Z[G]$ basis for $\mathcal{O}_M$.
Case (2) Let $\alpha = \frac{1+\sqrt{D}}{2}\left(\frac{1+\sqrt{D}}{2}+\sqrt{A\epsilon_0\sqrt{D}}\right)^{\frac{1}{2}}$ and $\beta = ((\frac{1+\sqrt{D}}{2})^2+1+\sqrt{A\epsilon_0\sqrt{D}})^{\frac{1}{2}}$. Then $\mathrm{tr}(\beta) - \mathrm{tr}(\alpha) = 1$. Now consider $\beta = (\frac{1+2\sqrt{D}+D}{4}+1+\sqrt{A\epsilon_0\sqrt{D}})^{\frac{1}{2}} = (\frac{5+D+2\sqrt{D}}{4}+\sqrt{A\epsilon_0\sqrt{D}})^{\frac{1}{2}}$. In this case one can show that $D \equiv 5 \pmod 8$. Therefore, we can write D as $8x+5$ for some $x \in Z$. Substituting the value of D we get $\beta = (\frac{10+8x+2\sqrt{D}}{4}+\sqrt{A\epsilon_0\sqrt{D}})^{\frac{1}{2}} = \frac{4+4x}{4} + (\frac{1+\sqrt{D}}{2}+\sqrt{A\epsilon_0\sqrt{D}})^{\frac{1}{2}}$. Therefore, $(\frac{1+\sqrt{D}}{2}+\sqrt{A\epsilon_0\sqrt{D}})^{\frac{1}{2}} = (1+x)(tr(\alpha)-tr(\beta))+\beta$. This implies that α and β form a $Z[G]$ basis for $\mathcal{O}_M$. ∎

3 Galois module structure for Kummer extensions of degree 3 and 4.

In this chapter we give an Explicit Galois Module Structure result for the following cases:

1. $K = Q(\omega)$, $L = K[\sqrt[3]{A}]$, where ω is a primitive cube root of unity and $A = fg^2$ is a cube free integer for some $f, g \in \mathcal{O}_K$ and $f, g \not\equiv -1 \pmod{\sqrt{-3}}$.

2. $K = Q(\iota)$, $L = K(\sqrt[4]{a})$ where $\iota^2 = -1$ and a is an integer which is fourth power free.

In the first section of this chapter we will prove the result in the cubic case and in the second section we will give proof for the quartic case.

1 Cubic Galois extensions of $Q[\omega]$

Throughout this section, $K = Q[\omega]$ and $L = K[\sqrt[3]{A}]$, $A = fg^2$ is a cube free integer for some $f, g \in \mathcal{O}_K$ and $f, g \not\equiv -1 \pmod{\sqrt{-3}}$. Here $\mathcal{O}_L$ and $\mathcal{O}_k$ are rings of integers of L and K respectively. Let $\theta = \sqrt[3]{A}$ and $\theta^* = \theta^2/g$.

Theorem 13: (Wada [25]) *Let $K = Q[\omega]$, $L = K[\sqrt[3]{A}]$ and let $\mathcal{O}_L$ and $\mathcal{O}_K$ denote rings of integers of L and K respectively then, a basis for $\mathcal{O}_L$ over $\mathcal{O}_k$ is as follows:*

$\{1, \theta, \theta^*\}$ when $f \not\equiv g \pmod 3$,

$\{1, \theta, \frac{(1+\theta+\theta^*)}{\sqrt{-3}}\}$ when $f \equiv g \pmod 3$ and $f \not\equiv g \pmod{3\sqrt{-3}}$

$\{1, \frac{(1-\theta)}{\sqrt{-3}}, \frac{(f+\theta+\theta^*)}{3}\}$ when $f \equiv g \pmod{3\sqrt{-3}}$

A primitive cube root of unity ω is fixed once for all. Let $\sigma \in G = Gal(L/K)$ be defined by $\sigma(\theta) = \omega\theta$, and χ, a character of G be defined by $\chi(\sigma) = \omega\sigma$. For $1 \leq i \leq 3$, let

$\chi_i = \chi^i$ and $e_i = \frac{1}{3}\sum_{n=1}^{3} \chi_i(\sigma^n)\sigma^{-n}$ denote the idempotent in KG corresponding to χ_i. Then, $M = \oplus_{n=1}^{n=3}\mathcal{O}_K.e_i$ is the maximal $\mathcal{O}_K$-order in KG and $\mathcal{A}_{L/K} \subset M$. So, any element $\underline{x}$ in $\mathcal{A}_{L/K}$ can be written uniquely in the form $\sum_{n=1}^{n=3} x_i e_i$ for some $x_i \in \mathcal{O}_K$.

In this section, the associated order is determined by determining the conditions on x_i. For this, the basis given by Wada will be used.

Theorem 14: *Let $K = Q[\omega]$, $L = K[\sqrt[3]{A}]$ and let $\mathcal{O}_L$ and $\mathcal{O}_K$ denotes rings of integers of L and K. Then the associated order and the structure of $\mathcal{O}_L$ as an $\mathcal{A}_{L/K}$ module, is as follows:*

Conditions	$\mathcal{A}_{L/K}$	Generator γ
$f \not\equiv g \pmod 3$	$\mathcal{O}_K e_1 + \mathcal{O}_K e_2 + \mathcal{O}_K e_3$	$1 + \theta + \theta^*$
$f \equiv g \pmod 3$ $f \not\equiv g \pmod{3\sqrt{-3}}$	$\mathcal{O}_K(e_1 + e_2 + e_3) +$ $\sqrt{-3}\mathcal{O}_K e_1 + \sqrt{-3}\mathcal{O}_K e_2$	$\frac{1 + \theta + \theta^*}{\sqrt{-3}}$
$f \equiv g \pmod{3\sqrt{-3}}$	$\mathcal{O}_K G$	$\frac{u + \theta + \theta^*}{3}$

Proof. **Case 1:** $f \not\equiv g \pmod 3$. Here, by Wada's result, $\{1, \theta, \theta^*\}$ is an integral basis for $\mathcal{O}_L$ over $\mathcal{O}_K$. One checks that every element of the maximal order takes the basis elements into $\mathcal{O}_L$. So, the maximal order is the associated order. Taking $\gamma = 1 + \theta + \theta^*$, one verifies that $\mathcal{O}_L = \mathcal{A}_{L/K}.\gamma$.

Case 2: $f \equiv g \pmod 3$ and $f \not\equiv g \pmod{3\sqrt{-3}}$. The integral base in this case is $\{1, \theta, (1 + \theta + \theta^*)/\sqrt{-3}\}$. One easily checks that $M = \oplus \mathcal{O}_L.v_i$ where

$$v_1 = e_3; \qquad v_2 = e_1; \qquad v_3 = e_1 + e_2 + e_3.$$

Now, if $\underline{x} = \sum_{n=1}^{n=3} x_i v_i \in \mathcal{A}_{L/K}$, it takes every element of the basis into $\mathcal{O}_L$ if and only if,

$$\underline{x}\frac{(1 + \theta + \theta^*)}{\sqrt{-3}} = \left(\frac{x_1}{\sqrt{-3}} + \frac{x_2}{\sqrt{-3}}\theta + x_3\frac{(1 + \theta + \theta^*)}{\sqrt{-3}}\right) \in \mathcal{O}_L.$$

This implies that

$$x_1 \equiv 0 \pmod{\sqrt{-3}}; \quad x_2 \equiv 0 \pmod{\sqrt{-3}}; \quad x_3 \text{ arbitrary.}$$

Now from the relations

$$\sqrt{-3}v_1.\gamma = 1; \quad \sqrt{-3}v_2.\gamma = \theta; \quad v_3.\gamma = \gamma.$$

it follows that $\gamma = (1 + \theta + \theta^*)/\sqrt{-3}$ is a generator of $\mathcal{O}_L$ over $\mathcal{A}_{L/K}$.

Case 3: $f \equiv g \pmod{3\sqrt{-3}}$. Since the sixth roots of unity are distinct (mod 3), one can find a root of unity u such that $f \equiv u \pmod 3$. So, $(u + \theta + \theta^*)/3$ is an integer. Recall that for an abelian tame extension, an element $\gamma \in \mathcal{O}_L$ generates $\mathcal{O}_L$ over $\mathcal{O}_K G$ if and only if

$$\left(\prod_{\chi}(\gamma, \chi)\right)^2 = \text{Discriminant of } L/K$$

where the product is over the characters of the Galois group $G = Gal(L/K)$ and $(\gamma, \chi) = \sum_{g \in G} \chi(g) g^{-1}(\gamma)$ is the *resolvent* of γ with respect to χ. In this case the discriminant of the extension L over K is $(fg)^2$. One can check that $\left(\prod_\chi(\gamma, \chi)\right)$ for $\gamma = (u + \theta + \theta^*)/3$ is $(u\theta\theta^*) = (fg)$. ∎

2 Quartic extensions of $Q[\iota]$

In this section, f, g and h denote square free positive integers such that $f > 1$ and h is odd. Also, $\eta = \sqrt[4]{fg^2h^3}$, $\overline{\eta} = \sqrt{fh}$, $\overline{\overline{\eta}} = \sqrt[4]{f^3g^2h}$,

$$\alpha = \begin{cases} (1 + \iota)\eta & \text{when } g \text{ is odd.} \\ \left(\frac{1+\iota}{2}\right)\eta & \text{when } g \text{ even.} \end{cases}$$

and

$$\overline{\overline{\alpha}} = \begin{cases} (\iota - 1)\overline{\overline{\eta}} & \text{when } f \text{ and } g \text{ odd.} \\ \left(\frac{\iota-1}{2}\right)\overline{\overline{\eta}} & \text{when } f \text{ or } g \text{ even.} \end{cases}$$

Throughout this section $K = Q[\iota]$, $L = Q(\eta, \iota)$ and $\mathcal{O}_L$ and $\mathcal{O}_K$ are rings of integers of L and K respectively. Let $\sigma \in G = Gal(L/K)$ be defined by $\sigma(\eta) = \iota\eta$. Let χ be the character of G defined by $\chi(\sigma) = \iota$. Then $\chi_i = \chi^i$, $1 \le i \le 4$ gives all the characters of G. Let $e_i = \frac{1}{4}\sum_{n=1}^{4} \chi_i(\sigma^n)\sigma^{-n}$ be the corresponding idempotents in KG. The maximal order is $M = \oplus_{n=1}^{4} \mathcal{O}_K.e_i$.

The following result, due to Parry and Hymo [11], gives a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$.

Theorem 15: (Parry-Hymo) *$K = Q[\iota]$, $L = Q(\eta, \iota)$ and $\mathcal{O}_L$ and $\mathcal{O}_K$ are rings of integers of L and K respectively. Then an integral basis of L over K is as follows:*

$$\left\{1, \frac{\eta(1+\iota)+\overline{\overline{\eta}}}{2}, \frac{\overline{\eta}(i+\iota)}{2}, \frac{\overline{\overline{\eta}}(1+\iota)}{2}\right\} \quad \text{when} \quad fh \equiv 2 \pmod 4, \quad g\text{—odd},$$

$$\left\{1, \eta, \frac{1+\iota\overline{\eta}}{2}, \frac{\eta+\iota\overline{\overline{\eta}}}{2}\right\}, \quad \text{when} \quad fh \equiv 3 \pmod 4, \quad g\text{—odd},$$

$$\left\{1, \frac{1+\iota\overline{\eta}}{2}, \frac{1+\eta+\overline{\eta}}{2}, \frac{1+3\iota+\eta+(1+\iota)\overline{\eta}+(-1)^{(h-1)/2}\iota\overline{\overline{\eta}}}{4}\right\} \quad \text{when} \quad fh \equiv 3 \pmod 8, \quad g\text{—even},$$

$$\left\{1, \frac{1+\iota\overline{\eta}}{2}, \frac{1+\eta+(g/2)h\overline{\eta}}{2}, \frac{1+(g/2)f\iota+\eta+((g/2)h+\iota)\overline{\eta}+(-1)^{(h-1)/2}\iota\overline{\overline{\eta}}}{4(1+\iota)}\right\}, \quad \text{when} \quad fh \equiv 7 \pmod 8, \quad g\text{—even},$$

$$\left\{1, \alpha, \frac{1+\iota\overline{\alpha}}{2}, \frac{\alpha+\iota\overline{\overline{\alpha}}}{2}\right\} \quad \text{when} \quad fh \equiv 1 \pmod 4, \quad g\text{—even},$$

$$\left\{1, \frac{1+\iota\overline{\alpha}}{2}, \frac{1+\alpha+\overline{\alpha}}{2}, \frac{1+3\iota+\alpha+(1+\iota)\overline{\alpha}+(-1)^{(h-1)/2}\iota\overline{\overline{\alpha}}}{4}\right\}, \quad \text{when} \quad fh \equiv 5 \pmod 8 \quad g\text{—odd},$$

$$\left\{1, \frac{1+\iota\alpha}{2}, \frac{1+\alpha+gh\overline{\alpha}}{2}, \frac{1-gf\iota+\alpha+(gh+\iota)\overline{\alpha}+(-1)^{(h-1)/2}\iota\overline{\overline{\alpha}}}{4(1+\iota)}\right\} \quad \text{when} \quad fh \equiv 1 \pmod 8 \quad g\text{—odd}.$$

Now $\mathcal{A}_{L/K}$ and the structure of $\mathcal{O}_L$ as an $\mathcal{A}_{L/K}$ module will be determined.

Theorem 16: *$K = Q[\iota]$,$L = Q(\eta, \iota)$ and $\mathcal{O}_L$ is the ring of integers of L. The associated order and the structure of $\mathcal{O}_L$ as an $\mathcal{A}_{L/K}$- module is as follows:*

Conditions	$\mathcal{A}_{L/K}$	γ
$fh \equiv 2 \pmod 4$ g-odd	$\mathcal{O}_K e_4 + \mathcal{O}_K e_2$ $+(1+\iota)\mathcal{O}_K e_1 + \mathcal{O}_K.1$	$\frac{2+\overline{\overline{\eta}}+\eta(1+\iota)+\overline{\eta}(1+\iota)}{2}$
$fh \equiv 3 \pmod 4$ g-odd	$2\mathcal{O}_K.e_4 + 2\mathcal{O}_K.e_1 +$ $\mathcal{O}_K(e_1+e_3) + \mathcal{O}_K.1$	$\frac{1+\eta+\iota\overline{\eta}+\iota\overline{\overline{\eta}}}{2}$
$fh \equiv 3 \pmod 8$ g-even	$2(1+\iota)\mathcal{O}_K e_2 + (1+\iota)\mathcal{O}_K(e_2+e_4)$ $+2\mathcal{O}_K(e_1+e_2) + \mathcal{O}_K.1$	$\frac{1-\iota+\eta+(1+\iota)\overline{\eta}+(-1)^s\iota\overline{\overline{\eta}}}{4}$

$fh \equiv 1 \pmod 4$ g-even	$2\mathcal{O}_K.e_4 + 2\mathcal{O}_K.e_1$ $+\mathcal{O}_K(e_1+e_3) + \mathcal{O}_K.1$	$\frac{1+\alpha+\iota\overline{\alpha}+\iota\overline{\overline{\alpha}}}{2}$
$fh \equiv 5 \pmod 8$ g-even	$2(1+\iota)\mathcal{O}_K.e_4 + (1+\iota).\mathcal{O}_K(e_2+e_4)$ $+2\mathcal{O}_K(e_1+e_2) + \mathcal{O}_K.1$	$\frac{1-\iota+\alpha+(1+\iota)\overline{\alpha}+(-1)^s\iota\overline{\overline{\alpha}}}{4}$
$fh \equiv 7 \pmod 8$ g-even	$\mathcal{O}_K G$	$\frac{u(1+\iota)+\eta+(1+\iota)u\overline{\eta}+(-1)^s\iota\overline{\overline{\eta}}}{4(1+\iota)}$
$fh \equiv 1 \pmod 8$ g-odd	$\mathcal{O}_K G$	$\frac{u(1+\iota)+\alpha+(1+\iota)u\overline{\alpha}+(-1)^s\iota\overline{\overline{\alpha}}}{4(1+\iota)}$

Proof. Here, two of the extensions are tame and the others are non-tame. Proofs will be given for a typical tame case and a typical non-tame case. The proofs for the other cases are analogous.

Non-tame case. $fh \equiv 3 \pmod 8$, g-even. Let

$$v_1 = e_4; \qquad v_2 = e_2 + e_4; \qquad v_3 = e_1 + e_2; \qquad v_4 = e_1 + e_2 + e_3 + e_4 = id.$$

Note that v_i's span the maximal order M in KG over $\mathcal{O}_K$:

$$M = \oplus_{n=1}^{n=4} \mathcal{O}_K v_n.$$

The integral base in this case is,

$$\alpha_1 = 1, \quad \alpha_2 = \frac{1+\iota\overline{\eta}}{2}, \quad \alpha_3 = \frac{1+\eta+\overline{\eta}}{2}, \quad \alpha_4 = \frac{1-\iota+\eta+(1+\iota)\overline{\eta}+(-1)^{(h-1)/2}\iota\overline{\overline{\eta}}}{4(1+\iota)}.$$

Let $\underline{x} = x_1v_1 + x_2v_2 + x_3v_3 + x_4v_4 \in M$. Then, a necessary and sufficient condition for $\underline{x}$ to be in $\mathcal{A}_{L/K}$ is that $\underline{x}\alpha_i \in \mathcal{O}_L$, for $1 \le i \le 4$. Applying $\underline{x}$ to α_2, we get

$$\underline{x}\alpha_2 = \frac{x_1 - x_3}{2} + (x_2 + x_3 + x_4)\alpha_2.$$

Thus, $\underline{x}\alpha_2 \in \mathcal{O}_L$ if and only if $x_1 \equiv x_3 \pmod 2$. Applying $\underline{x}$ to α_3 one deduces that $\underline{x}\alpha_3 \in \mathcal{O}_L$ if and only if $x_1 - x_3 + (1+\iota)x_2 \equiv 0 \pmod 2$. Applying $\underline{x}$ to α_4, one deduces that $\underline{x}\alpha_4 \in \mathcal{O}_L$ if and only if $x_1 \equiv (1+\iota)x_3 \pmod{2(1+\iota)}$ and $(1+\iota)x_2 \equiv x_3 \pmod 2$. One easily checks that all these conditions are together equivalent to the following conditions:

$$x_1 \equiv 0 \pmod{2(1+\iota)}; \quad x_2 \equiv 0 \pmod{(1+\iota)}; \quad x_3 \equiv 0 \pmod 2; \quad x_4 \text{ arbitrary.}$$

Now if $\gamma = \dfrac{1-\iota+\eta+(1+\iota)\overline{\eta}+(-1)^{(h-1)/2}\iota\overline{\overline{\eta}}}{4}$ then it can be easily checked that

$$\mathcal{A}_{L/K}.\gamma = \mathcal{O}_K\alpha_1' + \mathcal{O}_K\alpha_2' + \mathcal{O}_K\alpha_3' + \mathcal{O}_K\alpha_4',$$

where,

$$\alpha_1' = \alpha_1; \quad \alpha_2' = \alpha_2; \quad \alpha_3' = -\alpha_1 + \alpha_2 + \alpha_3; \quad \alpha_4' = \alpha_4.$$

The determinant of the matrix that maps $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ to $\{\alpha_1', \alpha_2', \alpha_3', \alpha_4'\}$ is one. Therefore $\{\alpha_1', \alpha_2', \alpha_3', \alpha_4'\}$ is also an integral basis for L/K. Therefore γ generates $\mathcal{O}_L$ over $\mathcal{A}_{L/K}$ i.e. $\mathcal{A}_{L/K}.\gamma = \mathcal{O}_L$.

Tame case. $fh \equiv 7 \pmod 8$. A generator of $\mathcal{O}_L$ over $\mathcal{O}_K G$ will be constructed by modifying suitably the last element of the integral basis. Let $g_1 = (g/2)$. Since $fh \equiv -1 \pmod 8$, it follows that $h \equiv -f \pmod 8$. From the observation made at the beginning,

$$\frac{1+g_1f\iota+\eta+(\iota-g_1f)\overline{\eta}+(-1)^{(h-1)/2}\iota\overline{\overline{\eta}}}{4(1+\iota)} = \frac{1+g_1f\iota+\eta+(1+g_1f\iota)\iota\overline{\eta}+(-1)^{(h-1)/2}\iota\overline{\overline{\eta}}}{4(1+\iota)}$$

is also an integer. In each of the following cases, one checks that the square of the product of the resolvents of the modified element over the characters of G equals the field discriminant which is, in the present case, $f^3g^2h^3/4$.

If $g_1f \equiv 1 \pmod 8$ then

$$\frac{1+\iota+\eta+(1+\iota)\iota\overline{\eta}+(-1)^{(h-1)/2}\iota\overline{\overline{\eta}}}{4(1+\iota)}$$

is an integer and, in fact, is a generator of $\mathcal{O}_L$ over $\mathcal{A}_{L/K}$.

If $g_1f \equiv 3 \pmod 8$, then,

$$\begin{aligned}\frac{1+3\iota+\eta+(1+3\iota)\iota\overline{\eta}+(-1)^{(h-1)/2}\iota\overline{\overline{\eta}}}{4(1+\iota)} - \frac{1+\iota\eta}{2} \\ = \frac{-1+\iota+\eta+(-1+\iota)\iota\overline{\eta}+(-1)^{(h-1)/2}\iota\overline{\overline{\eta}}}{4(1+\iota)}\end{aligned}$$

is an integer and this generates $\mathcal{O}_L$ over $\mathcal{O}_K G$.

Similarly, if $g_1f \equiv 5 \pmod 8$,

$$\begin{aligned}\frac{1+5\iota+\eta+(1+5\iota)\iota\overline{\eta}+(-1)^{(h-1)/2}\iota\overline{\overline{\eta}}}{4(1+\iota)} + \iota\frac{1+\iota\eta}{2} \\ = \frac{-1+7\iota+\eta+(-1+7\iota)\iota\overline{\eta}+(-1)^{(h-1)/2}\iota\overline{\overline{\eta}}}{4(1+\iota)}\end{aligned}$$

is an integer. So, $\frac{-1-\iota+\eta+(-1-\iota)\iota\overline{\eta}+(-1)^{(h-1)/2}\iota\overline{\overline{\eta}}}{4(1+\iota)}$ is an integer and this is a generator.

If $g_1 f \equiv 7 \pmod 8$,

$$\frac{1-\iota+\eta+(1-\iota)\iota\overline{\eta}+(-1)^{(h-1)/2}\iota\overline{\overline{\eta}}}{4(1+\iota)}$$

is an integer and this generates $\mathcal{O}_L$ over $\mathcal{O}_K G$. ∎

4 Galois Module Structure of Quartic Galois Extension of $Q(\iota)$

In this chapter we will find explicitly the associated order and structure of $\mathcal{O}_F$ as an $\mathcal{A}_{F/K}$-module for the case when $K = Q(\iota)$ and $F = K(\sqrt[4]{fg^2h^3})$, where f, g and h are pairwise coprime, squarefree integers in $Z[\iota]$.

In the first section, we will give notation used in this chapter. In the second section, we will give an integral basis for F over K. In the 3rd section we will prove Galois Module structure result when F over K is tame and in the 4th section we will prove Galois Module structure result when F over K is a non-tame extension.

1 Notation

Let f, g and h be pairwise coprime, squarefree integers in $Z[\iota]$. $\alpha = \sqrt[4]{fg^2h^3}$, $\alpha^2 = gh\sqrt{fh}$, $m = fg^2h^3$. $K = Q(\iota)$, $L = K(\sqrt{fh})$, $F = K(\sqrt[4]{fg^2h^3})$. $\mathcal{O}_K$, $\mathcal{O}_L$, $\mathcal{O}_F$ are rings of integers of K, L and F respectively. Let $G = Gal(F/K)$. We fix a primitive fourth root of unity ι. We define $\sigma \in G$ by $\sigma(\alpha) = \iota\alpha$. Then, G is generated by σ. Let χ be the character defined by $\chi(\sigma) = \iota\sigma$. Then χ generates the group $\hat{G}$ of characters of G. $\chi_i = \chi^i$ are the characters of G. $e_i = \frac{1}{4}\sum_{n=1}^{4} \chi_i(\sigma^n)\sigma^{-n}$is the idempotent corresponding to the character χ_i. Let $G_i(F/K)$(resp.$G_i(L/K)$) denote the i^{th}−ramification group of the extension F/K(resp. L/K).

2 Integral Basis

In this section we determine an integral basis for the extension F/K. When f, g and h are rational integers, this was done by Parry and Hymo in [12].

Let R be a P.I.D with quotient field K, where K is a finite extension of Q. Let N be an extension of degree n over K and S, the integral closure of R in N. Let $\alpha \in S$ be such that $K(\alpha) = N$. We have the following result (cf. [15]):

There exist $d_1, d_2, \ldots, d_n \in R$ *and monic polynomials* $f_i(X) \in R[X]$, $1 \leq i \leq n-1$, $deg(f_i(X)) = i$, *such that* $\{1, \frac{f_1(\alpha)}{d_1}, \frac{f_2(\alpha)}{d_2} \ldots, \frac{f_{n-1}(\alpha)}{d_{n-1}}\}$ *is a basis for* S *over* R. *Further,* d_i*'s satisfy the following conditions:*

1. $d_i d_j \mid d_{i+j}$ *if* $i + j < n$.

2. $(d_1 d_2 \ldots d_{n-1})^2 disc(S/R) = disc(\alpha)$.

3. *The* f_i*'s can be replaced by any monic polynomial* g *of the same degree such that* $\frac{g(\alpha)}{d_i} \in S$.

4. $d_1^{n(n-1)} \mid disc(\alpha)$.

5. *If* $\frac{g(\alpha)}{n} \in S$ *for some monic polynomial* $g(X) \in R[X]$ *of degree* i *and* $n \in R$, $n \mid d_i$.

In particular, if N/K *is quadratic and* $\alpha = \sqrt{\gamma}$, $\gamma \in R$, γ *square free, then* $\{1, \frac{a+\sqrt{\gamma}}{d}\}$ *is an integral basis for* S *over* R. *Then,*

6. $d^2 \mid 4$.

7. $x^2 \equiv \gamma \pmod{d^2}$ *has a solution and* d^2 *is the largest square divisor of* 4 *for which this congruence has a solution.*

Since $Z[\iota]$ is a P.I.D, there is a basis

$$\left\{1, \alpha_2 = \frac{a+\alpha}{d_1}, \alpha_3 = \frac{b+c\alpha+\alpha^2}{d_2}, \alpha_4 = \frac{d+e\alpha+f\alpha^2+\alpha^3}{d_3}\right\}.$$

We will determine d_1, d_2, d_3 and the reader can easily check that the elements in the integral basis given in the following table are integers.

Before we prove the theorem we will give an integral basis for L/K. This follows from the general statements about quadratic extensions and the following facts. (a) ± 1 are the only squares $\pmod{4Z[\iota]}$, (b) $\pm 1 + 2\iota$ is a square $\pmod 2$, but not a square $\pmod 4$, (c) $\iota, 1+\iota$ are non squares $\pmod 2$ and $2(1+\iota)$ is not a square $\pmod 4$.
The integral basis for L/K is as follows:

Case	Integral basis	Discriminant
$fh \equiv 1 \pmod 4$	$\{1, \frac{1+\sqrt{fh}}{2}\}$	fh
$fh \equiv -1 \pmod 4$	$\{1, \frac{\iota+\sqrt{fh}}{2}\}$	fh
$fh \equiv 1+2\iota \pmod 4$	$\{1, \frac{1+\sqrt{fh}}{1+\iota}\}$	$2fh$
$fh \equiv -1+2\iota \pmod 4$	$\{1, \frac{\iota+\sqrt{fh}}{1+\iota}\}$	$2fh$
$fh \equiv \iota \pmod 2$ or $0 \pmod{1+\iota}$	$\{1, \sqrt{fh}\}$	$4fh$

Theorem 17: *An integral basis of F over K can be given as follows:*

Condition	*Integral Basis*
$m \equiv 1 \pmod 8$	$1, \ \frac{1+\alpha}{1+\iota}, \ \frac{\lvert gh\rvert^2(\iota+(1+\iota)\alpha)+\alpha^2}{2(1+\iota)gh}, \ \frac{\lvert gh^2\rvert^2(1+\alpha+\alpha^2)+\alpha^3}{4gh^2}$
$m \equiv 1+4\iota \pmod 8$	$1, \ \frac{1+\alpha}{1+\iota}, \ \frac{\lvert gh\rvert^2(-\iota+(1+\iota)\alpha)+\alpha^2}{2(1+\iota)gh}, \ \frac{\lvert gh^2\rvert^2(2-\iota+\alpha+\iota\alpha^2)+\alpha^3}{4gh^2}$
$m \equiv 2\iota \pmod 4$ $fh \equiv 1 \pmod 4$	$1, \ \alpha, \ \frac{gh+\alpha^2}{2gh}, \ \frac{\alpha+\alpha^3/gh^2}{2}$
$m \equiv 2\iota \pmod 4$ $fh \equiv -1 \pmod 4$	$1, \ \alpha, \ \frac{\iota gh+\alpha^2}{2gh}, \ \frac{\iota\alpha+\alpha^3/gh^2}{2}$
$m \equiv 2\iota \pmod 4$ $fh \equiv \pm 1 \pmod{2(1+\iota)}$ $f\bar{h} \equiv 1 \pmod{2(1+\iota)}$	$1, \ \alpha, \ \frac{gh+\alpha^2}{(1+\iota)gh}, \ \frac{\alpha+\alpha^3/gh^2}{2}$
$m \equiv 2\iota \pmod 4$ $fh \equiv \pm 1 \pmod{2(1+\iota)}$ $f\bar{h} \equiv -1 \pmod{2(1+\iota)}$	$1, \ \alpha, \ \frac{gh+\alpha^2}{(1+\iota)gh}, \ \frac{\iota\alpha+\alpha^3/gh^2}{2}$
$m \equiv 3+2\iota \pmod 4$	$1, \ \alpha, \ \frac{\lvert gh\rvert^2+\alpha^2}{(1+\iota)gh}, \ \frac{\lvert gh^2\rvert^2(1+\alpha+\alpha^2)+\alpha^3}{2gh^2}$
$m \equiv 1+2\iota \pmod 4$	$1, \ \alpha, \ \frac{\lvert gh\rvert^2(1+(1+\iota)\alpha)+\alpha^2}{2gh}, \ \frac{\lvert gh^2\rvert^2(\alpha+(1+\iota)\alpha^2)+\alpha^3}{2gh^2}$
$m \equiv 3 \pmod 4$	$1, \ \alpha, \ \frac{\iota\lvert gh\rvert^2+\alpha^2}{2gh}, \ \frac{\lvert gh^2\rvert^2(\iota+\iota\alpha+\alpha^2)+\alpha^3}{2gh^2}$

$m \equiv 5 \pmod 8$ *or* $m \equiv 5 + 4\iota \pmod 8$	$1, \quad \frac{1+\alpha}{1+\iota}, \quad \frac{\lvert gh\rvert^2+\alpha^2}{2gh}, \quad \frac{\lvert gh^2\rvert^2(1+\alpha+\alpha^2)+\alpha^3}{2(1+\iota)gh^2}$
f *is even or* h *is even* *or* $m \equiv \iota \pmod 2$	$1, \quad \alpha, \quad \alpha^2/gh, \quad \alpha^3/gh^2$
$fh \equiv \iota \pmod 2$ *and* g *is even*	$1, \quad \alpha, \quad \alpha^2/gh \quad \frac{\iota\alpha+\alpha^3/gh^2}{1+\iota}$

Proof. Consider the extension F/K. Let $\delta_1, \delta_2, \delta_3$ denote the even parts of d_1, d_2, d_3 and g_1, h_1 the odd parts of g and h. Since

$$\mathrm{disc}(\alpha) = (1+\iota)^{16} f^3 g^6 h^9 \tag{8}$$

from the relation

$$(d_1 d_2 d_3)^2 \mathrm{disc}(F/K) = \mathrm{disc}(\alpha) \tag{9}$$

it follows that $g_1 \not| d_1$, $h_1 \not| d_1$ since $d_1^{12} \mid \mathrm{disc}(\alpha)$. From the fact that $\frac{\alpha^2}{gh}, \frac{\alpha^3}{gh^2} \in \mathcal{O}_F$, it follows that $g_1 h_1 \mid d_2$, $g_1 h_1^2 \mid d_3$. From (9), it follows that $g_1 h_1 \parallel d_2$, $g_1 h_1^2 \parallel d_3$.

It remains to determine $\delta_1, \delta_2, \delta_3$. Before that we list some trivial facts that will be needed:

10. If F/K is unramified, f, g and h are odd. (If f or h is even, $1+\iota$ ramifies in L/K. If g is even, since $gh\sqrt{fh}$ is a uniformiser at all primes in L dividing $1+\iota$, the congruence $x^2 \equiv gh\sqrt{fh} \pmod{P_L^{2i}}$ has no solution for any prime P_L in L dividing $1+\iota$. Thus, from 7, $d = 1$ and $4 \mid \mathrm{disc}(F/K)$).

11. If m is odd and $d_3 = 4$, F/K is unramified at 2. ($Tr_{F/K}(\alpha^3\alpha_4) = m$ is odd. So L/K is tamely ramified.)

12. $d_1 | 1+\iota$ and $d_1 = 1+\iota$ if and only if $m \equiv 1 \pmod{4\mathcal{O}_K}$. ($d_1^{12} | \mathrm{disc}(\alpha)$. So, it follows from (8) that $d_1 | 1+\iota$. $\frac{a+\alpha}{1+\iota}$ is an integer if and only if $a^4 \equiv m \pmod{4\mathcal{O}_K}$(Consider $N_{F/K}(\alpha_2)$). The only odd fourth power $\pmod{4\mathcal{O}_K}$ is 1.)

13. $d_3 | 4$ when m is odd.

Case 1 F/K is unramified. In this case, from 10, m is odd. Since L/K is unramified, $fh \equiv \pm 1 \pmod 4$. So $m \equiv \pm 1 \pmod 4$. Further $\frac{gh+\alpha^2}{2gh}$(resp. $\frac{\iota gh+\alpha^2}{2gh}$) is an integer when $fh \equiv 1 \pmod 4$(resp. $-1 \pmod 4$)). So $2|d_2$. Let P_F be any prime ideal in F dividing $1+\iota$,

$$\begin{aligned} F/K \text{ unramified} &\Leftrightarrow \sigma^2 \notin G_0(F/K) \\ &\Leftrightarrow \sigma^2(\alpha_3)-\alpha_3 \notin P_F \quad \text{or} \quad \sigma^2(\alpha_4)-\alpha_4 \notin P_F \\ &\Leftrightarrow \frac{2c}{\delta_2} \notin P_F \quad \text{or} \quad \frac{e+\alpha^2}{\delta_3} \notin P_F \end{aligned}$$

First we check that, if $\frac{2(e+\alpha^2)}{\delta_3} \notin P_F$, $\frac{2c}{\delta_2} \notin P_F$. Suppose not. Since $\delta_1|(1+\iota)$ and $\delta_3|4$, if $\delta_2 = 2$ then $(\delta_1\delta_2\delta_3)^2|(1+\iota)^{14}$. So, from (8), $(1+\iota)^2|\mathrm{disc}(F/K)$ and F/K ramifies at $1+\iota$. So $2(1+\iota)|\delta_2$. If $\frac{2c}{\delta_2} \in P_F$, $v_{1+\iota}(2c) \geq v_{1+\iota}(\delta_2)+1 \geq 4$. So $c \equiv 0 \pmod 2$. Considering

$$Tr_{L/K}(\alpha^2 N_{F/L}(\alpha_3)) = \frac{4m(2b-c^2)}{\delta_3^2}$$

we get $b \equiv 0 \pmod{1+\iota}$. It follows that $\alpha^2 \equiv 0 \pmod{1+\iota}$, which is a contradiction. So F/K is unramified at $1+\iota$ if and only if $\frac{2c}{\delta_2} \notin P_F$.

Suppose $\frac{2c}{\delta_2} \notin P_F$. Since $2(1+\iota)|\delta_2$, $c \equiv 0 \pmod{1+\iota}$. As before, $c \not\equiv 0 \pmod 2$. So $\delta_2 = 2(1+\iota)$. Hence $2b-c^2 \equiv 0 \pmod 4$, which implies that $c^2 \equiv 2\iota \pmod 4$. So b and c can be replaced by $\pm\iota$ and $1 \pm \iota$ respectively. If $\delta_1 = 1$ or $\delta_3 = 2(1+\iota)$, F/K ramifies at $1+\iota$. So $\delta_1 = 1+\iota$(which implies that $m \equiv 1 \pmod 4$) and $\delta_3 = 4$. Consider

$$N_{F/L}(\alpha_3) = \frac{b^2+m+\alpha^2(2b-c^2)}{8}$$

Since $b = \pm\iota$ and $c = 1 \pm \iota$, $2b-c^2 \equiv 0$ or $4\iota \pmod 8$ and $b^2+m = m-1$. When $2b-c^2 \equiv 0 \pmod 8$, $\frac{m-1}{8} \in \mathcal{O}_K$ or $m \equiv 1 \pmod 8$. When $2b-c^2 \equiv 4\iota \pmod 8$, $\frac{m-1+4\iota\alpha^2}{8}$ is an integer only when $m \equiv 1+4\iota \pmod 8$. So if F/K is unramified, $m \equiv 1$ or $1+4\iota \pmod 8$. Conversely, if $m \equiv 1$ or $1+4\iota \pmod 8$, $\delta_1 = 1+\iota$. If $m \equiv 1 \pmod 8$, $\frac{\iota+(1+\iota)\alpha+\alpha^2}{2(1+\iota)} \in \mathcal{O}_F$. So $2(1+\iota)|\delta_2$. Thus, $4|\delta_1\delta_2|\delta_3$ and $\delta_3 = 4$. It follows that $\delta_2 = 2(1+\iota)$. If $m \equiv 1+4\iota \pmod 8$ the same argument goes through with $\frac{-\iota+(1+\iota)\alpha+\alpha^2}{2(1+\iota)}$. Thus F/K is unramified in this case.

Case 2 F/L is ramified and L/K is unramified. Note that $fh \equiv \pm 1 \pmod 4$ since L/K is unramified.

Case 2(a) f, g, h are odd.

Since m is odd and $m \equiv \pm 1 \pmod 4$, $m \equiv 5$ or $5+4\iota \pmod 8$ or $m \equiv 3 \pmod 4$. When $m \equiv 5$ or $5+4\iota \pmod 8$, $\delta_1 = 1+\iota$ and so $2|\delta_2$ and $2(1+\iota)|\delta_3$. Since F/L is ramified at $1+\iota$, from 12, it follows that $4 \nmid \delta_3$ and $\delta_3 = 2(1+\iota)$. As $\delta_1\delta_2|\delta_3$, $2(1+\iota) \nmid \delta_2$. Thus, $\delta_2 = 2$.

Let $m \equiv 3 \pmod 4$. Then $\delta_1 = 1$. We have $N_{F/K}(\alpha - 1) = m - 1 \equiv 2 \pmod 4$. Since primes above $1+\iota$ are *unramified* in L/K, $\alpha - 1$ is a uniformiser at all primes P_F in F dividing $1+\iota$. We have $\sigma^2(\alpha-1) - (\alpha-1) = -2\alpha \in P_F^4$ when $1+\iota$ is inert in L and P_F is the unique prime in F dividing $1+\iota$. So $\sigma^2 \in G_3(F/L)$ and $\sigma^2 \notin G_4(F/L)$. Using the formula for the different(cf. [18])

$$v_p(\mathcal{D}) = \sum_{i=0}^{\infty}(|G_i| - 1)$$

we get $(1+\iota)^4 \parallel \mathrm{disc}(F/L)$. If $1+\iota$ splits in L and P_F is one of the two primes in F dividing $1+\iota$, $P_F^4 \parallel 2\alpha$. From this, it follows that for any prime P_L in L dividing $1+\iota$, we have $P_L^4 \parallel \mathrm{disc}(F/L)$. So $(1+\iota)^4|\mathrm{disc}(F/L)$ and $(1+\iota)^8|\mathrm{disc}(F/K)$. Therefore, from (9), it follows that $\delta_2\delta_3 = 4$. Since

$$\frac{\iota|gh|^2 + \alpha^2}{2gh}, \frac{|gh^2|^2\iota\alpha + \alpha^3}{2gh^2} \in \mathcal{O}_F,$$

$\delta_2 = \delta_3 = 2$.

Case 2(b) Suppose g is even and $fh \equiv \pm 1 \pmod 4$. Then

$$v_{P_L}(N_{F/L}(\alpha)) = v_{P_L}(gh\sqrt{fh}) = 1$$

where P_L is a prime in L dividing $1+\iota$. So α is uniformiser at all primes in F dividing $1+\iota$. We have $\sigma^2(\alpha) - \alpha = 2\alpha$. As in the previous case we can check that $(1+\iota)^{10} \parallel \mathrm{disc}(F/K)$ and $\delta_2\delta_3 = (1+\iota)^6$. Since

$$\frac{gh + \alpha^2}{2gh}, \frac{igh^2 + \alpha^3}{2gh^2} \in \mathcal{O}_F$$

$\delta_2 = \delta_3 = 2(1+\iota)$.

Case 3 F/K is totally ramified at $1+\iota$. Note that F/K is totally ramified at $1+\iota$ if and only if $1+\iota$ ramifies in L/K. If L/K alone is ramified, $G_0(F/K)$ is of order 2 and there is a sub-extension of F/K which is unramified at $1+\iota$ and is of degree 2 over K. Since $G(F/K)$ is cyclic, L is the unique sub-extension of F/K which is of degree 2 over K.

We will use the results from [28]. Let b_i and b^i denote the i^{th} lower and upper break numbers of the extension L/K.

Case 3(a) $m \equiv \iota \pmod 2$.

In this case, $4 \parallel \mathrm{disc}(L/K)$. From the formula for the different, it follows that the break number for the extension for L/K is 3. So it follows that $b^1 = b_1 = 3$ for the extension for F/K. Using Theorem 3 of Wyman [28], it follows that $b^2 = 5$ and therefore $b_2 = 7$ for the extension F/K. Using the formula for the different, we get that $(1+\iota)^{16} \parallel \mathrm{disc}(F/K)$. From (8), it follows that $\delta_1\delta_2\delta_3 = 1$.

Case 3(b) $fh \equiv \iota \pmod 2$, g *is even* .

As before, $(1+\iota)^{16} \parallel \mathrm{disc}(F/K)$. So we get, from (8), $\delta_2\delta_3 = (1+\iota)^3$. Since $\alpha^2/gh \in \mathcal{O}_F$ and $\delta_2|\delta_3$, the only possibility is $\delta_2 = 1+\iota$ and $\delta_3 = 2$.

Case 3(c) f or h is divisible by $1+\iota$.

In either case $(1+\iota)^5 \parallel \mathrm{disc}(L/K)$. As in the previous case, we conclude that $b^1 = b_1 = 4$, $b^2 = 6$ and $b_2 = 8$. So using the formula for the different, we get $(1+\iota)^{19} \parallel \mathrm{disc}(F/K)$.

When f is even, $\delta_2\delta_3 = 1$. When h is even, $\delta_2\delta_3 = (1+\iota)^3$. As $\alpha^2/gh \in \mathcal{O}_F$, $\delta_2 = 1+\iota$ and $\delta_3 = 2$.

Since $2 \parallel \mathrm{disc}(L/K)$ when $fh \equiv \pm 1 + 2\iota \pmod 4$, the break number is 1 for L/K and so $b_1 = 1$ for F/K. So the break numbers are odd.

Case 3(d) $m \equiv 1 + 2\iota \pmod 4$.

Since the break numbers are odd, $b_2 \geq 3$. $(1+\iota)^8 | \mathrm{disc}(F/L)$. Thus, $\delta_2\delta_3 | (1+\iota)^4$.

When $m \equiv 1 + 2\iota$, $\dfrac{1 + (1+\iota)\alpha + \alpha^2}{2} \in \mathcal{O}_F$. Therefore $\delta_2 = 2$, $\delta_3 = 2$.

When $m \equiv 3 + 2\iota \pmod 4$,

$$N_{F/K}(\alpha - 1) = m - 1 \equiv 2(1+\iota) \pmod 4$$

So $\dfrac{(\alpha-1)^3}{2}$ is a uniformiser for the unique prime in F dividing $1+\iota$. We have

$$\sigma^2\left(\frac{(\alpha-1)^3}{2}\right) - (\alpha-1)^3 = \alpha(\alpha^2+3)$$

and $N_{F/K}(\alpha^2+3) = (m-9)^2$. Since $m - 9 \equiv 2(1+\iota) \pmod 4$, $(1+\iota)^6 \parallel N_{F/K}\alpha(\alpha^2+3)$ and so $\sigma^2 \in G_5(F/K)$ and $\sigma^2 \notin G_6(F/K)$. So, in this case, $b_2 = 5$ for F/K. Thus,

$(1+\iota)^{10}|\mathrm{disc}(F/K)$. Therefore, $\delta_2\delta_3 \parallel (1+\iota)^6$. So $\delta_2\delta_3|(1+\iota)^3$. Since $\frac{|gh|^2+\alpha^2}{1+\iota}$ is an integer, $\delta_2 = (1+\iota)$, $\delta_3 = 2$.

Case3(e) Let $fh \equiv \pm 1 + 2\iota \pmod 4$, g be even.

Since $fh \equiv \pm 1 \pmod{2(1+i)}$, $f \equiv \pm h \pmod{2(1+\iota)}$. When $f \equiv h \pmod{2(1+\iota)}$, consider the element $\mathcal{X} = 1 + \frac{\alpha + \alpha^3/gh^2}{2}$. We have

$$N_{F/K}(\mathcal{X}) = \frac{16 - (g(f-h))^2 - 16fgh}{16}$$

Since $g \equiv (1+\iota) \pmod 2$, $g = a + \iota b$ with a and b odd. So $g^2 \equiv \pm 2\iota \pmod 8$. One checks easily that $(g(f-h))^2 \equiv 16 \pmod{32}$ and $16fgh \equiv 16(1+\iota) \pmod{32}$. So $\mathcal{X}$ is a uniformiser. We have

$$\sigma^2(\mathcal{X}) - \mathcal{X} = \alpha + \alpha^3/gh^2$$

and

$$(1+\iota)^8 \parallel N_{F/K}(\alpha + \alpha^3/gh^2) = g^2fh(f-h)^2.$$

So $G_7 \neq \{1\}$. Since b_1 is odd, so is b_2. So $b_2 \neq 8$. Since $G_9(F/K) = 1$, $b_2 = 7$. ($G_i(N/K) = \{1\}$ if $i > e/(p-1)$ for any extension of local fields N/K, where p is the characteristic of the residue field and e is the valuation of p in L. Cf. [18], Exercise (2)c at the end of §2 in Chapter 4.) So $(1+\iota)^{12}|\mathrm{disc}(F/K)$ and therefore $\delta_2\delta_3 = 5$. Since $\frac{gh+\alpha^2}{gh}$ and $\frac{\alpha+\alpha^3/gh^2}{2}$ are in $\mathcal{O}_F$, $\delta_2 = 2$, $\delta_3 = 2(1+\iota)$.

Similarly, when $f \equiv -h \pmod{2(1+\iota)}$, $1 + \frac{\iota\alpha + \alpha^3/gh^2}{2}$ is a uniformiser. As before, it can be checked that $(1+\iota)^{12}|\mathrm{disc}(F/K)$. Since $\frac{gh+\alpha^2}{(1+\iota)gh}$ and $\frac{\iota\alpha+\alpha^3/gh^2}{2}$ are in $\mathcal{O}_F$, $\delta_2 = 2$, $\delta_3 = 2(1+\iota)$. ∎

3 Galois Module Structure in the tame case

Theorem 18: *Let F/K be a tamely ramified extension. Then,*

1. *When $m \equiv 1 \pmod 8$, $\mathcal{O}_F$ has a normal integral basis over L if and only if $h \equiv u \pmod 4$ for some unit u in $\mathcal{O}_K$.*

2. *When* $m \equiv 1 + 4\iota \pmod 8$, *normal integral basis exists for* $\mathcal{O}_F$ *if and only if* h *is not congruent* $\pmod 4$ *to any unit in* $\mathcal{O}_K$.

Before we prove this result we recall some facts about locally free modules over the group ring. Throughout, P in the subscript denotes the completion at P.

Let M be a locally free module over $\mathcal{O}_K G$. Suppose $MK = KG.v$ for some $v \in M$. Then, at each prime P, $M_P = \mathcal{O}_{K_P}\alpha_P.v$ for some α_P in $K_P G$. We have $(\alpha_P) \in \mathbf{J}(KG)$ and the map $(M) \xrightarrow{\phi} [(\alpha_P)]$ gives an isomorphism

$$\mathcal{C}\ell(\mathcal{O}_K G) \longrightarrow \frac{\mathbf{J}(KG)}{(KG)^* U(\mathcal{O}_K G)}$$

Here, $[(\alpha_P)]$ denotes the coset $(\alpha_P)(KG)^* U(\mathcal{O}_K G)$, $\mathbf{J}(KG)$ denotes the ideĺe group of KG, $U(\mathcal{O}_K G)$ denotes the subgroup of unit ideĺes and $(KG)^*$ denotes the unit group of KG. cf. [9] for details.

Remarks

1. Let R be a Dedekind Domain and let K be its quotient field. Suppose G is an abelian group, $|G| = n$ and that K contains n^{th} roots of unity. Let $\{e_\chi\}$ denote the set of idempotents corresponding to the characters of G. Then $\mathcal{M} = \oplus_\chi R e_\chi$ is the maximal $R-$order in KG. Let $\alpha \in RG$. Then, $\alpha \in RG^*$ if and only if $\alpha \in \mathcal{M}^*$. This is because $RG \hookrightarrow \mathcal{M}$ is an integral extension. Further, $\gamma = \sum x_\chi e_\chi \in \mathcal{M}$ is a unit if and only if $x_\chi \in R^*$ for all χ.

2. To show that $\mathcal{O}_F$ is free over $\mathcal{O}_K G$, it is enough to produce an integer of the form

$$\frac{u_0 + u_1\alpha + u_2\alpha^2/gh + \alpha^3/gh^2}{4}$$

for some units u_0, u_1, u_2. This is because it can be easily checked that the square of the product over the resolvents of this element is equal to the discriminant of the extension.(In our context the resolvent of an element $\gamma \in F$ with respect to χ_i is $4e_i(\gamma)$.)

3. During the course of the proof, whenever we say something like $\overline{g}$ is a unit $\pmod 4$, we mean that $\overline{g}$ is congruent is to a unit in $\mathcal{O}_K$ modulo $4\mathcal{O}_K$.

Proof. Let $m \equiv 1 \pmod 8$. The integral base in this case can be re-written as

$$\left\{1, \frac{1+\alpha}{(1+\iota)}, \frac{\overline{gh}(\iota+(1+\iota)\alpha)+\alpha^2/gh}{2(1+\iota)}, \frac{\overline{gh^2}(1+\alpha+gh\alpha^2/gh)+\alpha^3/gh^2}{4}\right\}$$

Since $h^2 \equiv \pm 1 \pmod 4$ and $|gh|^2 \equiv 1 \pmod 4$. So

$$\frac{\epsilon\overline{g}+\epsilon\overline{g}\alpha+\overline{h}\alpha^2/gh+\alpha^3/gh^2}{4}$$

is an integer, $\epsilon = \pm 1$. If g is a unit $\pmod 4$,

$$\frac{u+u\alpha+\overline{h}\alpha^2/gh+\alpha^3/gh^2}{4}$$

is an integer for some unit $u \in \mathcal{O}_K^*$. If $\overline{g}$ is not a unit $\pmod 4$, adding $\frac{1+\alpha}{1+\iota}$ to $\frac{\epsilon\overline{g}+\epsilon\overline{g}\alpha+\overline{h}\alpha^2/gh+\alpha^3/gh^2}{4}$, we get that

$$\frac{u_1+u_1\alpha+\overline{h}\alpha^2/gh+\alpha^3/gh^2}{4}$$

is an integer for some unit $u_1 \in \mathcal{O}_K$. This is because (a non-unit) $\pmod 4 + 2(1+\iota)$ is a (unit) $\pmod 4$. So we can always assume that

$$\frac{u+u\alpha+\overline{h}\alpha^2/gh+\alpha^3/gh^2}{4}$$

is an integer for some unit $u \in \mathcal{O}_K^*$.

If $\overline{h}$ is a unit $\pmod 4$, say $\overline{h} \equiv u_1 \pmod 4$, we can replace $\overline{h}$ by u_1 and the resulting element generates $\mathcal{O}_F$ over $\mathcal{O}_K G$. One checks this by computing the resultant of this element.

We show that, if $\mathcal{O}_F$ is free over $\mathcal{O}_K G$, $\overline{h}$ is congruent to a unit $\pmod 4$.

Choose

$$v = \frac{u+u\alpha+\overline{h}\alpha^2/gh+\alpha^3/gh^2}{4}$$

Then,

$$\alpha_P = \begin{cases} e_1+e_2+e_3+e_4 & \text{if } P \not| h \\ e_1+\overline{h}^{-1}e_2+e_3+e_4 & \text{if } P|h \end{cases}$$

Let $\lambda = e_1+\overline{h}e_2+e_3+e_4 \in KG^*$. Then, it is necessary that $(\lambda\alpha_P)$ is in $U(\mathcal{O}_K G)KG^*$, for $(\mathcal{O}_F) = 0$ in the class group. Here

$$(\tilde{\alpha}_P) = (\lambda\alpha_P) = \begin{cases} e_1+\overline{h}e_2+e_3+e_4 & \text{if } P \not| h \\ e_1+e_2+e_3+e_4 & \text{if } P|h \end{cases}$$

If $(\tilde{\alpha}_P) \in U(\mathcal{O}_K G)KG^*$, there is an element $\mathrm{x} = x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4$ such that $(\mathrm{x}\tilde{\alpha}_P) \in U(\mathcal{O}_K G)$. We have that,

$$\mathrm{x}\tilde{\alpha}_P = \begin{cases} x_1e_1 + x_2\overline{h}e_2 + x_3e_3 + x_4e_4 & \text{if } P \not| h \\ x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4 & \text{if } P|h \end{cases}$$

is an element of $U(\mathcal{O}_K G)$. So it follows that $x_1, x_2, x_3, x_4 \in \mathcal{O}^*_{K_P}$(from the first Remark in this section) when $P|h$ and $x_1, \overline{h}x_2, x_3, x_4 \in \mathcal{O}^*_{K_P}$ for $P \not| h$. It follows that x_i are units. If $P|h$, $(P,4) = 1$ and therefore $x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4 \in (\mathcal{O}_{K_P}G)^*$. When $P \not| h$, a necessary condition for $x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4$ to be in $\mathcal{O}_K G$ is

$$\begin{aligned} x_1\frac{(1 + \iota\sigma^3 - \sigma^2 - \iota\sigma)}{4} &+ \overline{h}x_2\frac{(1 - \sigma^3 + \sigma^2 - \sigma)}{4} \\ +x_3\frac{(1 - \iota\sigma^3 - \sigma^2 + \iota\sigma)}{4} &+ x_4\frac{(1 + \sigma^3 + \sigma^2 + \sigma)}{4} \end{aligned}$$

is in $\mathcal{O}_K G$. Regrouping the terms, we get the following congruence conditions:

$$x_1 + \overline{h}x_2 + x_3 + x_4 \equiv 0 \pmod 4 \tag{14}$$

$$\iota x_1 - \overline{h}x_2 - \iota x_3 + x_4 \equiv 0 \pmod 4 \tag{15}$$

$$-x_1 + \overline{h}x_2 - x_3 + x_4 \equiv 0 \pmod 4 \tag{16}$$

$$-\iota x_1 - \overline{h}x_2 + \iota x_3 + x_4 \equiv 0 \pmod 4 \tag{17}$$

Subtracting (16) from (14), we get $2(x_1 + x_3) \equiv 0 \pmod 4$ or $x_1 \equiv x_3 \pmod 2$. Since $x_1, x_2, x_3, x_4 \in \{\pm 1, \pm\iota\}$, this implies that $x_1 = \pm x_3$. If $x_1 = x_3$, using this in (15), we get $\overline{h} \equiv u \pmod 4$. If $x_1 = -x_3$, we use this in (16) to get the result.

Let $m \equiv 1 + 4\iota \pmod 8$. In this case, the integral base is

$$\left\{1, \tfrac{1+\alpha}{1+\iota}, \frac{\overline{gh}(-\iota + (1+\iota)\alpha) + \alpha^2/gh}{2(1+\iota)}, \frac{\overline{gh^2}(2 - \iota + \alpha + gh\alpha^2/gh) + \alpha^3/gh^2}{4}\right\}$$

As in the previous case,

$$\frac{(2-\iota)\overline{g}\epsilon + \overline{g}\epsilon\alpha + \overline{h}\alpha^2/gh + \alpha^3/gh^2}{4}$$

is an integer.

We will show that $\mathcal{O}_F$ is free over $\mathcal{O}_K G$ when $\overline{g}$ is a unit and $\overline{h}$ is a non-unit or when $\overline{g}$ and $\overline{h}$ are both non-units. If $\overline{g}$ is a unit and $\overline{h}$ is not a unit

$$\frac{u(2-\iota) + u_1\alpha + \overline{h}\alpha^2/gh + \alpha^3/gh^2}{4}$$

is an integer for some units u, u_1. Since $\overline{h}$ is a non-unit, adding $\dfrac{1+\alpha^2/gh}{1+\iota}$ to this element, we get an element of the form

$$\frac{u_0 + u_1\alpha + u_2\alpha^2/gh + \alpha^3/gh^2}{4} \in \mathcal{O}_F$$

and this generates $\mathcal{O}_F$ over $\mathcal{O}_K G$.

Suppose $\overline{g}$ and $\overline{h}$ are non-units. Then $\overline{g} \equiv u_0(2+\iota)$ for some unit u_0. So

$$\frac{u_0\epsilon + \overline{g}\epsilon\alpha + \overline{h}\alpha^2/gh + \alpha^3/gh^2}{4} \in \mathcal{O}_F$$

Adding $\dfrac{\alpha+\alpha^2/gh}{1+\iota}$, we get an element of the form

$$\frac{u + u_1\alpha + u_2\alpha^2/gh + \alpha^3/gh^2}{4} \in \mathcal{O}_F,$$

and this generates $\mathcal{O}_F$ over $\mathcal{O}_K G$.

Next we show that, if h is congruent (mod 4) to any unit in $\mathcal{O}_K$ then $\mathcal{O}_F$ is not free over $\mathcal{O}_K G$.

Suppose g is unit mod 4 to some unit in O_K. Then, there is an integer of the form

$$\frac{u_0(2-\iota) + u_1\alpha + u_2\alpha^2/gh + \alpha^3/gh^2}{4}$$

Choose this for v. Then

$$\alpha_P = \begin{cases} e_1 + e_2 + e_3 + e_4 & \text{if } P \not| 2-\iota \\ e_1 + e_2 + e_3 + (2-\iota)^{-1}e_4 & \text{if } P|2-\iota \end{cases}$$

As before, we can modify this to

$$(\tilde{\alpha}_P) = (\lambda\alpha_P) = \begin{cases} e_1 + e_2 + e_3 + (2-\iota)e_4 & \text{if } P \not| (2-\iota) \\ e_1 + e_2 + e_3 + e_4 & \text{if } P|(2-\iota) \end{cases}$$

$$\mathrm{x}\tilde{\alpha}_P = \begin{cases} x_1e_1 + x_2e_2 + x_3e_3 + x_4(2-\iota)e_4 & \text{if } P \not| 2-\iota \\ x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4 & \text{if } P|2-\iota \end{cases}$$

As before, we get $x_1, x_2, x_3, x_4 \in \mathcal{O}_K^*$ and the following congruence conditions if we assume that $(\mathrm{x}\tilde{\alpha}_P) \in U(\mathcal{O}_K G)$. (Again, $(P,2) = 1$ if $P|2-\iota$.)

$$x_1 + x_2 + x_3 + (2-\iota)x_4 \equiv 0 \pmod 4 \tag{18}$$

$$\iota x_1 - x_2 - \iota x_3 + (2-\iota)x_4 \equiv 0 \pmod 4 \tag{19}$$

$$-x_1 + x_2 - x_3 + (2-\iota)x_4 \equiv 0 \pmod 4 \tag{20}$$

$$-\iota x_1 - x_2 + \iota x_3 + (2-\iota)x_4 \equiv 0 \pmod 4 \tag{21}$$

Subtracting (20) from (18), we get $2(x_1+x_3)\equiv 0 \pmod 4$ or $x_1=\pm x_3$. If $x_1=x_3$, using this in (19), we get $2-\iota\equiv u \pmod 4$ for some unit u, which is a contradiction. If $x_1=-x_3$, using this fact in the (18) one gets a contradiction.

If g is a nonunit mod 4 then, there is an integer of the form

$$\frac{u_0+\epsilon\overline{g}\alpha+u_1\alpha^2/gh+\alpha^3/gh^2}{4}$$

Choose this for v. Then

$$\alpha_P=\begin{cases} e_1+e_2+e_3+e_4 & \text{if } P\not|\overline{g} \\ \overline{g}^{-1}e_1+e_2+e_3+e_4 & \text{if } P|\overline{g}\end{cases}$$

Again, we could work with $(\tilde{\alpha}_P)$ instead, where

$$(\tilde{\alpha}_P)=\begin{cases} \overline{g}e_1+e_2+e_3+e_4 & \text{if } P\not|\overline{g} \\ e_1+e_2+e_3+e_4 & \text{if } P|\overline{g}\end{cases}$$

The congruence conditions in this case are

$$\overline{g}x_1+x_2+x_3+x_4 \equiv 0 \pmod 4 \tag{22}$$

$$\iota\overline{g}x_1-x_2-\iota x_3+x_4 \equiv 0 \pmod 4 \tag{23}$$

$$-\overline{g}x_1+x_2-x_3+x_4 \equiv 0 \pmod 4 \tag{24}$$

$$-\iota\overline{g}x_1-x_2+\iota x_3+x_4 \equiv 0 \pmod 4 \tag{25}$$

Adding (22) to (24) we get $x_2=\pm x_4$. If $x_2=x_4$, using this in (25), we get $\overline{g}\equiv u \pmod 4$. If $x_2=-x_4$, we use this in (22) to get the same result. ∎

4 Galois Module Structure in the non-tame case

Let e_1, e_2, e_3 and e_4 as before. Let 1_G denote the identity element of G.

Theorem 19: *Let F over K be a non-tame extension. Then the associated order of F over K and a generator γ of $\mathcal{O}_F$ as an $\mathcal{A}_{F/K}$-module is given as follows.*

Conditions	*Associated Order $\mathcal{A}_{F/K}$*	*Generator γ*
$m\equiv 2\iota \pmod 4$ $fh\equiv 1 \pmod 4$	$2\mathcal{O}_K e_4+2\mathcal{O}_K e_1$ $+\mathcal{O}_K(e_4+e_2)+\mathcal{O}_K 1_G$	$\frac{1+\alpha+\alpha^2/gh+\alpha^3/gh^2}{2}$

$m \equiv 2\iota \pmod 4$ $fh \equiv -1 \pmod 4$	$2\mathcal{O}_K e_4 + 2\mathcal{O}_K e_1$ $+\mathcal{O}_K(e_4+e_2) + \mathcal{O}_K 1_G$	$\frac{\iota+\iota\alpha+\alpha^2/gh+\alpha^3/gh^2}{2}$
$m \equiv 2\iota \pmod 4$ $fh \equiv \pm 1 \pmod{2(1+\iota)}$ $f\bar{h} \equiv 1 \pmod{2(1+\iota)}$	$(1-\iota)\mathcal{O}_K e_4 + 2\mathcal{O}_K e_1$ $+\mathcal{O}_K(e_4+e_2) + \mathcal{O}_K 1_G$	$\frac{1-\iota+\alpha+(1-\iota)\alpha^2/gh+\alpha^3/gh^2}{2}$
$m \equiv 2\iota \pmod 4$ $fh \equiv \pm 1 \pmod{2(1+\iota)}$ $f\bar{h} \equiv -1 \pmod{2(1+\iota)}$	$(1-\iota)\mathcal{O}_K e_4 + 2\mathcal{O}_K e_1$ $+\mathcal{O}_K(e_4+e_2) + \mathcal{O}_K 1_G$	$\frac{1-\iota+\iota\alpha+(1-\iota)\alpha^2/gh+\alpha^3/gh^2}{2}$
$m \equiv 3+2\iota \pmod 4$	$2\mathcal{O}_K e_4 + 2\mathcal{O}_K e_1$ $+(1+\iota)(e_4+e_2) + \mathcal{O}_K 1_G$	$\frac{1+\alpha+\alpha^2/gh+\alpha^3/gh^2}{2}$
$m \equiv 1+2\iota \pmod 4$	$2\mathcal{O}_K e_4 + 2\mathcal{O}_K e_1$ $+(1+\iota)\mathcal{O}_K(e_4+e_2) + \mathcal{O}_K 1_G$	$\frac{\lvert gh^2\rvert^2(1+\iota\alpha+\iota\alpha^2)+\alpha^3}{2gh^2}$
$m \equiv 3 \pmod 4$	$2\mathcal{O}_K e_4 + 2\mathcal{O}_K e_1$ $\mathcal{O}_K(e_4+e_2) + \mathcal{O}_K 1_G$	$\frac{\lvert gh^2\rvert^2(\iota+\iota\alpha+\alpha^2)+\alpha^3}{2gh^2}$
$m \equiv 5 \pmod 8$ or $m \equiv 5+4\iota \pmod 8$	$2(1+\iota)\mathcal{O}_K e_4 + 2\mathcal{O}_K(e_4+e_1)$ $+(1+\iota)\mathcal{O}_K(e_4+e_2) + \mathcal{O}_K 1_G$	$\frac{1+\alpha+\alpha^2/gh+\alpha^3/gh^2}{2(1+\iota)}$
$m \equiv \iota \pmod 2$ or $m \equiv 2+2\iota \pmod 4$ or f *even*	*Maximal order*	$1+\alpha+\frac{\alpha^2}{gh}+\frac{\alpha^3}{gh^2}$
$fh \equiv \iota \pmod 2$ g *even*	$\mathcal{O}_K e_4 + (1+\iota)\mathcal{O}_K e_1$ $+\mathcal{O}_K e_2 + \mathcal{O}_K 1_G$	$\frac{1+\iota+\iota\alpha+(1+\iota)\alpha^2/gh+\alpha^3/gh^2}{1+\iota}$

Proof. We will give the proof for a typical non-tame case. Proofs in the other cases are analogous.

Case : $m \equiv 5 \pmod 8$ or $m \equiv 5+4\iota \pmod 8$

Let $v_1 = e_4$, $v_2 = e_4 + e_1$, $v_3 = e_4 + e_2$, and $v_4 = e_1 + e_2 + e_3 + e_4$. Note that the v_i's span the maximal order $\mathcal{M}$ in $K[G]$ over $\mathcal{O}_K$:

$$\mathcal{M} = \oplus_{n=1}^{n=4} \mathcal{O}_K v_n$$

In this case, $\alpha_1 = 1$, $\alpha_2 = \frac{1+\alpha}{1+\iota}$, $\alpha_3 = \frac{|gh|^2+\alpha^2}{2gh}$ and $\alpha_4 = \frac{|gh^2|^2(1+\alpha+\alpha^2)+\alpha^3}{2(1+\iota)gh^2}$ generates $\mathcal{O}_F$ over $\mathcal{O}_K$. Then, a necessary and sufficient condition for $\mathrm{x} \in \mathcal{M}$ to be in $\mathcal{A}_{F/K}$ is that $\mathrm{x}\alpha_i \subseteq \mathcal{O}_F$,

for $1 \leq i \leq 4$. Applying $\mathbf{x}$ on α_i, we get,

- $\mathbf{x}\alpha_2 = \frac{a}{1+\iota} + b\frac{1+\alpha}{1+\iota} + \frac{c}{1+\iota} + d\frac{1+\alpha}{1+\iota}$, so, $a \equiv c \pmod{1+\iota}$ and $b+d \in \mathcal{O}_K$
- $\mathbf{x}\alpha_3 = \frac{a|gh^2|}{2gh} + \frac{b|gh|^2}{2gh} + (c+d)\frac{|gh|^2+\alpha^2}{2gh}$, which implies $\frac{a+b}{2} \in O_K$
- $\mathbf{x}\alpha_4 = a\frac{|gh^2|^2}{2(1+\iota)gh} + b\frac{|gh^2|^2(1+\alpha)}{2(1+\iota)gh^2} + c\frac{|gh^2|^2(1+\alpha^2)}{2(1+\iota)gh^2} + d\frac{|gh^2|^2(1+\alpha+\alpha^2)+\alpha^3}{2(1+\iota)gh^2}$

One easily checks that all these conditions are together equivalent to the following conditions: $a \equiv 0 \pmod{2(1+\iota)}$, $b \equiv 0 \pmod 2$ and $c \equiv 0 \pmod{1+\iota}$. Therefore, every element of $\mathcal{A}_{F/K}$ is of the form $2(1+\iota)O_k e_1 + 2O_k e_2 + (1+\iota)O_k e_3 + O_k e_4$ and obviously any element of $\mathcal{M}$ of this form is in $\mathcal{A}_{F/K}$. Therefore,

$$\mathcal{A}_{F/K} = 2(1+\iota)O_k e_1 + 2O_k e_2 + (1+\iota)O_k e_3 + O_k e_4.$$

Now we will show that $\gamma = \dfrac{|gh^2|^2(1+\alpha+\alpha^2)+\alpha^3}{2(1+\iota)gh^2}$ generates $\mathcal{O}_F$ over $\mathcal{A}_{F/K}$. It is easily checked that $\mathcal{A}_{F/K}.\gamma = \mathcal{O}_K\alpha_1' + \mathcal{O}_K\alpha_2' + \mathcal{O}_K\alpha_3' + \mathcal{O}_K\alpha_4'$, where

$$\alpha_1' = \overline{gh^2};\quad \alpha_2' = \overline{gh^2}\alpha_2;\quad \alpha_3' = \overline{gh^2}\left(\frac{1-|gh|^2}{2} + \alpha_3\right);\quad \alpha_4' = \alpha_4.$$

The determinant of the change from the old integral basis to the new one is unit in $\mathcal{O}_K$. Therefore, in this case, $\mathcal{O}_F$ is free over $\mathcal{A}_{F/K}$ with generator $\gamma = \frac{|gh^2|^2(1+\alpha+\alpha^2)+\alpha^3}{2(1+\iota)gh^2}$ ∎

Bibliography

[1] A. M Bergé. Sur l'arithmetique d'une extension dihedral. *Ann. Inst. Fourier, Grenoble*, 22:31–59, 1972.

[2] A. M Bergé. Arithmetique d'une extension ġroupe d'inertie cyclique. *Ann. Inst. Fourier, Grenoble*, 28(4):17–44, 1978.

[3] F. Bertrandias, J. P Bertrandias, and M. J Ferton. Sur l'anneau d'entiers d'une extension cyclique de degré premier d'une corps local. *C.R.A.S Paris*, 274:1388–1391, 1972.

[4] Robert H. Bird and Charles J. Parry. Integral bases for bicyclic biquadratic fields over quadratic subfields. *Pacific Journal of Mathematics*, 66(1):29–36, 1976.

[5] D. Burns. Factorisability and wildly ramified galois extensions. *Ann. Inst. Fourier, Grenoble*, 41(2):393–430, 1991.

[6] Ph. Cassou-Nogués, T.Chinburg, A. Frohlich, and M. J Taylor. *l*-functions and galois modules. In J. Coates and M. J Taylor, editors, *L-functions and Arithmetic*, number 153 in London Mathematical Society Series. Cambridge University Press, 1991.

[7] S. P Chan and C. H Lim. Relative galois module structure of rings of integers of cyclotomic fields. *J. Reine. angew. Math.*, 434:205–220, 1993.

[8] A. Frohlich. The module structure of kummer extensions over dedekind domains. *J. Reine Angew. Math*, 209:39–53, 1962.

[9] A. Frohlich. Locally free modules over arithmetic orders. *J. reine. angwe. math.*, 274/275:112–124, 1975.

[10] K. Hardy, R.H. Hudson, D. Richman, K.S.Williams, and N.M. Holtz. *Calculations of The Class Numbers of Imaginary Cyclic Quartic Fields.* Number 7 in Carleton-Ottawa Mathematics Lecture Note Series. Carleton University, Ottawa, Canada, July 1986.

[11] John A. Hymo and Charles J. Parry. On relative integral bases for cyclic quartic fields. *Journal of Number Theory*, 34:189–197, 1990.

[12] John A. Hymo and Charles J. Parry. On relative integral bases for pure quartic fields. *Indian Journal of Pure and Applied Mathematics*, 23(5):359–376, 1992.

[13] H. W. Leopoldt. Über die hauptordnung der ganzen elements eine abelschen zahlkörper. *J. Reine. Angew. Math.*, 201:119–149, 1959.

[14] G. Lettl. Note on the galois module structure of quadratic extensions. *Colloquium Mathematicum*, LXVII(1):15–19, 1994.

[15] D. Marcus. *Number Fields.* Springer– Verlag, New York, Berlin, Heidelberg, 1977.

[16] E. Noether. Normalbasis bei korpen ohne hohere verzweigung. *J. Reine. Angew. Math*, 167:147–152, 1932.

[17] Ph. Cassou Nogués and M. J Taylor. *Elliptic functions and rings of integers.* Number 66 in Progress in Mathematics. Birkhauser, Boston, 1987.

[18] J. P Serre. *Local Fields.* Number 67 in G.T.M. Springer-Verlag, New York, Berlin, Heidelberg, 1979.

[19] R. Shertz. Galois modulstruktur und elliptische funktionen. *J. Number. Theory*, 39:327–338, 1991.

[20] Anupam Srivastav and S. Venkataraman. Relative galois module structure of quadratic extensions. *Indian Jl. Of Pure and Applied Mathematics*, May, 1994.

[21] M. J. Taylor. On frohlich conjucture for ring of integers of finite extensions. *Invent. Math.*, 63:41–79, 1981.

[22] M. J. Taylor. Formal groups and the galois module structure of local rings of integers. *J. Reine. Angew. Math.*, 358:97–103, 1985.

[23] M. J. Taylor. Relative galois module structure of rings of integers and elliptic functions ii. *Ann. Math.*, 121:415–431, 1985.

[24] M. J Taylor. Hopf orders and galois module structure. In K. W Roggemkamp and M. J Taylor, editors, *Group rings and Class groups*, number 18 in DMV. Birkhauser, 1992.

[25] Hideo Wada. On cubic galois extension of $q(\sqrt{-3})$. *Proc. Japan Acad.*, 46(5):397–400, 1970.

[26] D. T. Walker. On the diophantine equation $mx^2 + ny^2 = \pm 1$. *American Mathematical Monthly*, May:504–512, 1967.

[27] Kenneth S. Williams. Integers of biquadratic fields. *Canadian Mathematical Bulletin*, 13(4):519–526, 1970.

[28] B. Wyman. Wildly ramified gamma extensions. *Amer. J. of Math.*, 91:135–152, 1969.