The Discriminant and Conductor of Bicyclic Quartic Fields

by

Graeme Turner

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Mathematics

School of Mathematics and Statistics

Ottawa-Carleton Institute for Mathematics and Statistics

Carleton University

Ottawa, Ontario, Canada

Abstract

Let K be a bicyclic field of degree 4 over $\mathbb{Q}$ given in the form $K = \mathbb{Q}(\theta)$ where $\theta^4 + A\theta^2 + B\theta + C = 0$ for $A, B, C \in \mathbb{Z}$. The discriminant $d(K)$ and the conductor $f(K)$ are explicitly determined in terms of A, B and C.

Acknowledgements

I would like to begin by thanking my supervisor, Şaban Alaca, for his supervision, guidance and support throughout this project and for the confidence he has had in me and my abilities. I would also like to thank Kenneth S. Williams for his many insights and for motivating this project. I would also like to thank my undergraduate number theory professor, Donald Rideout, my honours supervisor, H.E.A. Campbell, and my Master's supervisor, Ross Willard, for their crucial roles in my development as a mathematician.

The pursuit of this research took an unusual turn when I was asked to apply for a term-appointed faculty position at the Grenfell Campus of Memorial University of Newfoundland at the end of my third year of Ph.D. studies at Carleton. Over the past three years, I have had the rare privilege of being both a faculty member and a Ph.D. candidate at the same time. I would like to thank my many students for their warmth and their enthusiasm, and for their many gracious and heartwarming comments which helped lift my spirits during the times of greatest stress. Teaching the students of Grenfell has been one of the greatest joys of my life to date. I would also like to thank my many excellent colleagues at Grenfell for their support and encouragement, several of whom once taught me as an undergraduate student. In particular, I would like to thank Robert Gallant and Georg Gunther for their mentorship, their collegiality and their friendship.

I would like to thank my family, especially my sister Heather and her partner Geoff, for their support in the final months of this project. Finally, I would like to thank my partner, Amber, for her enduring patience, support and encouragement throughout this process.

Contents

Introduction

Let K be a number field - that is, K is a finite extension of $\mathbb{Q}$. An **integral basis** of a number field K is a $\mathbb{Z}$-basis of $\mathcal{O}_K$, the ring of integral elements of K [5]. The **discriminant** of a number field K with $[K : \mathbb{Q}] = n$ is given by the value

$$d(K) = \det\left(\sigma_j(\theta_i)\right)$$

where, for $1 \leq j \leq n$, $\sigma_j : K \longrightarrow \mathbb{C}$ is an injective field homomorphism which fixes $\mathbb{Q}$ and $\{\theta_1, \theta_2, ..., \theta_n\}$ is an integral basis of K. First discovered by Richard Dedekind and published in the eleventh supplement to Dirichlet's *Vorlesungen über Zahlentheorie* [17], the discriminant is a quantity of fundamental importance in understanding the properties of a number field. It was established in 1922 by C.L. Siegel that non-trivial extensions of $\mathbb{Q}$ which lie completely in $\mathbb{R}$ have a discriminant greater than 1 and was expanded to all non-trivial finite extensions of $\mathbb{Q}$ by J.M. Calloway (see [14]), a result contained in his Ph.D. thesis.

Dedekind also discovered that the prime divisors of $d(K)$ are exactly the set of primes which ramify in K [17]. It is used in determining the upper bound of the norm of an ideal of $\mathcal{O}_K$, which can be used in some cases to compute the class number of a number field [40]. From the powerful conductor-discriminant formula, first deduced by Hasse [24] (see [44]), the sign of the discriminant (positive or negative) determines the parity of the number of complex embeddings of the field. It is also used in determining the maximum norm of a fractional ideal in a given ideal class, which in turn proves very useful in the deduction of class numbers in certain cases (see, for example, [40, p.116]). This bound on fractional ideal norms is known as the Minkowski bound and is derived using Minkowski's Convex Body Theorem. Another consequence of the deduction of the Minkowski bound is a lower bound for the discriminant of a number field, given by

$$| d(K) | \geq \frac{n^{2n}}{(n!)^2}\left(\frac{\pi}{4}\right)^{2r_2}$$

where r_2 is the number of injective $\mathbb{Q}$-homomorphisms $\varphi : K \longrightarrow \mathbb{C}$ [26]. For an abelian extension, the Kronecker-Weber theorem [40, p.244] implies that there is a positive integer f such that $K \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{f}}\right)$. The least such integer f is known as the **conductor** of K and is denoted by $f(K)$. This result was first proven (with some gaps) by Weber and completed by Hilbert (see [40, p.254] and [25]). The conductor-discriminant formula also links the conductor of an abelian number field to the conductors of its characters, which allows for the deduction that $f(K) \mid d(K)$ [42, p.416]. Moreover, $p \mid d(K)$ if and only if $p \mid f(K)$, meaning the conductor can also be used to determine the primes which ramify in K. The conductor-discriminant formula will be described in more detail in Section 1.1.

Much of the current research in discriminant formulas for certain classes of abelian number fields has been relying on a number field's defining irreducible polynomial, which is guaranteed to exist as abelian extensions of $\mathbb{Q}$ are necessarily Galois over $\mathbb{Q}$. The discriminant of a quadratic extension of $\mathbb{Q}$ is well-known: for $K = \mathbb{Q}\left(\sqrt{a}\right)$ where $a \neq 0, 1$ is square-free, the minimal polynomial of $\sqrt{a}$ is $g(x) = x^2 - a$ and we have

$$d(K) = \begin{cases} a, & \text{if } a \equiv 1 \pmod 4, \\ 4a, & \text{if } a \equiv 2, 3 \pmod 4. \end{cases}$$

The discriminant of a cubic extension of $\mathbb{Q}$ has been determined by Llorente, Nart and Vila [37] and Alaca [2], and is given more concisely in [3] in terms of a defining cubic trinomial $x^3 - ax + b$. In both cases, a general irreducible quadratic or cubic polynomial can be assumed to be of the forms given above using the same rationale as in Section 1.2. The discriminant of a cyclotomic extension of $\mathbb{Q}$, $\mathbb{Q}(\zeta_n)$, is

$$d(\mathbb{Q}(\zeta_n)) = (-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}},$$

where $\zeta_n = e^{2\pi i/n}$ and φ is Euler's totient function [52].

Beyond these fields, the theoretical computation of discriminants relies heavily on special cases of defining polynomials, usually with a restricted number of terms. A far-reaching result was obtained by Llorente and Nart in 1984 [36] for the primes dividing the discriminant of a number field defined by a general trinomial $x^n + Ax^s + B$ for $n > s \geq 1$, though it does not completely treat such cases. The cases of quartic and quintic trinomials have been treated in [6] and [1], respectively. The case of cyclic quintic fields defined by Lehmer quintics has been addressed in [30] and [19]. The discriminant of octic extensions K with $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$ given by an irreducible octic trinomial of the form $x^8 + Ax^2 + 1$ has been treated by [48]. Recent developments in the utilization of higher Newton polygons have provided another avenue in the deduction of field discriminants and construction of integral bases (see [23] and [22]).

Bicyclic quartic fields (also referred to as bicyclic biquadratic fields or occasionally as biquadratic fields) have been the subject of much study. Research completed in the past half-century on bicyclic quartic fields has included a focus on integral bases, discriminants and class numbers of bicyclic quartic fields.

A bicyclic quartic field K is a number field such that $[K : \mathbb{Q}] = 4$ and $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Bicyclic quartic fields may be expressed as $\mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ for square-free integers m and n where $m \neq 1$, $n \neq 1$ and $m \neq n$. Given K of the form $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$, the formulas for an integral basis and discriminant of K were deduced by Williams [53] based on simple congruence conditions of m, n and $\gcd(m, n)$ modulo 4. One key component of Williams' work is the use of explicit descriptions of K and its quadratic subfields. Work on finding other integral bases in terms of m and n has largely focused on power integral bases (see, for example, [41], [43] and [35]). Other notable work has been done to study the indices of elements of a bicyclic quartic field [29], the construction of a non-Euclidean ideal in a real bicyclic quartic field [21], sums of three squares of integral elements of a bicyclic quartic field [31] and the construction of a fundamental system of units assuming the abc conjecture [34].

Much work has been done in investigating the class numbers of biquadratic fields. The work of Stark [50], Uchida [51], and Brown and Parry [10] deduced that there are exactly 47 imaginary bicyclic quartic fields with class number 1. Setzer [47] then proved there are exactly 7 imaginary cyclic quartic fields of class number 1, concluding the investigation of class numbers of imaginary abelian quartic fields of class number 1. The case of imaginary bicyclic quartic fields of class number 2 was treated by Buell and Hugh and Kenneth S. Williams [13], where they determined there are exactly 160 imaginary bicyclic quartic fields of class number 2 by deducing any quadratic subfield must have class number 1, 2 or 4 and using previous results on the class numbers of quadratic extensions. Much later, in 1998, a list of all imaginary bicyclic quartic fields with class number 3 was completed by Jung and Kwong [32].

Gauss conjectured that there are infinitely-many quadratic fields of class number 1 and the search to prove or disprove this assertion has, in part, involved determining which bicyclic quartic fields contain a quadratic subfield of class number one (see, for example, [54]). Of course, all quartic extensions of $\mathbb{Q}$ are contained within a bicyclic quartic field, so it makes sense to investigate what restrictions a bicyclic quartic field would place on a quadratic subfield of a given class number. However, the conjecture has not yet been resolved as special cases are still being treated separately (see, for example, [7]). Computationally, it has been estimated, based on heuristics developed by Cohen and Lenstra, that approximately 75.45% of the class numbers of $\mathbb{Q}(\sqrt{p})$ are 1, where $p \equiv 1 \pmod 4$ is a prime (see [46] and [15]), which certainly lends some computational support to Gauss' conjecture.

The approach used in this thesis was made possible by the result stated by Kappe and Warren [33], which gives a powerful and complete classification of Galois groups of the splitting fields defined by irreducible quartic polynomials of the general form $g(x) = x^4 + Dx^3 + Ax^2 + Bx + C$ based entirely on their resolvent cubic $q(x)$ where $q(x) = x^3 - Ax^2 + (BD - 4C)x + 4AC - B^2 - CD^2$. The condition for a quartic polynomial to have a Klein-4 Galois group has been known for some time (see, for example, [27, Proposition 4.11] and [28, Theorem 43]). Spearman and Williams [49] used this result to obtain the conductor and discriminant of cyclic quartic fields.

The objective of this thesis is to determine both the conductor $f(K)$ and the discriminant $d(K)$ of a bicyclic quartic field K arithmetically in terms of A, B and C. While the discriminant of a bicyclic quartic field is known from the work of Williams [53], the work in this thesis will express both the conductor and discriminant of K in terms of the coefficients of a defining quartic polynomial without an explicit description of K and its subfields. We will begin in Chapter 1 with a discussion of the conductor-discriminant formula and its application to bicyclic quartic extensions to develop simple and effective formulas for finding the conductor and discriminant of such fields. Moreover, we will establish the simplifying assumptions on the defining quartic of K, $g(x) = x^4 + Ax^2 + Bx + C$, which are essential in making the proofs contained in this thesis more concise. In Chapter 2 we use the main theorem in [33] discussed above in the case where $\mathrm{Gal}_{\mathbb{Q}}(g(x)) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which implies that $q(x) = x^3 - Ax^2 - 4Cx + 4AC - B^2$ splits over $\mathbb{Z}$. Denoting the roots of $q(x)$ as r, s and t, we show that when $B \neq 0$, the quadratic subfields of K are given by $\mathbb{Q}\left(\sqrt{r-A}\right)$, $\mathbb{Q}\left(\sqrt{s-A}\right)$ and $\mathbb{Q}\left(\sqrt{t-A}\right)$. From there, the square-free parts of $r - A$, $s - A$ and $t - A$ (denoted r_1, s_1 and t_1, respectively) become the subject of our interest and the chapter is concluded with results from Chapter 1 applied to this new information. If p is a prime and m is a non-zero integer, we define the non-negative integer $v_p(m)$ by $p^{v_p(m)} \| m$. The results from the end of Chapter 2 illustrate why $v_p(f(K))$ and $v_p(d(K))$ require separate treatments from $\alpha = v_2(f(K))$ and $\beta = v_2(d(K))$, where p is an odd prime. Chapter 3 is the treatment of $v_p(f(K))$ and $v_p(d(K))$ in the first main case, where $AB(A^2 - 4C) \neq 0$. Chapters 4 and 5 deal with finding α and β in this first main case. Chapter 4 contains a collection of technical results on congruences modulo powers of 2 and uses these and subsequent results to break down Main Case 1 into 13 primary cases based on conditions on A, B and C modulo powers of 2. As this case breakdown is quite involved, a flowchart is included in Appendix Appendix B to help make this breakdown more accessible to the reader. It is certainly the case that Chapters 4 and 5 represent the most challenging and detail-intensive portions of the thesis. The treatments of Main Cases 2-5 are far less complex and are each treated in individual chapters, Chapters 6-9, respectively. As $B = 0$ in Main Cases 3 and 5 (Chapters 7 and 9, respectively), alternative methods different than those developed in Chapter 2 are used to deduce $f(K)$ and $d(K)$. Finally, we close with a discussion of future work directions. As the discriminant of a number field is closely related to its integral basis and ramification of integer primes, we briefly explore the connections between the thesis results and previous results on these subjects. As the conductor and discriminant of cyclic quartic extensions are given in terms of the coefficients of a defining irreducible quartic polynomial in [49] and for bicyclic quartic extensions in this thesis, natural future research arises in deducing the discriminants of other fields defined by irreducible quartic polynomials. However, since the only abelian fields which arise as the splitting field of an irreducible quartic polynomial are cyclic and bicyclic quartic extensions, the deduction of the conductor of fields defined by an irreducible quartic polynomial in terms of its coefficients is complete.

Chapter 1

Preliminaries

1.1 The Conductor-Discriminant Formula

We begin with developing an understanding of the Conductor-Discriminant Formula. Let $U = \{z \in \mathbb{C} \; : \; |z| = 1\}$ be the complex unit circle, $\zeta_n = e^{\frac{2\pi i}{n}}$ and G be a finite abelian group. A **character** is a group homomorphism $h : G \longrightarrow \mathbb{C}^*$, where $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$. Since G is finite and h is a group homomorphism, we have that $h(g)$ is an element of $\mathbb{C}^*$ of finite order. It follows that $h(g) \in U$, so we consider characters to be group homomorphisms with codomain U.

The **character group** of G is the set of all characters of G and is denoted $\hat{G}$. The identity element of $\hat{G}$ is the **principal character** P of G and is the trivial homomorphism from G to U; that is, $P(G) = \{1\}$. It is known that $G \cong \widehat{G}$ and $\hat{\hat{G}} \cong G$ [52, p.22]. We now wish to establish a couple of lemmas:

Lemma 1.1. Let G be a finite abelian group and let $H \leq G$. Define the restriction map

$$\rho : \hat{G} \longrightarrow \hat{H}$$

$$\gamma \mapsto \gamma\restriction_H .$$

Then $\ker(\rho) \cong G/H$.

Proof: We have

$$\ker(\rho) = \{\gamma \in \hat{G} \ \mid \ \gamma(h) = h \ \forall \ h \in H\}.$$

Let $g, g_1 \in G$ with $g_1 \in gH$, so $g_1 = gh_1$ for some $h_1 \in H$. Then for $\gamma \in \ker(\rho)$, we have that

$$\gamma(g_1) = \gamma(gh_1) = \gamma(g) \cdot 1 = \gamma(g)$$

thus the action of γ on cosets of H can be uniquely determined by its action on any coset representative. Therefore, each character $\gamma \in \ker(\rho)$ is in one-to-one correspondence with a character $\widetilde{\gamma} \in \widehat{G/H}$. Clearly, this correspondence represents a group isomorphism. Therefore, $\ker(\rho) \cong \widehat{G/H} \cong G/H$. $\square$

Lemma 1.2. Let G be a finite abelian group, let $H \leq G$ and define the set

$$X_H = \{\gamma \in \hat{G} \ \mid \ \ker(\gamma) \supseteq H\}.$$

Then $|X_H| = [G : H]$ and $H = \bigcap_{\gamma \in X_H} \ker(\gamma)$.

Proof: From the proof of Lemma 1.1, with $\rho : \hat{G} \longrightarrow \hat{H}$ as above, we know that $X_H = \ker(\rho)$, so $|X_H| = [G : H]$ and $X_H \cong G/H$. Moreover, every $\gamma \in X_H$ corresponds to a character $\widetilde{\gamma} \in \widehat{G/H}$ where $\gamma(g) = \widetilde{\gamma}(gH)$. From the Fundamental Theorem of Finitely-Generated Abelian Groups, we know that for some $k \geq 1$ we can express any $gH \in G/H$ as

$$gH = \prod_{i=1}^{k} g_i^{\alpha_i} H$$

where $\langle g_i H\rangle \cap \langle g_j H\rangle = H$ whenever $i \neq j$. Let $|g_i H| = n_i$ for $1 \leq i \leq k$ and define the character $\widetilde{\gamma_i} \in \widehat{G/H}$ by extending

$$\widetilde{\gamma_i}(g_i H) = \zeta_{n_i}$$

$$\widetilde{\gamma_i}(g_j H) = H \text{ when } j \neq i$$

to all of G/H. From here, we see that $\ker(\widetilde{\gamma_i}) = \langle g_1 H, g_2 H, ..., g_{i-1} H, g_{i+1} H, ..., g_k H\rangle$ and that $\bigcap_{i=1}^{k} \ker(\widetilde{\gamma_i}) = H$. Since $\gamma_i(g) = \widetilde{\gamma_i}(gH)\ \forall g \in G$, we have that $\bigcap_{i=1}^{k} \ker(\gamma_i) = H$. As $H \subseteq \ker(\gamma_i)$ for $1 \leq i \leq k$, we have that $\gamma_i \in X_H$ for $1 \leq i \leq k$. We then have

$$H = \bigcap_{i=1}^{k} \ker(\widetilde{\gamma_i}) \supseteq \bigcap_{\gamma \in X_H} \ker(\gamma) \supseteq H,$$

thus $\bigcap_{\gamma \in X_H} \ker(\gamma) = H$. $\square$

Denote $U_n = \{\zeta_n^k \mid 0 \leq k < n\}$ as the group of n^{th} roots of unity in $\mathbb{C}^*$. Define on U_n the group homomorphism $\widetilde{\psi_k} : \zeta_n \mapsto \zeta_n^k$. When $\gcd(k, n) = 1$, we can extend $\widetilde{\psi_k}$ to a $\mathbb{Q}$-automorphism ψ_k of $\mathbb{Q}(\zeta_n)$. We denote

$$G(n) = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\psi_k \mid 1 \leq k < n,\ \gcd(k, n) = 1\}.$$

We know that $G(n) \cong (\mathbb{Z}/n\mathbb{Z})^*$ via the group isomorphism $\phi : G(n) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$ which maps $\psi_k \mapsto k + n\mathbb{Z}$. A character $h : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow U$ may be extended to what is known as a **Dirichlet character** $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$, which is given by

$$\chi(k) = \begin{cases} h(\overline{k}), & \overline{k} \in (\mathbb{Z}/n\mathbb{Z})^*, \\ 0, & \text{otherwise}, \end{cases}$$

where $\overline{k} = k + n\mathbb{Z}$. When χ is defined via a character $h : (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow U$, we say that χ is a **Dirichlet character modulo n**. The smallest such n for which a given χ can be defined is known as the **conductor** of χ and is denoted $f(\chi)$. When n is as small as possible, χ is a **primitive character**. Therefore, all Dirichlet characters may be considered primitive modulo their conductor. We will assume from this point onward that all Dirichlet characters modulo n are defined to be primitive modulo n unless otherwise stated.

Now, let h be a character of $(\mathbb{Z}/n\mathbb{Z})^*$ such that the associated Dirichlet character χ_h is primitive modulo n. Define $\gamma_h = h \circ \phi$ where ϕ is the group isomorphism listed above between $G(n)$ and $(\mathbb{Z}/n\mathbb{Z})^*$. So $\gamma_h : G(n) \longrightarrow U$ is a group character where $\gamma_h(\psi_k) = h(k)$. The character γ_h as defined above is known as a **Galois character**. We consider the **conductor** of γ_h to be the conductor of the primitive Dirichlet character associated with h and denote this value $f(\gamma_h)$. We note that the principal character P has conductor 1. A Galois character γ_h is said to be **odd** if $h(-1 + n\mathbb{Z}) = -1$ and **even** if $h(-1 + n\mathbb{Z}) = 1$.

Let K be a finite abelian Galois extension of $\mathbb{Q}$. The Kronecker-Weber theorem [40, p. 256] implies that there is a positive integer f such that $K \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{f}}\right)$. The least such integer f is known as the **conductor** of K and is denoted by $f(K)$. For convenience of notation in this section, we will set $n = f(K)$. Now, let $H \leq G(n)$ such that $H = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)$. Replace the notation X_H with $X(K)$, so

$$X(K) = \{\gamma_h \in \widehat{G(n)} \mid \ker(\gamma_h) \supseteq H\}$$

is a set of Galois characters. We have from Lemma 1.1 that $X(K) \cong G(n)/H$. Since $G(n)$ is abelian, $\mathrm{Gal}(K/\mathbb{Q})$ is a normal subgroup of $G(n)$. Therefore, by the Fundamental Theorem of Galois Theory, $K/\mathbb{Q}$ is also a Galois extension of $\mathbb{Q}$ and $G(n)/H \cong \mathrm{Gal}(K/\mathbb{Q})$ [18, p.574]. Therefore, $X(K) \cong \mathrm{Gal}(K/\mathbb{Q})$. The **discriminant** of a number field K with $[K : \mathbb{Q}] = n$ is given by the value

$$d(K) = \det\left(\sigma_j(\alpha_i)\right)$$

where, for $1 \leq j \leq n$, $\sigma_j : K \longrightarrow \mathbb{C}$ is an injective field homomorphism which fixes $\mathbb{Q}$ and $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ is an integral basis of K.

We are finally able to present the conductor-discriminant formula [38, p. 182], [42, Proposition 8.7, p. 416].

Theorem 1.1 (Conductor-Discriminant Formula)**.** If $K/\mathbb{Q}$ is abelian, then

$$d(K) = (-1)^u \prod_{\gamma_h \in X(K)} f(\gamma_h) \tag{1.1}$$

and

$$f(K) = \operatorname{lcm}\{f(\gamma_h) \mid \gamma_h \in X(K)\} \tag{1.2}$$

where u denotes the number of odd characters in $X(K)$.

Since the principal character P has conductor 1, we have from (1.2) the following corollary:

Corollary 1.1. Let $F = \mathbb{Q}\left(\sqrt{m}\right)$ where $m \neq 1$ is square-free. Then if $\gamma \in X(F)$ is the non-principal character of $X(F)$, we have that $f(\gamma) = f(F) = |d(F)|$.

Proof: Since P has conductor 1, we have from (1.1) that $d(F) = (-1)^u f(\gamma)$. We know that $f(\gamma)$ is a positive integer and that

$$d\left(\mathbb{Q}\left(\sqrt{m}\right)\right) = \begin{cases} m, \; m \equiv 1 \pmod 4, \\ 4m, \; m \equiv 2, 3 \pmod 4. \end{cases}$$

Therefore, the signs of $d(F)$ and m are the same. Thus, $u = 0$ when m and $d(F)$ are positive and $u = 1$ when m and $d(F)$ are negative. Hence, $f(\gamma) = |d(F)|$. Furthermore, we have from (1.2) that

$$f(F) = \operatorname{lcm}\{f(\gamma_h) \mid \gamma_h \in X(F)\} = f(\gamma) = |d(F)|. \quad \square$$

1.2 Bicyclic Quartic Fields

Let K be a bicyclic quartic field; that is, $[K : \mathbb{Q}] = 4$ and $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. As K is an abelian extension, the Kronecker-Weber theorem [40, p. 256] implies that there is a positive integer f such that $K \subseteq \mathbb{Q}\left(e^{\frac{2\pi i}{f}}\right)$. The least such integer f is known as the **conductor** of K and is denoted by $f(K)$.

Claim. Let $g(x)$ be a defining polynomial for K. We show that $g(x)$ can be taken in the form

$$g(x) = x^4 + Ax^2 + Bx + C \in \mathbb{Z}[x], \tag{1.3}$$

$$x^4 + Ax^2 + Bx + C \text{ irreducible}, \tag{1.4}$$

$$\mathrm{Gal}(x^4 + Ax^2 + Bx + C) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \tag{1.5}$$

$$\text{and there does not exist a prime } p \text{ such that } p^2|A,\ p^3|B, \text{ and } p^4|C. \tag{1.6}$$

Proof: Let $g_0(x) = x^4 + a_0x^3 + b_0x^2 + c_0x + d_0 \in \mathbb{Z}[x]$ be a defining polynomial for K. Let

$$g_1(x) = g_0\left(x - \frac{a_0}{4}\right) = x^4 + a_1x^2 + b_1x + c_1 \in \mathbb{Q}[x]$$

so that $g_1(x)$ is a defining polynomial for K. Let d be the least positive integer such that $d^2a_1,\ d^3b_1,\ d^4c_1 \in \mathbb{Z}$. Letting

$$g_2(x) = d^4g_1\left(\frac{x}{d}\right) = x^4 + d^2a_1x^2 + d^3b_1x + d^4c_1 \in \mathbb{Z}[x],$$

we note that $g_2(x)$ is also a defining polynomial for K. As $g_2(x)$ is irreducible, we have that

$d^4 c_1 \neq 0$, so we can let k denote the largest positive integer such that $k^2 | d^2 a_1,\ k^3 | d^3 b_1,\ k^4 | d^4 c_1$. Then

$$g(x) = \frac{1}{k^4} g_2(kx) = x^4 + Ax^2 + Bx + C \in \mathbb{Z}[x]$$

is a defining polynomial for K such that there does not exist a prime p with $p^2|A$, $p^3|B$, and $p^4|C$. $\square$

As K is a bicyclic quartic field, there are square-free integers m and n with $m \neq 1$, $n \neq 1,\ m \neq n$ such that

$$K = \mathbb{Q}\left(\sqrt{m},\ \sqrt{n}\right). \tag{1.7}$$

Let $\rho = \dfrac{mn}{\gcd(m,n)^2}$. The three distinct quadratic subfields of K are

$$K_1 = \mathbb{Q}\left(\sqrt{m}\right),\ K_2 = \mathbb{Q}\left(\sqrt{n}\right),\ K_3 = \mathbb{Q}\left(\sqrt{\rho}\right).$$

Observe that ρ is square-free and

$$n = \frac{m\rho}{\gcd(m,\rho)^2},\quad m = \frac{n\rho}{\gcd(n,\rho)^2}.$$

Therefore, the roles of m, n and ρ may be interchanged. Moreover, these quantities are the unique square-free integers with the property that

$$K = \mathbb{Q}\left(\sqrt{m},\ \sqrt{n}\right) = \mathbb{Q}\left(\sqrt{n},\ \sqrt{\rho}\right) = \mathbb{Q}\left(\sqrt{m},\ \sqrt{\rho}\right).$$

Lemma 1.3. Let $K = \mathbb{Q}\left(\sqrt{m},\ \sqrt{n}\right)$ be a bicyclic quartic field, where m and n are square-free integers with $m \neq 1,\ n \neq 1,\ m \neq n$ and let $\rho = \dfrac{mn}{\gcd(m,n)^2}$. Then, up to a permutation of m, n and ρ, exactly one of the following is true:

(a) $m \equiv n \equiv \rho \equiv 1 \pmod 4$,

(b) $m \equiv n \equiv 3 \pmod 4$, $\rho \equiv 1 \pmod 4$,

(c) $m \equiv n \equiv 2$ or $6 \pmod 8$, $\rho \equiv 1 \pmod 4$,

(d) $m \equiv 2 \pmod 8$, $n \equiv 6 \pmod 8$, $\rho \equiv 3 \pmod 4$.

Proof: As we may interchange the roles of m, n and ρ, we will show that the value of ρ modulo 4 follows directly from conditions taken on m and n. First, suppose that m and n are odd, so that $\gcd(m,n)^2 \equiv 1 \pmod 4$. If $(m,n) \equiv (1,1) \pmod 4$ we have that $\rho \equiv 1 \pmod 4$. If $(m,n) \equiv (3,3) \pmod 4$ then we have $\rho \equiv 1 \pmod 4$. Supposing instead that m and n are even, we have that $2 \parallel \gcd(m,n)$, so $\rho \equiv \frac{m}{2} \cdot \frac{n}{2} \pmod 4$. If $(m,n) \equiv (2,2) \pmod 8$, then

$$\frac{m}{2} \cdot \frac{n}{2} \equiv 1 \cdot 1 \equiv 1 (\mathrm{mod}\ 4),$$

we have that $\rho \equiv 1 \pmod 4$. If $(m,n) \equiv (2,6) \pmod 8$ then we have

$$\frac{m}{2} \cdot \frac{n}{2} \equiv 1 \cdot 3 \equiv 3 \pmod 4,$$

so $\rho \equiv 3 \pmod 4$. If $(m,n) \equiv (3,6) \pmod 8$ then we have

$$\frac{m}{2} \cdot \frac{n}{2} \equiv 3 \cdot 3 \equiv 1 \pmod 4,$$

so $\rho \equiv 1 \pmod 4$. $\square$

As $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}] = [K_3 : \mathbb{Q}] = 2$, we have

$$f(K_1) = |d(K_1)|,\ f(K_2) = |d(K_2)|,\ f(K_3) = |d(K_3)|,$$

where $f(K_j)$ denotes the conductor of K_j and $d(K_j)$ denotes the discriminant of K_j for each $j \in \{1,2,3\}$ [38, p. 98]. By the conductor-discriminant formula (1.2) and Corollary 1.1, for the bicyclic quartic field K we have

$$f(K) = \operatorname{lcm}(f(K_1), f(K_2), f(K_3)) = \operatorname{lcm}(d(K_1), d(K_2), d(K_3)).$$

Note: we assume that the least common multiple of two or more integers is always non-negative. Now, by [42, Theorem 2.18, p. 61], we have

$$d(K_1) = \begin{cases} m, & \text{if } m \equiv 1 \pmod 4, \\ 4m, & \text{if } m \not\equiv 1 \pmod 4, \end{cases}$$

$$d(K_2) = \begin{cases} n, & \text{if } n \equiv 1 \pmod 4, \\ 4n, & \text{if } n \not\equiv 1 \pmod 4, \end{cases}$$

$$d(K_3) = \begin{cases} \rho, & \text{if } \rho \equiv 1 \pmod 4, \\ 4\rho, & \text{if } \rho \not\equiv 1 \pmod 4. \end{cases}$$

If $(m, n) \equiv (1, 1) \pmod 4$, then $\rho \equiv\ 1(\bmod 4)$, so

$$f(K) = \operatorname{lcm}(m, n, \rho) = \operatorname{lcm}(m, n).$$

If $(m, n) \not\equiv (1, 1) \pmod 4$, then $m \equiv 2$ or $3 \pmod 4$ or $n \equiv 2$ or $3 \pmod 4$. Interchanging m and n, if necessary, we may suppose that $m \equiv 2$ or $3 \pmod 4$, so $f(K_1) = 4|m|$. As $f(K_2) = |n|$ or $|4n|$ and $f(K_3) = |\rho|$ or $|4\rho|$, we have that

$$f(K) = 4\operatorname{lcm}(m, n, \rho) = 4\operatorname{lcm}(m, n).$$

Thus, we have established the following:

Lemma 1.4. Let $K = \mathbb{Q}\left(\sqrt{m},\ \sqrt{n}\right)$ be a bicyclic quartic field, where m and n are square-free integers with $m \neq 1,\ n \neq 1,\ m \neq n$. Then the conductor $f(K)$ of K is given by:

$$f(K) = 2^{\gamma} \cdot \operatorname{lcm}(m, n), \tag{1.8}$$

where

$$\gamma = \begin{cases} 0, \text{ if } m \equiv n \equiv 1 \pmod 4, \\ 2, \text{ otherwise.} \end{cases} \tag{1.9}$$

Corollary 1.2. Let $K = \mathbb{Q}\left(\sqrt{m},\ \sqrt{n}\right)$ be a bicyclic quartic field, where m and n are square-free integers with $m \neq 1,\ n \neq 1,\ m \neq n$. Then $\alpha = v_2(f(K))$ is given by:

$$\alpha = \begin{cases} 0, & \text{if } m \equiv n \equiv 1 \pmod 4, \\ 2, & \text{if at least one of } m \text{ or } n \ \equiv 3 \pmod 4 \text{ and } m \equiv n \equiv 1 \pmod 2, \\ 3, & \text{if at least one of } m \text{ or } n \ \equiv 2 \pmod 4. \end{cases}$$

Proof: If $m \equiv n \equiv 1 \pmod 4$ then by (1.9) we have that $\gamma = 0$ and $2 \nmid \operatorname{lcm}(m, n)$, therefore by (1.8) we have that $2 \nmid f(K)$, hence $\alpha = 0$. If $(m, n) \not\equiv (1, 1) \pmod 4$ we have $\gamma = 2$ by (1.9). If both m and n are odd, then again $2 \nmid \operatorname{lcm}(m, n)$, so by (1.8) we have that $2^2 \parallel f(K)$, hence $\alpha = 2$. Finally, if at least one of m and n is even, then as m and n are square-free we have that $2 \parallel \operatorname{lcm}(m, n)$, thus from (1.8) we have that $2^3 \parallel f(K)$, hence $\alpha = 3$. □

Note that $m \cdot n \cdot \rho = \left(\dfrac{mn}{\gcd(m, n)}\right)^2 = \operatorname{lcm}(m, n)^2$. As $d(K) = |d(K_1)d(K_2)d(K_3)|$ by the conductor-discriminant formula (1.1), we have the following result (which agrees with [53]):

Lemma 1.5. Let $K = \mathbb{Q}\left(\sqrt{m},\ \sqrt{n}\right)$ be a bicyclic quartic field, where m and n are square-free integers with $m \neq 1,\ n \neq 1,\ m \neq n$. Then the discriminant $d(K)$ of K is given by

$$d(K) = 2^{\delta} \operatorname{lcm}(m, n)^2, \tag{1.10}$$

where

$$\delta = \begin{cases} 0, & m \equiv n \equiv 1 \pmod 4, \\ 4, & m \equiv 1 \pmod 4,\ n \equiv 2 \text{ or } 3 \pmod 4, \\ 6, & m, n \not\equiv 1 \pmod 4. \end{cases} \tag{1.11}$$

If p is a prime and m is a non-zero integer, we define the non-negative integer $v_p(m)$ by $p^{v_p(m)} \| m$. Let $\beta = v_2(d(K))$. Then $\beta = \delta + 2v_2(\mathrm{lcm}(m, n))$ is determined in the following table:

Table 1.1

m	n	ρ	δ	$v_2(\mathrm{lcm}(m,n))$	α	β
1 (mod 4)	1 (mod 4)	1 (mod 4)	0	0	0	0
1 (mod 4)	3 (mod 4)	3 (mod 4)	4	0	2	4
3 (mod 4)	3 (mod 4)	1 (mod 4)	4	0	2	4
2 (mod 8)	2 (mod 8)	1 (mod 4)	4	1	3	6
2 (mod 8)	6 (mod 8)	3 (mod 4)	6	1	3	8
6 (mod 8)	6 (mod 8)	1 (mod 4)	4	1	3	6

We note from the table that $\beta = 2\alpha$ whenever m and n are odd as $\delta = 2\alpha$. Therefore, once the conductor is known, it is only when $\alpha = 3$ that extra calculation is required. Hence, we have deduced the following:

Corollary 1.3. Let $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ be a bicyclic quartic field, where m and n are square-free integers with $m \neq 1,\ n \neq 1,\ m \neq n$. Then, up to permutation of m and n, $\beta = v_2(d(K))$

is given by

$$\beta = \begin{cases} 2\alpha, & \text{if } \alpha \neq 3, \\ 6, & \text{if } (m,n) \equiv (1,2) \pmod 4 \text{ or when } m \equiv n \equiv 2 \text{ or } 6 \pmod 8, \\ 8, & \text{if } (m,n) \equiv (2,3) \pmod 4 \text{ or when } (m,n) \equiv (2,6) \pmod 8. \end{cases} \tag{1.12}$$

The objective of this thesis is to determine both the conductor $f(K)$ and the discriminant $d(K)$ of K arithmetically in terms of $A,\ B$ and C. As $g(x) = x^4 + Ax^2 + Bx + C$ is irreducible, we have

$$C \neq 0. \tag{1.13}$$

From Lemma 1.4, Corollary 1.2 and Corollary 1.3, we have the following theorem:

Theorem 1.2. Let $K = \mathbb{Q}\left(\sqrt{m},\ \sqrt{n}\right)$ be a bicyclic quartic field, where m and n are squarefree integers with $m \neq 1,\ n \neq 1,\ m \neq n,$ and $\rho = \dfrac{mn}{\gcd(m,n)^2}$. Furthermore, let $f(K) = 2^{\alpha} f_0(K)$ and $d(K) = 2^{\beta} d_0(K)$ where $\alpha = v_2(f(K))$ and $\beta = v_2(d(K))$. Then, up to a permutation of m, n and ρ, we have:

(a) $d_0(K) = f_0(K)^2$.

(b) $$\alpha = \begin{cases} 0, & \text{if } m \equiv n \equiv \rho \equiv 1 \pmod 4, \\ 2, & \text{if } m \equiv 1 \pmod 4 \text{ and } n \equiv \rho \equiv 3 \pmod 4, \\ 3, & \text{if } mn\rho \equiv 0 \pmod 2. \end{cases}$$

(c) $$\beta = \begin{cases} 2\alpha, & \text{if } \alpha \neq 3, \\ 6, & \text{if } m \equiv 1 \pmod 4 \text{ and } n \equiv \rho \equiv 2 \text{ or } 6 \pmod 8, \\ 8, & \text{if } m \equiv 3 \pmod 4 \text{ and } (n,\rho) \equiv (2,6) \pmod 8. \end{cases}$$

(d) When $\alpha \neq 3$, $d(K) = f(K)^2$.

Proof: For part **(a)**, from (1.8) and (1.10) we have

$$f(K) = 2^{\gamma} \operatorname{lcm}(m, n)$$

and

$$d(K) = 2^{\delta} \operatorname{lcm}(m, n)^2 .$$

Let $m_2 = v_2(m)$ and $n_2 = v_2(n)$, so that $m_0 = \frac{m}{2^{m_2}}$ and $n_0 = \frac{n}{2^{n_2}}$ are odd integers. Then, from (1.8) we have

$$f_0(K) = \operatorname{lcm}(m_0, n_0)$$

and

$$d_0(K) = \operatorname{lcm}(m_0, n_0)^2 = f_0(K)^2.$$

Parts **(b)** and **(c)** follow directly from Lemma 1.3, Corollary 1.2 and Corollary 1.3. Part **(d)** follows immediately from part **(a)** and Corollary 1.3. □

We set

$$a_p = v_p(A), \text{ if } A \neq 0,$$

$$b_p = v_p(B), \text{ if } B \neq 0,$$

$$c_p = v_p(C), \text{ if } C \neq 0,$$

$$l_p = v_p(A^2 - 4C), \text{ if } A^2 - 4C \neq 0,$$

$$e_p = \min(b_p, l_p) \text{ if } A^2 - 4C \neq 0 \text{ and } B \neq 0,$$

$$a = a_2,$$

$$b = b_2,$$

$$c = c_2,$$

$$l = l_2,$$

$$E = \frac{A^2 - 4C}{2^l} \equiv 1 \pmod 2,$$

$$\alpha = v_2(f(K)),$$

$$\beta = v_2(d(K)).$$

Five main cases naturally arise:

Main Case 1 : $A \neq 0,\ B \neq 0,\ A^2 - 4C \neq 0,$

Main Case 2 : $A \neq 0,\ B \neq 0,\ A^2 - 4C = 0,$

Main Case 3 : $A \neq 0,\ B = 0,$

Main Case 4 : $A = 0,\ B \neq 0,$

Main Case 5 : $A = 0,\ B = 0.$

In Main Case 3, as $x^4 + Ax^2 + Bx + C$ is irreducible, we have $A^2 - 4C \neq M^2$ for any integer M, therefore $A^2 - 4C \neq 0$. In Main Cases 4 and 5 we have $A^2 - 4C = -4C \neq 0$.

Main Case 1 is treated in Chapters 2-5. We prove the following result:

Theorem 1.3 (Main Case 1)**.** Let K be a bicyclic quartic field. Suppose that $K = \mathbb{Q}(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$ and A, B, C are integers satisfying (1.3), (1.4), (1.5), (1.6), and $AB(A^2 - 4C) \neq 0$. Then $f(K) = 2^\alpha f_0(K)$, where

$$f_0(K) = \prod_{\substack{p \text{ (prime)} \neq 2 \\ e_p \text{ odd}}} p \prod_{\substack{p \text{ (prime)} \neq 2 \\ e_p \geq 2 \text{ even} \\ p | A}} p$$

and the values of α are given in Table 1 in Appendix A. Moreover, $d(K) = 2^\beta (f_0(K))^2$ where the values of β are given in Tables 1 and 2 in Appendix A.

Main Case 2 is treated in Chapters 2 and 6. We prove the following result:

Theorem 1.4 (Main Case 2)**.** Let K be a bicyclic quartic field. Suppose that $K = \mathbb{Q}(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$ and A, B, C are integers satisfying (1.3), (1.4), (1.5), (1.6), $AB \neq 0$ and $A^2 - 4C = 0$. Then C is odd and $f(K) = 2^{\alpha} f_0(K)$, where

$$f_0(K) = \prod_{\substack{p \text{ (prime)} \neq 2 \\ v_p(B) \text{ odd}}} p,$$

and

$$\alpha = \begin{cases} 2, & \text{if } b \equiv 1 \pmod 2, \\ 3, & \text{if } b \equiv 0 \pmod 2. \end{cases}$$

Moreover, $d(K) = 2^{\beta} (f_0(K))^2$, where

$$\beta = \begin{cases} 4, & \text{if } b \equiv 1 \pmod 2, \\ 8, & \text{if } b \equiv 0 \pmod 2. \end{cases}$$

Main Case 3 is treated in Chapter 7. We prove the following result:

Theorem 1.5 (Main Case 3)**.** Let K be a bicyclic quartic field. Suppose that $K = \mathbb{Q}(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$ and A, B, C are integers satisfying (1.3), (1.4), (1.5), (1.6) and $A \neq 0,\ B = 0$. Then C is the square of a non-zero integer and $f(K) = 2^{\alpha} f_0(K)$, where

$$f_0(K) = \prod_{\substack{p \text{ (prime)} \neq 2 \\ v_p(-A + 2\sqrt{C}) \text{ or } v_p(-A - 2\sqrt{C}) \text{ odd}}} p$$

and the values of α are given in Tables 3 and 4 in Appendix A. Moreover, $d(K) = 2^{\beta} (f_0(K))^2$, where β is given in Tables 3 and 4 in Appendix A.

Main Case 4 is treated in Chapters 2 and 8. We prove the following result:

Theorem 1.6 (Main Case 4)**.** Let K be a bicyclic quartic field. Suppose that $K = \mathbb{Q}(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$ and A, B, C are integers satisfying (1.3), (1.4), (1.5), (1.6), $A = 0$, $B \neq 0$ and $b = v_2(B)$. Then $f(K) = 2^{\alpha} f_0(K)$, where

$$f(K) = 2^{\alpha} \prod_{\substack{p \text{ (prime)} \neq 2 \\ p^2 \mid B \text{ and } p^2 \parallel C}} p$$

where

$$\alpha = \begin{cases} 2, & \text{if } C \text{ is even,} \\ 3, & \text{if } C \text{ is odd,} \end{cases}$$

and $d(K) = 2^{\beta} f_0(K)^2$, where

$$\beta = \begin{cases} 4, & \text{if } C \text{ is even,} \\ 6, & \text{if } b = 2, \\ 8, & \text{if } b \geq 3. \end{cases}$$

Main Case 5 is treated in Chapter 9. We prove the following result:

Theorem 1.7 (Main Case 5)**.** Let K be a bicyclic quartic field. Suppose that $K = \mathbb{Q}(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$ and A, B, C are integers satisfying (1.3), (1.4), (1.5), (1.6) and $A = B = 0$. Then $C = n^2$ for some square-free $n \in \mathbb{Z}$,

$$f(K) = \begin{cases} 8|n|, & \text{if } n \text{ is odd,} \\ 2|n|, & \text{if } n \text{ is even,} \end{cases}$$

and

$$d(K) = \begin{cases} 16n^2, & \text{if } n \text{ is odd,} \\ 4n^2, & \text{if } n \text{ is even.} \end{cases}$$

The corresponding determination of the conductor of a cyclic quartic field was carried out by Spearman and Williams [49] in 1996. The bicyclic quartic case is much more complicated.

Chapter 2

Roots of the Resolvent Cubic of $x^4 + Ax^2 + Bx + C$ when $B \neq 0$

The following theorem is a part of Theorem 1 of [33].

Theorem 2.1. Let $A,\ B$ and C be integers such that $x^4 + Ax^2 + Bx + C$ is irreducible and $\mathrm{Gal}(x^4 + Ax^2 + Bx + C) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then the cubic resolvent of $x^4 + Ax^2 + Bx + C$, namely $x^3 - Ax^2 - 4Cx + (4AC - B^2)$, has three integer roots.

Consider $q(x) = x^3 - Ax^2 - 4Cx + (4AC - B^2)$, the resolvent cubic of $g(x)$ where $g(x) = x^4 + Ax^2 + Bx + C$. For the entirety of this chapter, we assume that $B \neq 0$ so that the analysis carried out in this chapter applies to Main Cases 1, 2 and 4. By the above theorem, q has three integer roots, say r, s and t. Thus

$$q(x) = x^3 - Ax^2 - 4Cx + (4AC - B^2) = (x - r)(x - s)(x - t) \tag{2.1}$$

and

$$r + s + t = A, \tag{2.2}$$

$$rs + st + rt = -4C, \tag{2.3}$$

$$rst = B^2 - 4AC. \tag{2.4}$$

Evaluating $q(A)$ in view of (2.1), we obtain

$$(r - A)(s - A)(t - A) = B^2. \tag{2.5}$$

As we are assuming that $B \neq 0$, we deduce from (2.5) that

$$r - A \neq 0,\ \ s - A \neq 0,\ \ t - A \neq 0. \tag{2.6}$$

From (2.4) we have

$$r \neq 0,\ \ s \neq 0,\ \ t \neq 0\ \text{ when } B^2 - 4AC \neq 0. \tag{2.7}$$

Evaluating $q(r)$ in view of (2.1), we have

$$q(r) = r^3 - Ar^2 - 4Cr + (4AC - B^2) = 0 \tag{2.8}$$

so that

$$(r - A)(r^2 - 4C) = B^2. \tag{2.9}$$

Similarly, we have

$$(s - A)(s^2 - 4C) = B^2 \tag{2.10}$$

and

$$(t - A)(t^2 - 4C) = B^2. \tag{2.11}$$

As $B \neq 0$, we see from (2.9)-(2.11) that

$$r^2 - 4C \neq 0, \ s^2 - 4C \neq 0, \ t^2 - 4C \neq 0. \tag{2.12}$$

We next generalize (2.6). For convenience, denote by $\square$ the set of all integer squares.

Lemma 2.1. $r - A \notin \square, \ s - A \notin \square, \ t - A \notin \square.$

Proof: Let $\theta = \theta_1, \theta_2, \theta_3, \theta_4$ be the four roots of $g(x)$, so that

$$\theta_1 + \theta_2 + \theta_3 + \theta_4 = 0, \tag{2.13}$$

$$\theta_1\theta_2 + \theta_1\theta_3 + \theta_1\theta_4 + \theta_2\theta_3 + \theta_2\theta_4 + \theta_3\theta_4 = A, \tag{2.14}$$

$$\theta_1\theta_2\theta_3 + \theta_1\theta_2\theta_4 + \theta_2\theta_3\theta_4 = -B, \tag{2.15}$$

$$\theta_1\theta_2\theta_3\theta_4 = C. \tag{2.16}$$

Then, as $q(x) = x^3 - Ax^2 - 4Cx + (4AC - B^2)$ is the resolvent cubic of $g(x) = x^4 + Ax^2 + Bx + C$, we have without loss of generality that

$$\theta_1\theta_2 + \theta_3\theta_4 = r, \tag{2.17}$$

$$\theta_1\theta_3 + \theta_2\theta_4 = s, \tag{2.18}$$

$$\theta_1\theta_4 + \theta_2\theta_3 = t. \tag{2.19}$$

Now, $\text{Gal}(K/\mathbb{Q}) = \text{Gal}(x^4 + Ax^2 + Bx + C) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \langle\sigma\rangle \times \langle\tau\rangle$, where

$$\sigma^2 = \tau^2 = 1, \ \sigma\tau = \tau\sigma,$$
$$\sigma : \theta_1 \longleftrightarrow \theta_3, \quad \theta_2 \longleftrightarrow \theta_4,$$
$$\tau : \theta_1 \longleftrightarrow \theta_2, \quad \theta_3 \longleftrightarrow \theta_4.$$

Suppose that $r - A \in \square$. Then there exists an integer m such that $r - A = m^2$. By (2.6) we see that $m \neq 0$. Further, by (2.2), we have $s + t = A - r = -m^2$. Hence, by (2.13), (2.18) and (2.19), we obtain

$$\begin{aligned}(\theta_1 + \theta_2 - \theta_3 - \theta_4)^2 &= (\theta_1 + \theta_2 + \theta_3 + \theta_4)^2 - 4(\theta_1 + \theta_2)(\theta_3 + \theta_4)\\ &= -4(\theta_1\theta_3 + \theta_1\theta_4 + \theta_2\theta_3 + \theta_2\theta_4)\\ &= -4(s + t) = 4m^2,\end{aligned}$$

so that

$$\theta_1 + \theta_2 - \theta_3 - \theta_4 = 2m$$

for some choice of sign of m. Then, from (2.13) we deduce

$$\theta_1 + \theta_2 = m, \ \theta_3 + \theta_4 = -m.$$

Then,

$$m = \sigma(m) = \sigma(\theta_1 + \theta_2) = \theta_3 + \theta_4 = -m$$

so $m = 0$, a contradiction. Thus $r - A \notin \square$, and similarly for $s - A \notin \square$ and $t - A \notin \square$. $\square$

Lemma 2.2. There do not exist integers j and k such that $j^2(r-A) = k^2(s-A)$ (and similarly for $r-A$ and $t-A$, as well as $s-A$ and $t-A$).

Proof: Suppose there exist non-zero integers j and k such that

$$j^2(r-A) = k^2(s-A).$$

By (2.5) and (2.6) we deduce that

$$t-A = \frac{B^2}{(r-A)(s-A)} = \left(\frac{kB}{j(r-A)}\right)^2$$

so that $t-A$ is the square of a rational number. But $t-A$ is an integer, thus it must be the square of an integer, contradicting Lemma 2.1. □

Theorem 2.2. When $B \neq 0$, the three quadratic subfields of K are $\mathbb{Q}\left(\sqrt{r-A}\right)$, $\mathbb{Q}\left(\sqrt{s-A}\right)$ and $\mathbb{Q}\left(\sqrt{t-A}\right)$.

Proof: Let $\theta_1, \theta_2, \theta_3, \theta_4$ be the four roots of $g(x) = x^4 + Ax^2 + Bx + C$. By (2.2), (2.18) and (2.19), we have

$$\begin{aligned} -4(s+t) &= -4(\theta_1\theta_3 + \theta_2\theta_4 + \theta_1\theta_4 + \theta_2\theta_3) \\ &= (\theta_1 + \theta_2 + \theta_3 + \theta_4)^2 - 4(\theta_1 + \theta_2)(\theta_3 + \theta_4) \\ &= (\theta_1 + \theta_2 - \theta_3 - \theta_4)^2 \end{aligned}$$

so that

$$\pm\sqrt{-s-t} = \frac{1}{2}(\theta_1 + \theta_2 - \theta_3 - \theta_4) \in \mathbb{Q}(\theta_1, \theta_2, \theta_3, \theta_4) = \mathbb{Q}(\theta) = K.$$

But by (2.2) we have

$$r + s + t = A,$$

so $r - A = -s - t$. Thus, $\sqrt{r-A} \in K$. By Lemma 2.1, $r - A \notin \square$ so we have that $\left[\mathbb{Q}\left(\sqrt{r-A}\right) : \mathbb{Q}\right] = 2$. Hence $\mathbb{Q}\left(\sqrt{r-A}\right)$ is a quadratic subfield of K. Similarly, $\mathbb{Q}\left(\sqrt{s-A}\right)$ and $\mathbb{Q}\left(\sqrt{t-A}\right)$ are quadratic subfields of K. These three quadratic subfields are distinct in view of Lemma 2.2. $\square$

From Lemma 1.3, Theorem 1.2 and Theorem 2.2, we immediately have the following corollaries:

Corollary 2.1. When $B \neq 0$, let $r - A = r_1 x^2$, $s - A = s_1 y^2$ and $t - A = t_1 z^2$, where $r_1,\ s_1$ and t_1 are square-free integers and $x,\ y$ and z are non-negative integers. Then, up to a permutation of $r,\ s$ and t, exactly one of the following must be true:

(a) $r_1 \equiv s_1 \equiv t_1 \equiv 1 \pmod 4$,

(b) $r_1 \equiv s_1 \equiv 3 \pmod 4,\ t_1 \equiv 1 \pmod 4$,

(c) $r_1 \equiv s_1 \equiv 2$ or $6 \pmod 8,\ t_1 \equiv 1 \pmod 4$,

(d) $r_1 \equiv 2 \pmod 8,\ s_1 \equiv 6 \pmod 8,\ t_1 \equiv 3 \pmod 4$.

Corollary 2.2. When $B \neq 0$, let $r - A = r_1 x^2$, $s - A = s_1 y^2$ and $t - A = t_1 z^2$ where $r_1,\ s_1$ and t_1 are square-free integers and $x,\ y$ and z are non-negative integers. Then, up to a permutation of $r,\ s$ and t, we have

(A) If $r_1 s_1 t_1 \equiv 0 \pmod 2$, then $\alpha = 3$. Furthermore, if we have $r_1 \equiv 1 \pmod 4$ and $s_1 \equiv t_1 \equiv 2$ or $6 \pmod 8$, then $\beta = 6$; otherwise, $r_1 \equiv 3 \pmod 4$, $(s_1, t_1) \equiv (2, 6) \pmod 8$ and $\beta = 8$.

(B) If all of r_1, s_1 or t_1 are odd and at most one of r_1, s_1 or t_1 is congruent to 1 modulo 4, then $\alpha = 2$.

(C) If $r_1 \equiv s_1 \equiv t_1 \equiv 1 \pmod 4$, then $\alpha = 0$.

Lemma 2.3. The roots of $x^3 + 2Ax^2 + (A^2 - 4C)X - B^2$ are $r - A,\ s - A$, and $t - A$.

Proof: By (2.2) we have

$$(r - A) + (s - A) + (t - A) = (r + s + t) - 3A = A - 3A = -2A.$$

By (2.2) and (2.3) we have

$$\begin{aligned}&(r - A)(s - A) + (s - A)(t - A) + (r - A)(t - A)\\ &= (rs + st + rt) - 2A(r + s + t) + 3A^2\\ &= -4C - 2A^2 + 3A^2 = A^2 - 4C.\end{aligned}$$

By (2.5) we have

$$(r - A)(s - A)(t - A) = B^2.$$

The result follows. □

From Lemma 2.3, we have

$$(r - A)^3 + 2A(r - A)^2 + (A^2 - 4C)(r - A) - B^2 = 0, \tag{2.20}$$

$$(s - A)^3 + 2A(s - A)^2 + (A^2 - 4C)(s - A) - B^2 = 0, \tag{2.21}$$

$$(t - A)^3 + 2A(t - A)^2 + (A^2 - 4C)(t - A) - B^2 = 0. \tag{2.22}$$

Chapter 3

Main Case 1: $AB(A^2 - 4C) \neq 0$. The odd part of the conductor

By (2.6) we can define square-free integers r_1,s_1 and t_1 and positive integers x, y and z by

$$r - A = r_1 x^2, \tag{3.1}$$

$$s - A = s_1 y^2, \tag{3.2}$$

$$t - A = t_1 z^2. \tag{3.3}$$

Moreover, by Lemmas 2.1 and 2.2, we have

$$r_1 \neq 1,\ s_1 \neq 1,\ t_1 \neq 1, r_1 \neq s_1,\ s_1 \neq t_1,\ r_1 \neq t_1. \tag{3.4}$$

By (3.1)-(3.3) and Theorem 2.2 we have that

$$\mathbb{Q}\left(\sqrt{r_1}\right),\ \mathbb{Q}\left(\sqrt{s_1}\right),\ \mathbb{Q}\left(\sqrt{t_1}\right) \tag{3.5}$$

are the three distinct quadratic subfields of K. Clearly,

$$|r_1| = \prod_{\substack{p \text{ (prime)} \\ v_p(r-A) \text{ odd}}} p, \quad |s_1| = \prod_{\substack{p \text{ (prime)} \\ v_p(s-A) \text{ odd}}} p, \quad |t_1| = \prod_{\substack{p \text{ (prime)} \\ v_p(t-A) \text{ odd}}} p. \tag{3.6}$$

By Lemma 2.3 and (2.20)-(2.22), we see that

$$r_1x^2 + s_1y^2 + t_1z^2 = -2A, \tag{3.7}$$

$$r_1s_1x^2y^2 + s_1t_1y^2z^2 + r_1t_1x^2z^2 = A^2 - 4C, \tag{3.8}$$

$$r_1s_1t_1x^2y^2z^2 = B^2, \tag{3.9}$$

$$r_1^3x^6 + 2Ar_1^2x^4 + (A^2 - 4C)r_1x^2 - B^2 = 0, \tag{3.10}$$

$$s_1^3y^6 + 2As_1^2y^4 + (A^2 - 4C)s_1y^2 - B^2 = 0, \tag{3.11}$$

$$t_1^3z^6 + 2At_1^2z^4 + (A^2 - 4C)t_1z^2 - B^2 = 0. \tag{3.12}$$

From (3.9) we see that

$$r_1s_1t_1 = \left(\frac{B}{xyz}\right)^2. \tag{3.13}$$

From (3.1)-(3.3) we see that for a prime p we have

$$v_p(r-A) + v_p(s-A) + v_p(t-A) \equiv v_p(r_1) + v_p(s_1) + v_p(t_1) \pmod 2.$$

As $v_p(r_1) + v_p(s_1) + v_p(t_1) = v_p(r_1s_1t_1) \equiv 0 \pmod 2$, by (3.13), we obtain

$$v_p(r-A) + v_p(s-A) + v_p(t-A) \equiv 0 \pmod 2. \tag{3.14}$$

As the quadratic subfields of K are given by the square roots of $r - A$, $s - A$ and $t - A$

and the conductor is given in terms of the generators of the quadratic subfields of K, we wish to discover when $v_p(r-A)$, $v_p(s-A)$ and $v_p(t-A)$ are odd.

Lemma 3.1. Let p be an odd prime. If at least one of $v_p(r-A), v_p(s-A), v_p(t-A)$ is odd, then either e_p is odd or e_p is even with $e_p \geq 2$ and $p \mid A$.

Proof: As we may permute r, s, and t, we may suppose without loss of generality that $v_p(r-A)$ is odd, say $v_p(r-A) = 2h+1$ for some non-negative integer h. To prove the assertion of the lemma we must show that if e_p is even then $e_p \geq 2$ and that $p \mid A$.

Suppose that $e_p = 0$. Then $e_p = \min(v_p(A^2-4C), v_p(B)) = \min(l_p, b_p) = 0$. If $l_p > b_p$ then $b_p = 0$, so $p \nmid B$. Hence, by (2.5), we see that $p \nmid r-A$. Thus $v_p(r-A) = 0$, contradicting the assumption that $v_p(r-A)$ is odd. Now, if $b_p \geq l_p$ then $l_p = 0$ so $p \nmid A^2-4C$. As $v_p(r-A) = 2h+1$, we have $p^{2h+1} \parallel r-A$. Hence

$$p^{2h+2} \mid (r-A)^3,\ p^{2h+2} \mid 2A(r-A)^2,\ p^{2h+1} \parallel (A^2-4C)(r-A).$$

Thus

$$p^{2h+1} \parallel (r-A)^3 + 2A(r-A)^2 + (A^2-4C)(r-A).$$

By (2.20) we deduce $p^{2h+1} \parallel B^2$, which is impossible. Thus $e_p > 0$. As e_p is even, we have that $e_p \geq 2$.

Now, suppose that $p \nmid A$, so $a_p = 0$. We have

$$p^{6h+3} \parallel (r-A)^3,\ p^{4h+2} \parallel 2A(r-A)^2.$$

Thus, as p is odd, we have

$$p^{4h+2} \parallel (r-A)^3 + 2A(r-A)^2.$$

Recall (2.20); namely, that

$$(r-A)^3 + 2A(r-A)^2 + (A^2-4C)(r-A) - B^2 = 0. \tag{2.20}$$

Therefore, we have

$$p^{4h+2} \parallel (A^2-4C)(r-A) - B^2.$$

Then

$$p^{l_p+2h+1} \parallel (A^2-4C)(r-A), \ \ p^{2b_p} \parallel B^2.$$

From this, we deduce:

(i) $4h+2 = 2b_p$, if $l_p + 2h + 1 > 2b_p$,

(ii) $4h+2 = l_p + 2h + 1$, if $l_p + 2h + 1 < 2b_p$,

(iii) $4h+2 \geq 2b_p$, if $l_p + 2h + 1 = 2b_p$.

If (i) holds, then $b_p = 2h+1$ and $l_p > b_p$, so

$$e_p = \min(l_p, b_p) = b_p = 2h+1,$$

contradicting the fact that e_p is even.

If (ii) holds, then $l_p = 2h+1$ and $b_p > l_p$, so

$$e_p = \min(l_p, b_p) = l_p = 2h+1,$$

again contradicting the fact that e_p is even.

If (iii) holds, then $2h + 1 \geq b_p$, so $2b_p = l_p + 2h + 1 \geq l_p + b_p$, thus $l_p \leq b_p$. Hence

$$e_p = \min(l_p, b_p) = l_p = 2b_p - 2h - 1,$$

which contradicts e_p being even. Therefore, $p \nmid A$ is impossible, so $p \mid A$. This completes the proof of Lemma 3.1. □

Remark 3.1. If $a_p \geq 2$, $b_p \geq 3$ and $l_p \geq 4$, then, as $p^4 \mid A^2$, $p^4 \mid A^2 - 4C$ and $p \neq 2$, we deduce that $p^4 \mid C$, so that $p^2 \mid A$, $p^3 \mid B$, and $p^4 \mid C$, contradicting our simplifying assumption from (1.6). Thus

$$a_p \geq 2 \text{ and } b_p \geq 3 \text{ and } l_p \geq 4 \text{ cannot occur.} \tag{3.15}$$

Remark 3.2. If $p \mid B$ then from (2.5) we deduce that p divides one of $r - A$, $s - A$ and $t - A$. Relabelling r, s and t if necessary, we may suppose that $p \mid r - A$ without loss of generality. Thus

$$b_p \geq 1 \;\Rightarrow\; p \mid r - A. \tag{3.16}$$

Remark 3.3. If $v_p(r - A)$ is even, say $2h$ for some non-negative integer h (so $p^{2h} \parallel r - A$), then

$$p^{6h} \parallel (r - A)^3,\; p^{a_p + 4h} \parallel 2A(r - A)^2,\; p^{l_p + 2h} \parallel (A^2 - 4C)(r - A),\; p^{2b_p} \parallel B^2.$$

and solving (2.20) for B^2,

$$(r - A)^3 + 2A(r - A)^2 + (A^2 - 4C)(r - A) = B^2, \tag{2.20}$$

we have

$$v_p\left((r-A)^3 + 2A(r-A)^2 + (A^2-4C)(r-A)\right) = v_p(B^2).$$

Set $m_p = \min(v_p(r-A)^3, v_p(A(r-A)^2), v_p((A^2-4C)(r-A)))$. From this, we see that six cases arise:

Case (i): When $v_p((r-A)^3) = v_p(A(r-a)^2),\ 6h = a_p + 4h \leq \min(l_p + 2h, 2b_p)$,

Case (ii): When $v_p((r-A)^3) = v_p((A^2-4C)(r-A))$,
$6h = l_p + 2h \leq \min(a_p + 4h, 2b_p)$,

Case (iii): When $m_p = v_p((r-A)^3),\ 6h = 2b_p \leq \min(a_p + 4h, l_p + 2h)$,

Case (iv): When $v_p(A(r-A)^2) = v_p((A^2-4C)(r-A))$,
$a_p + 4h = l_p + 2h \leq \min(6h, 2b_p)$,

Case (v): When $m_p = v_p(A(r-A)^2),\ a_p + 4h = 2b_p \leq \min(l_p + 2h, 6h)$,

Case (vi): When $m_p = v_p((A^2-4C)(r-A)),\ l_p + 2h = 2b_p \leq \min(6h, a_p + 4h)$.

We now treat the converse of Lemma 3.1 in two parts.

Lemma 3.2. Let p be an odd prime. If e_p is odd, then at least one of $v_p(r-A)$, $v_p(s-A)$ or $v_p(t-A)$ is odd.

Proof: By way of contradiction, assume that $v_p(r-A)$, $v_p(s-A)$ and $v_p(t-A)$ are all even. We define the non-negative integer h by $v_p(r-A) = 2h$ and treat the six cases as described in Remark 3.3.

Cases (i),(ii),(iii). In these cases, we have $a_p \geq 2h,\ b_p \geq 3h,\ l_p \geq 4h$. As e_p is odd, we have $\min(l_p, b_p) = e_p \geq 1$ so that $l_p \geq 1$ and $b_p \geq 1$. From (3.16) we deduce that $p \mid r - A$, so $h \geq 1$. Thus, $a_p \geq 2$, $b_p \geq 3$ and $l_p \geq 4$. This is a contradiction by (3.15).

Case (iv). Here $a_p \leq 2h$, $b_p \geq \frac{a_p}{2} + 2h$ and $l_p = a_p + 2h$.

First, we treat the case $l_p \geq b_p$. If $a_p = 0$ then $b_p \geq 2h$ and $l_p = 2h$, so $l_p = b_p = 2h$, contradicting that $e_p = \min(l_p, b_p) = b_p$ is odd. If $a_p = 1$ then $b_p \geq \frac{1}{2} + 2h$ and $l_p = 1 + 2h$ so that $l_p = b_p = 1 + 2h$. Hence

$$p \parallel A,\ p^{1+2h} \parallel B,\ p^{1+2h} \parallel A^2 - 4C,\ p^{2h} \parallel r - A.$$

As $b_p \geq 1$ by (3.16) we have $h \geq 1$. Now by (2.5) we have

$$p^{2h+2} \parallel \frac{B^2}{r - A} = (s - A)(t - A),$$

so $p \mid s - A$ or $p \mid t - A$. Without loss of generality, we may suppose that $p \mid s - A$. From Lemma 2.3 we have

$$(r - A) + (s - A) + (t - A) = -2A \tag{3.17}$$

and, as $p \mid r - A$, $p \mid s - A$ and $p \mid A$, we deduce that $p \mid t - A$. But $v_p(r - A)$, $v_p(s - A)$, and $v_p(t - A)$ are all even, so $p^2 \mid r - A$, $p^2 \mid s - A$, and $p^2 \mid t - A$. Thus $p^2 \mid A$, contradicting $p \parallel A$. If $a_p \geq 2$, then $h \geq 1$ so $b_p \geq 3$ and $l_p \geq 4$. This contradicts (3.15).

We now turn to the case where $b_p > l_p$. In this case, we have $a_p \leq 2h$, $l_p \leq 4h$, $l_p = a_p + 2h$, $b_p \geq \frac{a_p}{2} + 2h$. If $a_p = 0$, then $b_p \geq 2h$ and $l_p = 2h$, so $e_p = \min(l_p, b_p) = 2h$ is even, a contradiction. If $a_p = 1$ then $h \geq 1$, $l_p = 1 + 2h$, $b_p \geq 1 + 2h$. As $b_p > l_p$ we have

$b_p \geq 2 + 2h$. Now, by (2.5), we deduce

$$p^{2h+4} \mid \frac{B^2}{r - A} = (s - A)(t - A),$$

so $p \mid s - A$ or $p \mid t - A$. Without loss of generality, we may suppose that $p \mid s - A$. Since $p \mid r - A$, $p \mid s - A$ and $p \mid A$, we deduce from (3.17) that $p \mid t - A$. But $v_p(r - A)$, $v_p(s - A)$ and $v_p(t - A)$ are all even, so $p^2 \mid r - A$, $p^2 \mid s - A$, $p^2 \mid t - A$. Thus $p^2 \mid A$, contradicting $p \parallel A$. If $a_p \geq 2$ then $h \geq 1$, $l_p \geq 2 + 2h \geq 4$ and $b_p > l_p \geq 4$ contradicting (3.15).

Case (v). Here a_p is even, $b_p = \frac{a_p}{2} + 2h$, $a_p \leq 2h$, $b_p \leq 3h$, $l_p \geq a_p + 2h$.

If $a_p = 0$ then $b_p = 2h$ and $l_p \geq 2h$, thus $e_p = \min(l_p, b_p) = b_p = 2h$, contradicting the fact that e_p is odd. If $a_p \geq 2$ then $h \geq 1$, so $b_p \geq 1 + 2h \geq 3$ and $l_p \geq 2 + 2h \geq 4$, contradicting (3.15).

Case (vi). Here l_p is even, $b_p = \frac{l_p}{2} + h$, $l_p \leq 4h$, $b_p \leq 3h$ and $a_p \geq l_p - 2h$.

If $h = 0$ then $l_p = b_p = 0$, so $e_p = \min(l_p, b_p) = 0$, contradicting the fact that e_p is odd.

If $h \geq 1$ and $l_p \geq b_p$ then $e_p = \min(l_p, b_p) = b_p$, so b_p is odd. But l_p is even, so $l_p \geq b_p + 1$. Thus $l_p \geq \frac{l_p}{2} + h + 1$, so $l_p \geq 2h + 2 \geq 4$ and $b_p = \frac{l_p}{2} + h \geq 2h + 1 \geq 3$. Also, $a_p \geq l_p - 2h \geq 2$. This contradicts (3.15).

If $h \geq 1$ and $b_p > l_p$ then $e_p = \min(l_p, b_p) = l_p$ is even, contradicting the fact that e_p is odd.

Therefore, all six cases are impossible, so our assumption that all of $v_p(r-A)$, $v_p(s-A)$ and $v_p(t - A)$ are even is invalid. This completes the proof of Lemma 3.2. □

Lemma 3.3. Let p be an odd prime. If e_p is even with $e_p \geq 2$ and $p \mid A$, then at least one of $v_p(r - A)$, $v_p(s - A)$ or $v_p(t - A)$ is odd.

Proof: By way of contradiction, assume that $v_p(r-A)$, $v_p(s-A)$ and $v_p(t-A)$ are all even.

Define the non-negative integer h by $v_p(r - A) = 2h$. As $p \mid A$ we have $a_p \geq 1$. As

$e_p = \min(l_p, b_p) \geq 2$ we have $l_p \geq 2$ and $b_p \geq 2$. As e_p is even, we have

$$\begin{cases} b_p \text{ even, if } l_p > b_p, \\ l_p \text{ even, if } b_p \geq l_p. \end{cases} \tag{3.18}$$

We treat the six cases described in Remark 3.3.

Cases (i), (ii), (iii). In these cases we have $a_p \geq 2h$, $b_p \geq 3h$, $l_p \geq 4h$.

As $b_p \geq e_p \geq 2$, by (3.16) we have $h \geq 1$. Thus $a_p \geq 2$, $b_p \geq 3$, $l_p \geq 4$, a contradiction to (3.15).

Case (iv). Here, $a_p \leq 2h$, $l_p \leq 4h$, $l_p = a_p + 2h$ and $b_p \geq \frac{a_p}{2} + 2h$.

As $a_p \geq 1$ we have $h \geq 1$. If $a_p = 1$ then $l_p = 1+2h$ and $b_p \geq \frac{1}{2}+2h$, so $b_p \geq 1+2h$. Thus $b_p \geq l_p$, so by (3.18) we have that l_p is even, a contradiction. If $a_p \geq 2$ then $b_p \geq 1 + 2h \geq 3$ and $l_p \geq 2 + 2h \geq 4$, contradicting (3.15).

Case (v). Here, a_p is even, $a_p \leq 2h$, $b_p \leq 3h$, $l_p \geq a_p + 2h$ and $b_p = \frac{a_p}{2} + 2h$.

As $a_p \geq 1$ and a_p is even we have $a_p \geq 2$. Also, $h \geq 1$. Thus, $b_p \geq 1 + 2h \geq 3$ and $l_p \geq 2 + 2h \geq 4$, contradicting (3.15).

Case (vi). Here l_p is even, $b_p = \frac{l_p}{2} + h$, $l_p \leq 4h$, $b_p \leq 3h$ and $a_p \geq l_p - 2h$.

As $b_p \geq 2$ we have $h \geq 1$. By (2.5) we have

$$p^{l_p} \; \Big\| \; \frac{B^2}{r-A} = (s-A)(t-A) \; .$$

As $l_p \geq 2$, p divides either $s - A$ or $t - A$. Without loss of generality, we may suppose that $p \mid s-A$. As $p \mid r-A$, $p \mid s-A$ and $p \mid A$, we deduce from (3.17) that $p \mid t-A$. But $v_p(r-A)$, $v_p(s-A)$ and $v_p(t-A)$ are all even, so $p^2 \mid r-A$, $p^2 \mid s-A$ and $p^2 \mid t-A$. Thus $p^2 \mid A$, hence

$a_p \geq 2$. Also,

$$p^6 \mid (r - A)(s - A)(t - A) = B^2,$$

so $b_p \geq 3$. Also, $p^4 \mid (s - A)(t - A)$, so $l_p \geq 4$. This contradicts (3.15).

Therefore, all six cases are impossible, so our assumption that all of $v_p(r-A)$, $v_p(s-A)$ and $v_p(t - A)$ are even is invalid. This completes the proof of Lemma 3.3. $\square$

Lemma 3.4. Let p be an odd prime. Then at least one of $v_p(r - A), v_p(s - A)$ or $v_p(t - A)$ is odd if and only if e_p is odd or e_p is even, $e_p \geq 2$ and $p \mid A$.

Proof: This follows immediately from Lemmas 3.1-3.3. $\square$

We are now in a position to determine the odd part of the conductor of a bicyclic quartic field in Main Case 1.

Theorem 3.1. Let K be a bicyclic quartic field. Suppose that $K = \mathbb{Q}(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$ and A, B, C are integers satisfying (1.5) and (1.6) and $AB(A^2 - 4C) \neq 0$. Then the odd part $f_0(K)$ of the conductor $f(K)$ is given by

$$f_0(K) = \prod_{\substack{p \text{ (prime)} \neq 2 \\ e_p \text{ odd}}} p \prod_{\substack{p \text{ (prime)} \neq 2 \\ p|A,\ e_p \text{ (even)} \geq 2}} p$$

and the odd part $d_0(K)$ of the discriminant $d(K)$ is given by

$$d_0(K) = \prod_{\substack{p \text{ (prime)} \neq 2 \\ e_p \text{ odd}}} p^2 \prod_{\substack{p \text{ (prime)} \neq 2 \\ p|A,\ e_p \text{ (even)} \geq 2}} p^2.$$

Proof: By (3.5) we have

$$K = \mathbb{Q}\left(\sqrt{r_1},\ \sqrt{s_1}\right).$$

By (3.6) we have

$$|r_1| = \prod_{\substack{p \text{ (prime)} \\ v_p(r-A) \text{ odd}}} p, \quad |s_1| = \prod_{\substack{p \text{ (prime)} \\ v_p(s-A) \text{ odd}}} p.$$

By (1.8) and (1.9) we have $f(K) = (1 \text{ or } 4)\mathrm{lcm}(r_1, s_1)$, hence

$$\begin{aligned} f_0(K) &= \mathrm{lcm}\left(\prod_{\substack{p \text{ (prime)} \neq 2 \\ v_p(r-A) \text{ odd}}} p, \prod_{\substack{p \text{ (prime)} \neq 2 \\ v_p(s-A) \text{ odd}}} p \right) \\ &= \prod_{\substack{p \text{ (prime)} \neq 2 \\ v_p(r-A) \text{ or } v_p(s-A) \text{ odd}}} p \\ &= \prod_{\substack{p \text{ (prime)} \neq 2 \\ \text{at least one of} \\ v_p(r-A), v_p(s-A), v_p(t-A) \text{ odd}}} p, \end{aligned}$$

by (3.14). By Lemma 3.4 we have

$$\prod_{\substack{p \text{ (prime)} \neq 2 \\ e_p \text{ odd}}} p \prod_{\substack{p \text{ (prime)} \neq 2 \\ e_p \geq 2 \text{ even} \\ p \mid A}} p = \prod_{\substack{p \text{ (prime)} \neq 2 \\ \text{at least one of} \\ v_p(r-A), v_p(s-A), v_p(t-A) \text{ odd}}} p.$$

The formula for $f_0(K)$ now follows. The formula for $d_0(K)$ follows directly from Theorem 1.2. $\square$

Chapter 4

Main Case 1: Congruences for A, B, C modulo powers of 2

Throughout this section A, B and C are integers such that (1.3)-(1.6) hold and A, B and $A^2 - 4C$ are all non-zero. The non-negative integers a, b, c and l and the odd integers A_1, B_1, C_1 and E are defined by

$$A = 2^a A_1,\ B = 2^b B_1,\ C = 2^c C_1,\ A^2 - 4C = 2^l E.$$

Since $\mathrm{Gal}(x^4+Ax^2+Bx+C) \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, there are restrictions on the residue classes modulo powers of 2 to which A, B, C and E can belong. We determine these residue classes in this section.

We recall from (2.2)-(2.4) that there are non-zero integers r, s and t such that

$$r + s + t = A, \tag{4.1}$$

$$rs + st + rt = -4C, \tag{4.2}$$

$$rst = B^2 - 4AC. \tag{4.3}$$

By Lemma 2.3 the integers $r-A$, $s-A$ and $t-A$ satisfy

$$(r-A)+(s-A)+(t-A) = -2A, \tag{4.4}$$

$$(r-A)(s-A)+(s-A)(t-A)+(r-A)(t-A) = A^2-4C, \tag{4.5}$$

$$(r-A)(s-A)(t-A) = B^2. \tag{4.6}$$

Our first result of this section gives results about the quantities $u+v+w$, $uv+vw+uw$ and uvw modulo powers of 2, where u, v and w are integers. These will be very useful in analyzing (4.1)-(4.6).

Proposition 4.1. Let $u, v, w \in \mathbb{Z}$. Let (P) indicate "up to permutation of u, v and w". Then

(i):

$$\left\{\begin{array}{c} u+v+w \equiv 1 \pmod 2 \\ uvw \equiv 8 \pmod{16} \end{array}\right\} \Rightarrow uv+vw+uw \equiv 2 \pmod 4,$$

(ii):

$$\left\{\begin{array}{c} u+v+w \equiv 0 \pmod 4 \\ uv+vw+uw \equiv 0 \pmod 4 \end{array}\right\} \Rightarrow \left\{\begin{array}{c} u \equiv v \equiv w \equiv 0 \pmod 2 \\ \text{at least one of } u, v, w \equiv 0 \pmod 4 \\ \text{and } uvw \equiv 0 \pmod{16} \end{array}\right\},$$

(iii):

$$\left\{\begin{array}{c} u+v+w \equiv 0 \pmod 4 \\ uv+vw+uw \equiv 0 \pmod 8 \end{array}\right\} \Rightarrow u \equiv v \equiv w \equiv 0 \pmod 4,$$

(iv):

$$\left\{\begin{array}{c} u+v+w \equiv 4 \pmod 8 \\ uv+vw+uw \equiv 4 \pmod{16} \end{array}\right\} \begin{array}{c}(P)\\ \Rightarrow\end{array} \left\{\begin{array}{c} u \equiv 0 \pmod 8,\ v \equiv w \equiv 2 \pmod 4 \\ v \equiv w \pmod 8 \end{array}\right\},$$

(v):

$$\left\{\begin{array}{c} u+v+w \equiv 4 \pmod 8 \\ uv+vw+uw \equiv 12 \pmod{16} \end{array}\right\} \begin{array}{c}(P)\\ \Rightarrow\end{array} \left\{\begin{array}{c} u \equiv 4 \pmod 8,\ v \equiv 2 \pmod 8 \\ w \equiv 6 \pmod 8 \end{array}\right\},$$

(vi):

$$\left\{\begin{array}{c} u+v+w \equiv 0 \pmod 8 \\ uv+vw+uw \equiv 4 \pmod 8 \\ uvw \equiv 0 \pmod{64} \end{array}\right\} \begin{array}{c}(P)\\ \Rightarrow\end{array} \left\{\begin{array}{c} u \equiv v \equiv 2 \pmod 4,\ w \equiv 0 \pmod{16} \\ u \equiv -v \pmod 8 \end{array}\right\},$$

(vii):

$$\left\{\begin{array}{c} u+v+w \equiv 0 \pmod 8 \\ uv+vw+uw \equiv 0 \pmod 4 \\ uvw \equiv 16 \pmod{64} \end{array}\right\} \begin{array}{c}(P)\\ \Rightarrow\end{array} \left\{\begin{array}{c} u \equiv v \equiv 2 \pmod 4,\ w \equiv 4 \pmod{16} \\ u \equiv v \pmod 8 \end{array}\right\},$$

(viii):

$$\left\{\begin{array}{c} u+v+w \equiv 2 \pmod 4 \\ uv+vw+uw \equiv 12 \pmod{16} \end{array}\right\} \Rightarrow\ u \equiv v \equiv w \equiv 2 \pmod 4.$$

Proof: (i): Clearly $uvw \neq 0$, so we can define non-negative integers α, β and γ and odd integers u_1, v_1, w_1 by

$$u = 2^{\alpha} u_1, \ v = 2^{\beta} v_1, \ w = 2^{\gamma} w_1.$$

By permuting u, v and w if necessary, we may suppose that $\alpha \le \beta \le \gamma$. Then

$$2^{\alpha} u_1 + 2^{\beta} v_1 + 2^{\gamma} w_1 \equiv 1 \pmod{2}$$

and

$$\alpha + \beta + \gamma = 3.$$

Hence $\alpha = 0$ and $\beta + \gamma = 3$. Thus $\beta = 1$ and $\gamma = 2$, giving

$$uv + vw + uw = 2u_1v_1 + 8v_1w_1 + 4u_1w_1 \equiv 2 \pmod{4}.$$

(ii): Suppose that u, v, w are not all even. Then, as $u + v + w \equiv 0 \pmod{2}$, exactly two of them are odd and one is even. Assuming without loss of generality that w is even, then $uv + vw + uw \equiv uv \equiv 1 \pmod{2}$, a contradiction. Thus u, v, w are all even, so there are integers u_1, v_1, w_1 such that $u = 2u_1$, $v = 2v_1$, $w = 2w_1$. The congruence $u + v + w \equiv 0 \pmod{4}$ then yields $u_1 + v_1 + w_1 \equiv 0 \pmod{2}$. Clearly, u_1, v_1, w_1 are not all odd, so at least one of them is even, say u_1. Then $u \equiv 0 \pmod{4}$ and $uvw \equiv 0 \pmod{16}$.

(iii): By (ii) we have $u \equiv v \equiv w \equiv 0 \pmod{2}$ and, without loss of generality, we have $u \equiv 0 \pmod{4}$. Then $v + w \equiv 0 \pmod{4}$ and $vw \equiv 0 \pmod{8}$. Hence $v \equiv w \equiv 0 \pmod{4}$.

(iv): By (ii) we have $u \equiv v \equiv w \equiv 0 \pmod{2}$ and, without loss of generality, we have

$u \equiv 0 \pmod 4$. Set $u = 4u_1$, $v = 2v_1$, and $w = 2w_1$, so that

$$2u_1 + v_1 + w_1 \equiv 2 \pmod 4,$$
$$2u_1v_1 + v_1w_1 + 2u_1w_1 \equiv 1 \pmod 4.$$

Clearly we have $v_1 \equiv w_1 \equiv 1 \pmod 2$, say $v_1 = 2v_2 + 1$ and $w_1 = 2w_2 + 1$. Using this in the first congruence above we get

$$2u_1 + 2v_2 + 2w_2 + 2 \equiv 2 \pmod 4 \;\Rightarrow\; 2u_1 \equiv 2v_2 + 2w_2 \pmod 4.$$

From the second congruence we then deduce the following:

$$\begin{aligned}
&2u_1v_1 + v_1w_1 + 2u_1w_1 \equiv 1 \pmod 4\\
&\;\Rightarrow\; 2u_1(v_1 + w_1) + 4v_2w_2 + 2v_2 + 2w_2 + 1 \equiv 1 \pmod 4\\
&\;\Rightarrow\; 2u_1(v_1 + w_1) + 2u_1 \equiv 0 \pmod 4\\
&\;\Rightarrow\; 2u_1(v_1 + w_1 + 1) \equiv 0 \pmod 4.
\end{aligned}$$

Since $v_1 + w_1 + 1$ is odd, we must have $u_1 \equiv 0 \pmod 2$. Then from the second congruence we quickly see that $v_1 \equiv w_1 \pmod 4$. Thus $u \equiv 0 \pmod 8$ and $v \equiv w \pmod 8$. Since $u + v + w \equiv v + w \equiv 4 \pmod 8$, we have that $v \equiv w \equiv 2 \pmod 4$.

(v): By (ii) we have $u \equiv v \equiv w \equiv 0 \pmod 2$ and, without loss of generality, $u \equiv 0 \pmod 4$. Set $u = 4u_1$, $v = 2v_1$ and $w = 2w_1$ so that

$$2u_1 + v_1 + w_1 \equiv 2 \pmod 4,$$
$$2u_1v_1 + v_1w_1 + 2u_1w_1 \equiv 3 \pmod 4.$$

Hence $v_1 \equiv w_1 \equiv 1 \pmod 2$, say $v_1 = 2v_2 + 1$ and $w_1 = 2w_2 + 1$. We then have that

$u_1 \equiv v_2 + w_2 \equiv 1 \pmod 2$. Without loss of generality, $v_2 \equiv 0 \pmod 2$ and $w_2 \equiv 1 \pmod 2$. Thus $u \equiv 4 \pmod 8$, $v \equiv 2 \pmod 8$ and $w \equiv 6 \pmod 8$.

(vi): By (ii) we have $u \equiv v \equiv w \equiv 0 \pmod 2$ and, without loss of generality, we have $w \equiv 0 \pmod 4$. Set $u = 2u_1$, $v = 2v_1$ and $w = 4w_1$. Then

$$u_1 + v_1 + 2w_1 \equiv 0 \pmod 4,$$
$$u_1 v_1 \equiv 1 \pmod 2,$$
$$u_1 v_1 w_1 \equiv 0 \pmod 4,$$

hence

$$u_1 \equiv v_1 \equiv 1 \pmod 2,\ w_1 \equiv 0 \pmod 4,\ u_1 + v_1 \equiv 0 \pmod 4.$$

Thus

$$u \equiv v \equiv 2 \pmod 4,\ w \equiv 0 \pmod{16},\ u + v \equiv 0 \pmod 8.$$

(vii): By (ii) we have $u \equiv v \equiv w \equiv 0 \pmod 2$ and, without loss of generality, we have $w \equiv 0 \pmod 4$. Set $u = 2u_1$, $v = 2v_1$ and $w = 4w_1$. Then

$$u_1 + v_1 + 2w_1 \equiv 0 \pmod 4,$$
$$u_1 v_1 w_1 \equiv 1 \pmod 4.$$

Hence $u_1 \equiv v_1 \equiv w_1 \equiv 1 \pmod 2$ and $w_1 \equiv u_1 v_1 \pmod 4$. Thus

$$u_1 + v_1 \equiv 2 \pmod 4,$$

so

$$u_1 \equiv v_1 \pmod 4, \; w_1 \equiv u_1^2 \equiv 1 \pmod 4.$$

Then

$$u \equiv v \equiv 2 \pmod 4, \; w \equiv 4 \pmod{16}, \; u \equiv v \pmod 8.$$

(viii): By (ii) we have that $u \equiv v \equiv w \equiv 0 \pmod 2$. Therefore, there are only two possibilities for u, v and w modulo 4 (up to permutation of u, v and w):

$$(u, v, w) \equiv (2, 2, 2) \text{ or } (2, 0, 0) \pmod 4.$$

Note, if $(u, v, w) \equiv (2, 0, 0) \pmod 4$, then we see that $8 \mid uv + vw + uw$, contradicting $uv + vw + uw \equiv 12 \pmod{16}$. Thus $u, v, w \equiv 2 \pmod 4$. □

Lemma 4.1. $B \equiv 0 \pmod 2$.

Proof: Suppose $B \equiv 1 \pmod 2$. Then, by (4.6), we have

$$r - A \equiv s - A \equiv t - A \equiv 1 \pmod 2.$$

Hence, $(r - A) + (s - A) + (t - A) \equiv 1 \pmod 2$, contradicting (4.4). Therefore, we must have that $B \equiv 0 \pmod 2$. □

Lemma 4.2. If $A \equiv 1 \pmod 2$ and $B \equiv 0 \pmod 4$ then $C \not\equiv 2 \pmod 4$.

Proof: In this case it is easier to use (4.1)-(4.3) rather than (4.4)-(4.6). Suppose that $A \equiv 1 \pmod 2$ and $B \equiv 0 \pmod 4$. If $C \equiv 2 \pmod 4$ then (4.1) and (4.3) yield $r + s + t \equiv 1 \pmod 2$ and $rst \equiv 8 \pmod{16}$, respectively. Hence, by Proposition 4.1(i), we have $rs + st + rt \equiv 2 \pmod 4$. This contradicts (4.2), thus $C \not\equiv 2 \pmod 4$. □

Lemma 4.3. If $A \equiv 0 \pmod 2$ then $B \equiv 0 \pmod 4$.

Proof: By (4.4) and (4.5) we have $(r-A)+(s-A)+(t-A) \equiv 0 \pmod 4$ and $(r-A)(s-A)+(s-A)(t-A)+(r-A)(t-A) \equiv 0 \pmod 4$. Then, by Proposition 4.1(ii), we have $(r-A)(s-A)(t-A) \equiv 0 \pmod{16}$. Hence, by (4.6), $B^2 \equiv 0 \pmod{16}$, thus $B \equiv 0 \pmod 4$. □

Lemma 4.4. If $A \equiv 2 \pmod 4$ then $B \equiv 0 \pmod 4$ and $C \not\equiv 3 \pmod 4$. Moreover,

$$B \equiv \begin{cases} 0 \pmod 8, & \text{if } C \equiv 0, 1 \pmod 4, \\ 4 \pmod 8, & \text{if } C \equiv 2 \pmod 4. \end{cases}$$

Proof: If $A \equiv 2 \pmod 4$ then $A = 4k+2$ for some integer k. We then have that $A^2 = 16k^2+16k+4$, so $A^2 \equiv 4 \pmod{16}$ and $A^2 - 4C \equiv 4 - 4C \equiv 4(1-C) \pmod{16}$. From (4.4) and (4.5), we obtain

$$(r-A)+(s-A)+(t-A) = -2A \equiv 4 \pmod 8$$

and

$$\begin{aligned}(r-A)(s-A)+(s-A)(t-A)+(r-A)(t-A) &= A^2 - 4C \\ &\equiv 4(1-C) \pmod{16}.\end{aligned}$$

Hence, by Proposition 4.1(ii), we have

$$(r-A)(s-A)(t-A) \equiv 0 \pmod{16}.$$

Appealing to (4.6), we obtain $B^2 \equiv 0 \pmod{16}$, so $B \equiv 0 \pmod 4$ as asserted.

Suppose $C \equiv 3 \pmod 4$. Then, from the above, we have

$$(r-A)+(s-A)+(t-A) \equiv 4 \pmod 8$$

and

$$(r-A)(s-A)+(s-A)(t-A)+(r-A)(t-A) \equiv 8 \pmod{16}.$$

Therefore, by Proposition 4.1(iii), we obtain

$$(r-A)(s-A)+(s-A)(t-A)+(r-A)(t-A) \equiv 0 \pmod{16},$$

a contradiction. Hence $C \not\equiv 3 \pmod 4$ as claimed.

If $C \equiv 0 \pmod 4$, then

$$(r-A)+(s-A)+(t-A) \equiv 4 \pmod 8$$

and

$$(r-A)(s-A)+(s-A)(t-A)+(r-A)(t-A) \equiv 4 \pmod{16}.$$

Thus, by (4.6) and Proposition 4.1(iv), we have

$$B^2 = (r-A)(s-A)(t-A) \equiv 0 \pmod{32}.$$

Hence $2v_2(B) = v_2(B^2) \geq 5$, so $v_2(B) \geq 3$. Therefore, $B \equiv 0 \pmod 8$.

If $C \equiv 1 \pmod 4$ then

$$(r-A)+(s-A)+(t-A) \equiv 4 \pmod 8$$

and

$$(r-A)(s-A)+(s-A)(t-A)+(r-A)(t-A) \equiv 0 \pmod{16}.$$

By (4.6) and Proposition 4.1(iii), we then have

$$B^2 = (r-A)(s-A)(t-A) \equiv 0 \pmod{64},$$

so $B \equiv 0 \pmod 8$.

If $C \equiv 2 \pmod 4$, then

$$(r-A)+(s-A)+(t-A) \equiv 4 \pmod 8$$

and

$$(r-A)(s-A)+(s-A)(t-A)+(r-A)(t-A) \equiv 12 \pmod{16}.$$

Thus, by (4.6) and Proposition 4.1(v), we have

$$B^2 = (r-A)(s-A)(t-A) \equiv 16 \pmod{32}.$$

Therefore, $2v_2(B) = v_2(B^2) = 4$, so $v_2(B) = 2$ and $B \equiv 4 \pmod 8$. □

Lemma 4.5. If $A \equiv 4 \pmod 8$ and $B \equiv 4 \pmod 8$ then $C \equiv 3 \pmod 4$.

Proof: By (4.4)-(4.6), we have

$$(r-A)+(s-A)+(t-A) \equiv 8 \pmod{16},$$

$$(r-A)(s-A)+(s-A)(t-A)+(r-A)(t-A) \equiv -4C \pmod{16},$$

$$(r-A)(s-A)(t-A) \equiv 16 \pmod{64}.$$

Appealing to Proposition 4.1(vii), we obtain

$$(r-A)(s-A)+(s-A)(t-A)+(r-A)(t-A) \equiv 4 \pmod{16}.$$

Hence $-4C \equiv 4 \pmod{16}$, so $C \equiv 3 \pmod 4$. □

Lemma 4.6. If $A \equiv 4 \pmod 8$, $B \equiv 0 \pmod 8$ and $C \equiv 1 \pmod 2$ then $C \equiv 1 \pmod 4$.

Proof: From (4.4)-(4.6) we have

$$(r-A)+(s-A)+(t-A) \equiv 8 \pmod{16},$$

$$(r-A)(s-A)+(s-A)(t-A)+(r-A)(t-A) \equiv -4C \pmod{16},$$

$$(r-A)(s-A)(t-A) \equiv 0 \pmod{64}.$$

As $C \equiv 1 \pmod 2$, we have $-4C \equiv 4 \pmod 8$. By Proposition 4.1(vi), we obtain

$$(r-A)(s-A)+(s-A)(t-A)+(r-A)(t-A) \equiv 12 \pmod{16}.$$

Hence $-4C \equiv 12 \pmod{16}$, so $C \equiv 1 \pmod 4$. □

Lemma 4.7. If $A \equiv 4 \pmod 8$, $B \equiv 0 \pmod 8$ and $C \equiv 0 \pmod 8$ then $B \equiv 0 \pmod{16}$ and $C \equiv 4 \pmod 8$.

Proof: By (4.4) and (4.5) we have

$$(r-A)+(s-A)+(t-A) \equiv 0 \pmod 8,$$
$$(r-A)(s-A)+(s-A)(t-A)+(r-A)(t-A) \equiv 0 \pmod 8.$$

Hence, by Proposition 4.1(iii), we deduce

$$r-A \equiv s-A \equiv t-A \equiv 0 \pmod 4.$$

Define integers x, y, z by

$$r-A = 4x, \ s-A = 4y, \ t-A = 4z.$$

Then (4.4)-(4.6) become

$$\begin{aligned} &x+y+z = \frac{-A}{2}, \\ &xy+yz+xz = \left(\frac{A}{4}\right)^2 - \frac{C}{4}, \\ &xyz = \left(\frac{B}{8}\right)^2, \end{aligned}$$

proving $C \equiv 0 \pmod 4$. As $\frac{A}{2}$ is even, at least one of x, y, z is even. Without loss of generality we may suppose that $x \equiv 0 \pmod 2$, say $x = 2x_1$, $x_1 \in \mathbb{Z}$. Then

$$\begin{aligned} &2x_1 + y + z = \frac{-A}{2}, \\ &2x_1(y+z) + yz = \left(\frac{A}{4}\right)^2 - \frac{C}{4}, \\ &2x_1yz = \left(\frac{B}{8}\right)^2. \end{aligned}$$

Hence $\frac{B^2}{128} = x_1yz$, so $256|B^2$ since $v_2(B^2)$ is even. Thus $B \equiv 0 \pmod{16}$ as asserted.

Define A_1, B_1, C_1 by $A = 8A_1 + 4$, $B = 16B_1$, $C = 4C_1$, so

$$2x_1 + y + z = -4A_1 - 2,$$
$$2x_1(y + z) + yz = 4A_1^2 + 4A_1 + 1 - C_1,$$
$$x_1yz = 2B_1^2.$$

Clearly $y \equiv z \pmod 2$. If $y \equiv z \equiv 1 \pmod 2$, then $x_1 \equiv 0 \pmod 2$, so

$$y + z \equiv 2 \pmod 4,$$
$$yz \equiv 1 - C_1 \pmod 4.$$

Thus

$$1 - C_1 \equiv yz \equiv y(2 - y) \equiv 2 - 1 \equiv 1 \pmod 4,$$

so $C_1 \equiv 0 \pmod 4$. Hence $C \equiv 0 \pmod{16}$, contradicting (1.6). Thus, we must have $y \equiv z \equiv 0 \pmod 2$. Then $C_1 \equiv 1 \pmod 4$, thus $C \equiv 4 \pmod{16}$. □

Lemma 4.8. If $A \equiv 0 \pmod 8$ and $B \equiv 4 \pmod 8$ then $C \equiv 3 \pmod 4$.

Proof: From (4.4) and (4.5) we have

$$(r - A) + (s - A) + (t - A) \equiv 0 \pmod{16},$$
$$(r - A)(s - A) + (s - A)(t - A) + (r - A)(t - A) \equiv 0 \pmod 4.$$

Hence, by Proposition 4.1(ii), after permutating of r, s and t, if necessary, the following:

$$r - A \equiv 0 \pmod 4,$$
$$s - A \equiv 0 \pmod 2,$$
$$t - A \equiv 0 \pmod 2.$$

Thus we can define integers x, y and z by

$$r - A = 4x, \ \ s - A = 2y, \ \ t - A = 2z.$$

Then (4.4)-(4.6) become

$$2x + y + z = -A,$$
$$2x(y + z) + yz = \left(\frac{A}{2}\right)^2 - C,$$
$$xyz = \left(\frac{B}{4}\right)^2.$$

As $\frac{B}{4} \equiv 1 \pmod 2$, we see that $x \equiv y \equiv z \equiv 1 \pmod 2$. Then, modulo 4, we have

$$2 + y + z \equiv 0 \pmod 4,$$
$$2x(y + z) + yz \equiv yz \equiv -C \pmod 4,$$
$$xyz \equiv 1 \pmod 4.$$

Thus

$$C \equiv -yz \equiv -y(2 - y) \equiv y^2 - 2y \equiv 1 - 2 \equiv 3 \pmod 4$$

as claimed. □

Lemma 4.9. If $A \equiv B \equiv 0 \pmod 8$ and $C \equiv 1 \pmod 2$ then $C \equiv 1 \pmod 4$.

Proof: By (4.4)-(4.6) we have

$$(r - A) + (s - A) + (t - A) \equiv 0 \pmod{16},$$
$$(r - A)(s - A) + (s - A)(t - A) + (r - A)(t - A) \equiv -4C \pmod{16},$$
$$(r - A)(s - A)(t - A) \equiv 0 \pmod{64}.$$

Appealing to Proposition 4.1(vi) we have

$$(r - A)(s - A) + (s - A)(t - A) + (r - A)(t - A) \equiv 12 \pmod{16}.$$

Hence $-4C \equiv 12 \pmod{16}$, so $C \equiv 1 \pmod{4}$. □

Lemma 4.10. If $A \equiv B \equiv 0 \pmod{8}$ and $C \equiv 0 \pmod{2}$ then $B \equiv 0 \pmod{16}$, $C \equiv 4 \pmod{16}$ and $B + C \equiv 4 \pmod{32}$.

Proof: By (4.4) and (4.5) we have

$$(r - A) + (s - A) + (t - A) \equiv 0 \pmod{16},$$
$$(r - A)(s - A) + (s - A)(t - A) + (r - A)(t - A) \equiv 0 \pmod{8}.$$

Hence, by Proposition 4.1(iii), we deduce that

$$r - A \equiv s - A \equiv t - A \equiv 0 \pmod{4}.$$

Thus there are integers x, y, z such that

$$r - A = 4x,\ s - A = 4y,\ t - A = 4z.$$

Then (4.4)-(4.6) become

$$x + y + z = \frac{-A}{2},$$
$$xy + yz + xz = \left(\frac{A}{4}\right)^2 - \frac{C}{4},$$
$$xyz = \left(\frac{B}{8}\right)^2,$$

proving that $C \equiv 0 \pmod 4$. As $\frac{A}{2}$ is even, at least one of x, y and z is even. Without loss of generality we may suppose that $x \equiv 0 \pmod 2$, say $x = 2x_1$ for some $x_1 \in \mathbb{Z}$. Then

$$2x_1 + y + z = \frac{-A}{2},$$
$$2x_1(y + z) + yz = \left(\frac{A}{4}\right) - \frac{C}{4},$$
$$2x_1 yz = \left(\frac{B}{8}\right)^2.$$

Hence $\frac{B}{8} \equiv 0 \pmod 2$, so $B \equiv 0 \pmod{16}$, as asserted. We define integers A_1, B_1, C_1 by $A = 8A_1$, $B = 16B_1$, $C = 4C_1$ so

$$2x_1 + y + z = -4A_1,$$
$$2x_1(y + z) + yz = 4A_1^2 - C_1,$$
$$x_1 yz = 2B_1^2.$$

Clearly $y \equiv z \pmod 2$. If $y \equiv z \equiv 0 \pmod 2$ then $C_1 \equiv 0 \pmod 4$, thus $C \equiv 0 \pmod{16}$, contradicting (1.6). Hence $y \equiv z \equiv 1 \pmod 2$, so we must have $x_1 \equiv 0 \pmod 2$. Therefore, $y + z \equiv 0 \pmod 4$ and $yz \equiv -C_1 \pmod 4$. Hence

$$C_1 \equiv -yz \equiv y^2 \equiv 1 \pmod 4,$$

so $C \equiv 4C_1 \equiv 4 \pmod{16}$, as asserted.

As $x_1 \equiv 0 \pmod 2$, we can define $x_2 \in \mathbb{Z}$ such that $x_1 = 2x_2$. Then

$$
\begin{aligned}
&4x_2 + y + z = -4A_1,\\
&4x_2(y+z) + yz = 4A_1^2 - C_1,\\
&x_2yz = B_1^2.
\end{aligned}
$$

As $y \equiv z \equiv 1 \pmod 2$ and $y + z \equiv 0 \pmod 4$, permuting y and z if necessary we have that $y \equiv 1 \pmod 4$ and $z \equiv 3 \pmod 4$. From this, we have

$$
\begin{aligned}
&(y-1)(z-1) \equiv 0 \pmod 8\\
&\ \Rightarrow\ yz - z - y + 1 \equiv 0 \pmod 8\\
&\ \Rightarrow\ yz \equiv yz + 1 \pmod 8.
\end{aligned}
$$

Therefore, we have

$$
\begin{aligned}
&4x_2 + yz + 1 \equiv 4A_1 \pmod 8,\\
&yz \equiv 4A_1^2 - C_1 \pmod 8,\\
&x_2 \equiv B_1 \pmod 2.
\end{aligned}
$$

Finally,

$$
\begin{aligned}
B + C = 16B_1 + 4C_1 &\equiv 16x_2 + (16A_1 - 4yz)\\
&\equiv 16x_2 + (16x_2 + 4yz + 4) - 4yz \equiv 4 \pmod{32}. \quad \square
\end{aligned}
$$

From Lemmas 4.1-4.10 we deduce that each triple (A, B, C) satisfying (1.3)-(1.6) and $AB(A^2 - 4C) \neq 0$ falls into one and only one of the thirteen cases listed in the table below. A flowchart outlining the deduction of this case breakdown using the lemmas in this section can be found in Appendix B. Appendix A contains examples of each case not considered to be invalid here, along with examples for all other main cases.

The rest of this section is devoted to a more detailed analysis of Case 6. This analysis justifies the breakdown of Case 6 into the nineteen subcases listed in table 1 of Appendix A. Recall that $a = v_2(A)$, $b = v_2(B)$, $c = v_2(C)$, $l = v_2(A^2 - 4C)$, and $E = \frac{A^2-4C}{2^l}$.

Lemma 4.11. Suppose that

$$A \equiv 2 \pmod 4,\ B \equiv 0 \pmod 8,\ C \equiv 1 \pmod 4.$$

Then

(i): $b \geq 3$,

(ii): $l \geq 4$,

(iii): if $l = 4$ then $b = 3$ and $A \equiv 2 \pmod 8$,

(iv): if $l \geq 5$ is odd and $b = l - 2$ then $l \geq 7$ and $A \equiv 6 \pmod 8$,

(v): if $l \geq 5$ is odd, $b < l - 3$ and b is odd then $b \geq 5$ and

$$\begin{cases} A \equiv 10 \pmod{16}, & \text{if } b = 5, \\ A \equiv 2 \pmod{16}, & \text{if } b \geq 7, \end{cases}$$

(vi): if $l \geq 6$ is even, $b \leq l-2$ and b is odd then $l \geq 8$, $b \geq 5$ and

$$\begin{cases} A \equiv 6 \pmod 8, & \text{if } b = l-2, \\ A \equiv 2 \pmod 8, & \text{if } b \leq l-3, \end{cases}$$

(vii): the possibility where $b = l-1$, l (even)≥ 6 cannot occur.

Proof: (i): As $B \equiv 0 \pmod 8$ we have $b \geq 3$.

(ii): As $A \equiv 2 \pmod 4$ we have $A^2 \equiv 4 \pmod{16}$. As $C \equiv 1 \pmod 4$ we have $4C \equiv 4 \pmod{16}$. Thus $A^2 - 4C \equiv 0 \pmod{16}$. But $2^l \| A^2 - 4C$ and $A^2 - 4C \neq 0$, hence $l \geq 4$.

(iii): Here $l = 4$ and we wish to show that $b = 3$ and $A \equiv 2 \pmod 8$. By part (i) we know that $b \geq 3$. By (4.4)-(4.6) the integers $r - A$, $s - A$ and $t - A$ satisfy

$$(r-A) + (s-A) + (t-A) = -2A = -4A_1 \equiv 4 \pmod 8, \tag{4.7}$$

$$(r-A)(s-A) + (s-A)(t-A) + (r-A)(t-A) = A^2 - 4C = 16E, \tag{4.8}$$

$$(r-A)(s-A)(t-A) = B^2 = 2^{2b}B_1^2 \equiv 0 \pmod{64}. \tag{4.9}$$

We deduce from (4.7) and (4.8), through Proposition 4.1 (iii), that

$$r - A \equiv s - A \equiv t - A \equiv 0 \pmod 4.$$

Thus we can define non-zero integers e, f and h by

$$r - A = 4e, \ s - A = 4f, \ t - A = 4h. \tag{4.10}$$

Then, from (4.7)-(4.10),we have

$$e + f + h = -A_1, \tag{4.11}$$

$$ef + fh + eh = E, \tag{4.12}$$

$$efh = 2^{2b-6}B_1^2. \tag{4.13}$$

From (4.11) and (4.12) we have

$$e + f + h \equiv 1 \pmod 2,$$

$$ef + fh + eh \equiv 1 \pmod 2,$$

so that

$$e \equiv f \equiv h \equiv 1 \pmod 2.$$

Then, from (4.13), we deduce

$$1 \equiv efh \equiv 2^{2b-6}B_1^2 \equiv 2^{2b-6} \pmod 2,$$

so $b = 3$ as claimed.

From here, (4.13) gives

$$efh = B_1^2 \equiv 1 \pmod 4$$

so $h \equiv ef \pmod 4$. Then, appealing to (4.11), we obtain

$$-A_1 \equiv e + f + ef \equiv (1 + e)(1 + f) - 1 \equiv -1 \pmod 4$$

so

$$A_1 \equiv 1 \pmod 4,\ A = 2A_1 \equiv 2 \pmod 8$$

as claimed.

(iv): Here $l \geq 5$ is odd and $b = l - 2$. We wish to prove that $l \geq 7$ and $A \equiv 6 \pmod 8$. With $l \geq 5$ we have that $A^2 - 4C \equiv 0 \pmod{32}$. By (4.4)-(4.6) the integers $r - A$, $s - A$ and $t - A$ satisfy

$$(r - A) + (s - A) + (t - A) = -2A = -4A_1 \equiv 4 \pmod 8, \tag{4.14}$$

$$(r - A)(s - A) + (s - A)(t - A) + (r - A)(t - A) \equiv 2^l E \equiv 0 \pmod{32}, \tag{4.15}$$

$$(r - A)(s - A)(t - A) = B^2 = 2^{2b} B_1^2 = 2^{2l-4} B_1^2. \tag{4.16}$$

By Proposition 4.1 (iii), we see from (4.14) and (4.15) that

$$r - A \equiv s - A \equiv t - A \equiv 0 \pmod 4.$$

Thus we can define non-zero integers e, f and h by

$$r - A = 4e,\ s - A = 4f,\ t - A = 4h.$$

Then (4.14)-(4.16) become

$$e + f + h = -A_1, \tag{4.17}$$

$$ef + fh + eh = 2^{l-4} E, \tag{4.18}$$

$$efh = 2^{2l-10} B_1^2. \tag{4.19}$$

We write

$$e = 2^u e_1,\ f = 2^v f_1,\ h = 2^w h_1, \tag{4.20}$$

where $u, v, w \in \mathbb{N}_0 = \mathbb{N}\cup\{0\}$ and $e_1, f_1, h_1 \in \mathbb{Z}$ are odd. By permuting e, f and h if necessary, we may suppose that $u \le v \le w$. From (4.17) and (4.20) we have

$$2^u + 2^v + 2^w \equiv 1 \pmod 2$$

so that $u = 0$. From (4.19) and (4.20) we deduce

$$2^{v+w} e_1 f_1 h_1 = 2^{2l-10} B_1^2$$

so

$$v + w = 2l - 10,\ e_1 f_1 h_1 \equiv 1 \pmod 4.$$

Hence

$$e = e_1 \equiv f_1 h_1 \pmod 4),\ f = 2^v f_1,\ h = 2^{2l-10-v} h_1, \tag{4.21}$$

so $0 \le v \le l - 5$. From (4.18) and (4.20) we deduce

$$2^v e_1 f_1 + 2^{2l-10} f_1 h_1 + 2^{2l-10-v} e_1 h_1 = 2^{l-4} E. \tag{4.22}$$

Suppose $l = 5$. Then $v = 0$ and (4.22) becomes

$$e_1 f_1 + f_1 h_1 + e_1 h_1 = 2E,$$

which is impossible as the left-hand side is odd and the right-hand side is even. Hence

$l > 5$. But l is odd, so $l \geq 7$ as claimed.

Suppose that $v \leq l - 6$. Then

$$l - 4 \leq 2l - 10 - v \leq 2l - 10$$

so that, by (4.22),

$$2^{l-4} \mid 2^{l-4}E - 2^{2l-10} f_1 h_1 - 2^{2l-10-v} e_1 h_1 = 2^v e_1 f_1.$$

But e_1 and f_1 are odd, so $l - 4 \leq v$. This contradicts $v \leq l - 6$. Thus $v > l - 6$. But $v \leq l - 5$, so $v = l - 5$. Then (4.22) yields

$$e_1(f_1 + h_1) + 2^{l-5} f_1 h_1 = 2E.$$

As $l \geq 7$ and $E \equiv 1 \pmod 2$, we deduce

$$e_1(f_1 + h_1) \equiv 2 \pmod 4.$$

As $e_1 \equiv 1 \pmod 2$ we see that $f_1 + h_1 \equiv 2 \pmod 4$. Then

$$f_1 h_1 \equiv f_1(2 - f_1) \equiv 2f_1 - f_1^2 \equiv 2 - 1 \equiv 1 \pmod 4.$$

Appealing to (4.21), we deduce that

$$e \equiv 1 \pmod 4, \ f = 2^{l-5} f_1 \equiv 0 \pmod 4, \ h = 2^{l-5} h_1 \equiv 0 \pmod 4,$$

so that $e + f + h \equiv 1 \pmod 4$. Then, by (4.17), we have $-A_1 \equiv 1 \pmod 4$, so $A \equiv 6 \pmod 8$.

(v): Here $l \geq 5$ odd, $b < l - 3$ and b is odd. By part (i), $b \geq 3$ so $l > b + 3 \geq 3 + 3 = 6$ and thus $l \geq 7$, so $A^2 - 4C \equiv 0 \pmod{128}$. By (4.4)-(4.6), the integers $r - A,\ s - A,\ t - A$ satisfy

$$(r - A) + (s - A) + (t - A) = -2A = -4A_1 \equiv 4 \pmod{8}, \tag{4.23}$$

$$(r - A)(s - A) + (s - A)(t - A) + (r - A)(t - A) = 2^l E \equiv 0 \pmod{128}, \tag{4.24}$$

$$(r - A)(s - A)(t - A) = B^2 = 2^{2b} B_1^2 \equiv 0 \pmod{64}. \tag{4.25}$$

Hence, by Proposition 4.1 (iii), we have

$$r - A \equiv s - A \equiv t - A \equiv 0 \pmod{4}.$$

Then we can define non-zero integers e, f, h by

$$r - A = 4e,\ s - A = 4f,\ t - A = 4h. \tag{4.26}$$

Then (4.23)-(4.26) give

$$e + f + h = -A_1 \equiv 1 \pmod{2}, \tag{4.27}$$

$$ef + fh + eh = 2^{l-4} E \equiv 0 \pmod{8}, \tag{4.28}$$

$$efh = 2^{2b-6} B_1^2. \tag{4.29}$$

We write

$$e = 2^u e_1,\ f = 2^v f_1,\ h = 2^w h_1, \tag{4.30}$$

where $u, v, w \in \mathbb{N}_0$ and $e_1, f_1, h_1 \in \mathbb{Z}$ are odd. By permuting e, f and h if necessary, we may suppose that $u \le v \le w$. By (4.27) we have

$$2^u + 2^v + 2^w \equiv 2^u(1 + 2^{v-u} + 2^{w-u}) \equiv 1 \pmod 2$$

so that $u = 0$. Then, from (4.29) and (4.30), we have

$$2^{v+w} e_1 f_1 h_1 = 2^{2b-6} B_1^2$$

so

$$v + w = 2b - 6, \ e_1 f_1 h_1 = B_1^2 \equiv 1 \pmod 8.$$

As $v \le w$, we deduce that $0 \le v \le b - 3$. Then, by (4.30), we have

$$e = e_1 \equiv f_1 h_1 \pmod 8, \ f = 2^v f_1, \ h = 2^{2b-6-v} h_1. \tag{4.31}$$

From (4.28) and (4.31) we deduce

$$2^v e_1 f_1 + 2^{2b-6} f_1 h_1 + 2^{2b-6-v} e_1 h_1 = 2^{l-4} E. \tag{4.32}$$

Suppose $b = 3$. Then $v = 0$. Thus (4.32) becomes

$$e_1 f_1 + f_1 h_1 + e_1 h_1 = 2^{l-4} E.$$

This is impossible as the left-hand side is odd and the right-hand side is even since $l \ge 7$. Thus $b > 3$. But b is odd, so $b \ge 5$ as asserted.

Suppose next that $v \le b - 4$. Then

$$2b - 6 - v > 0,\ 2b - 6 - 2v > 0,\ l - 4 - v > 0,$$

so (4.32) becomes

$$e_1 f_1 + 2^{2b-6-v} f_1 h_1 + 2^{2b-6-2v} e_1 h_1 = 2^{l-4-v} E.$$

This is impossible as the left-hand side is odd and the right-hand side is even. Hence $v > b - 4$. But $v \le b - 3$, so $v = b - 3$. Then (4.32) becomes

$$2^{b-3} e_1 f_1 + 2^{2b-6} f_1 h_1 + 2^{b-3} e_1 h_1 = 2^{l-4} E$$

so

$$e_1(f_1 + h_1) + 2^{b-3} f_1 h_1 = 2^{l-b-1} E.$$

Now $b - 3 \ge 2$ and $l - b - 1 \ge 3$ so that

$$\begin{cases} f_1 + h_1 \equiv 4 \pmod 8, & \text{if } b = 5, \\ f_1 + h_1 \equiv 0 \pmod 8, & \text{if } b \ge 7. \end{cases}$$

Hence

$$e = e_1 \equiv f_1 h_1 \equiv \begin{cases} f_1(4 - f_1) = 4f_1 - f_1^2 \equiv 4 - 1 \equiv 3 \pmod 8, & \text{if } b = 5, \\ -f_1^2 \equiv -1 \equiv 7 \pmod 8, & \text{if } b \ge 7. \end{cases}$$

Finally, by (4.27) and (4.31), as $v = b - 3$, $b \geq 5$ and $f \equiv h \equiv 1 \pmod 2$, we have

$$\begin{aligned} A_1 &= -e - f - h \\ &= -e_1 - 2^{b-3} f_1 - 2^{b-3} h_1 \\ &\equiv -e_1 \pmod 8 \\ &\equiv \begin{cases} 5 \pmod 8, & \text{if } b = 5, \\ 1 \pmod 8, & \text{if } b \geq 7, \end{cases} \end{aligned}$$

so

$$A = 2A_1 \equiv \begin{cases} 10 \pmod{16}, & \text{if } b = 5, \\ 2 \pmod{16}, & \text{if } b \geq 7, \end{cases}$$

as claimed.

(vi): Here $l \geq 6$ is even, so $A^2 - 4C \equiv 0 \pmod{64}$. We also have that $b \leq l - 2$ and b is odd. We wish to prove that $l \geq 8$, $b \geq 5$, and

$$\begin{cases} A \equiv 6 \pmod 8, & \text{if } b = l - 2, \\ A \equiv 2 \pmod 8, & \text{if } b \leq l - 3. \end{cases}$$

By (4.4)-(4.6), the integers $r - A$, $s - A$, $t - A$ satisfy

$$(r - A) + (s - A) + (t - A) = -2A = -4A_1 \equiv 4 \pmod 8, \tag{4.33}$$

$$\begin{aligned} (r - A)(s - A) + (r - A)(t - A) + (s - A)(t - A) &= A^2 - 4C \\ &= 2^l E \equiv 0 \pmod{64}, \end{aligned} \tag{4.34}$$

$$(r - A)(s - A)(t - A) = B^2 = 2^{2b} B_1^2 \equiv 0 \pmod{64}. \tag{4.35}$$

By Proposition 4.1 (iii), we see from (4.33) and (4.34) that

$$r - A \equiv s - A \equiv t - A \equiv 0 \pmod 4.$$

Hence, we can define non-zero integers e, f and h by

$$r - A = 4e,\ s - A = 4f,\ t - A = 4h. \tag{4.36}$$

Thus (4.33)-(4.35) become

$$e + f + h = -A_1 \equiv 1 \pmod 2, \tag{4.37}$$

$$ef + fh + eh = 2^{l-4}E \equiv 0 \pmod 4, \tag{4.38}$$

$$efh = 2^{2b-6}B_1^2. \tag{4.39}$$

We write

$$e = 2^u e_1,\ f = 2^v f_1,\ h = 2^w h_1, \tag{4.40}$$

where $u, v, w \in \mathbb{N}_0$ and $e_1, f_1, h_1 \in \mathbb{Z}$ are odd. By permuting e, f, and h if necessary, we may suppose that $u \leq v \leq w$. From (4.37) and (4.40), we obtain

$$2^u + 2^v + 2^w \equiv 1 \pmod 2$$

so that $u = 0$. Then, from (4.39) and (4.40), we obtain

$$2^{v+w} e_1 f_1 h_1 = 2^{2b-6} B_1^2,$$

so that

$$v + w = 2b - 6,$$
$$e_1 f_1 h_1 = B_1^2 \equiv 1 \pmod{8}.$$

As $v \le w$, we have $v \le b - 3$. Thus (4.40) becomes

$$e = e_1 \equiv f_1 h_1 \pmod{8},$$
$$f = 2^v f_1,$$
$$h = 2^{2b-6-v} h_1,$$

where $0 \le v \le b - 3$.

Suppose $l = 6$. Then $b \le 4$. But b is odd, so $b \le 3$. By part (i) we have $b \ge 3$, so $b = 3$. Thus $v = 0$. Then

$$e = e_1 \equiv f_1 h_1 \pmod{8}$$
$$f = f_1,$$
$$h = h_1,$$

and (4.38) gives

$$e_1 f_1 + f_1 h_1 + e_1 h_1 = 2^{l-4} E = 4E,$$

which is impossible as the left-hand side is odd. Thus $l > 6$. But l is even, so $l \ge 8$ as claimed.

Suppose next that $v \le b - 4$. From (4.38) and (4.40), we have

$$2^v e_1 f_1 + 2^{2b-6} f_1 h_1 + 2^{2b-6-v} e_1 h_1 = 2^{l-4} E.$$

As

$$v < 2b - 6,\ v < 2b - 6 - v,\ v < l - 4,$$

we deduce that

$$e_1 f_1 + 2^{2b-6-v} f_1 h_1 + 2^{2b-6-2v} e_1 h_1 = 2^{l-4-v} E.$$

This is impossible as the left-hand side is odd and the right-hand side is even. Hence $v > b - 4$. But $v \le b - 3$, so $v = b - 3$. Then

$$e = e_1 \equiv f_1 h_1 \pmod 8),\ f = 2^{b-3} f_1,\ h = 2^{b-3} h_1,$$

and (4.38) becomes

$$2^{b-3} e_1 f_1 + 2^{2b-6} f_1 h_1 + 2^{2b-3} e_1 h_1 = 2^{l-4} E,$$

thus

$$e_1(f_1 + h_1) + 2^{b-3} f_1 h_1 = 2^{l-b-1} E.$$

If $b = 3$ then

$$e_1 f_1 + f_1 h_1 + e_1 h_1 = 2^{l-4} E.$$

This is impossible as the left-hand side is odd and the right-hand side is congruent to 0 modulo 16 since $l \ge 8$. Hence $b > 3$. But b is odd, so $b \ge 5$, as claimed. Then $b - 3 \ge 2$

and

$$e_1(f_1 + h_1) \equiv 2^{l-b-1}E \pmod 4.$$

If $l - b = 2$ then

$$e_1(f_1 + h_1) \equiv 2 \pmod 4$$

so

$$f_1 + h_1 \equiv 2 \pmod 4.$$

Hence

$$e \equiv f_1 h_1 \equiv f_1(2 - f_1) \equiv 2f_1 - f_1^2 \equiv 2 - 1 \equiv 1 \pmod 4,$$
$$f = 2^{b-3} f_1 \equiv 0 \pmod 4,$$
$$h = 2^{b-3} h_1 \equiv 0 \pmod 4,$$

so by (4.37), we have

$$-A_1 = e + f + h \equiv 1 \pmod 4.$$

Thus $A_1 \equiv 3 \pmod 4$ and

$$A = 2A_1 \equiv 6 \pmod 8.$$

If $l - b \geq 3$, then

$$e_1(f_1 + h_1) \equiv 0 \pmod 4$$

so

$$f_1 + h_1 \equiv 0 \pmod 4.$$

Hence

$$e \equiv f_1 h_1 \equiv -f_1^2 \equiv -1 \pmod 4,$$

$$f = 2^{b-3} f_1 \equiv 0 \pmod 4,$$

$$h = 2^{b-3} h_1 \equiv 0 \pmod 4,$$

so

$$-A_1 = e + f + h \equiv -1 \pmod 4$$

and thus $A_1 \equiv 1 \pmod 4$, so $A = 2A_1 \equiv 2 \pmod 8$.

(vii): By (4.4)-(4.6), the integers $r - A$, $s - A$ and $t - A$ satisfy

$$(r - A) + (s - A) + (t - A) = -2A = -4A_1 \equiv 4 \pmod 8, \tag{4.41}$$

$$(r - A)(s - A) + (s - A)(t - A) + (r - A)(t - A) = 2^l E \equiv 0 \pmod{64}, \tag{4.42}$$

$$(r - A)(s - A)(t - A) \equiv 0 \pmod{1024}. \tag{4.43}$$

Hence by Proposition 4.1 (iii), we have

$$r - A \equiv s - A \equiv t - A \equiv 0 \pmod 4.$$

Then we can define integers e, f and h by

$$r - A = 4e, \ s - A = 4f, \ t - A = 4h. \tag{4.44}$$

Thus, (4.41)-(4.43) become

$$e + f + h = -A_1 \equiv 1 \pmod 2, \tag{4.45}$$

$$ef + fh + eh = 2^{l-4}E \equiv 0 \pmod 4, \tag{4.46}$$

$$efh = 2^{2b-6}B_1^2 \equiv 0 \pmod{16}. \tag{4.47}$$

By (4.45), permuting e, f and h if necessary, we have that e is odd. Therefore, from (4.47) we have that $fh \equiv 0 \pmod{16}$, and in view of (4.46) we deduce that $e(f + h) \equiv 0 \pmod 4$, so $f + h \equiv 0 \pmod 4$. As $fh \equiv 0 \pmod{16}$, we conclude that $f \equiv h \equiv 0 \pmod 4$. We write

$$f = 2^v f_1, \ h = 2^w h_1, \tag{4.48}$$

where $v, w \in \mathbb{N}_0$ and $f_1, h_1 \in \mathbb{Z}$ are odd. By interchanging f and h, if necessary, we may suppose that $v \leq w$. We also have that $f \equiv h \equiv 0 \pmod 4$, so $2 \leq v \leq w$. From (4.47) and (4.48), we obtain

$$2^{v+w} e f_1 h_1 = 2^{2b-6} B_1^2,$$

so that

$$v + w = 2b - 6.$$

As $v \leq w$, we have $v \leq b - 3$ and we may write $w = 2b - 6 - v$. If $l = 6$, then $b = 5$ and

$v + w = 2b - 6 = 4$ yields $v = 2$ and $w = 2$. From (4.46), we then have

$$e(f + h) \equiv 4E - fh \equiv 4E \equiv 4 \pmod 8,$$

thus $e(f_1 + h_1) \equiv 1 \pmod 2$, which is impossible as $f_1 + h_1$ is even. Therefore, $l > 6$, so $l \geq 8$ as l is even. If $v \leq b - 4 = l - 5$, then dividing (4.46) by 2^v yields

$$ef_1 + 2^{2b-6-v} f_1 h_1 + 2^{2b-6-2v} eh_1 = 2^{l-4-v} E \equiv 0 \pmod 2,$$

a contradiction as the left-hand side of the congruence is odd. Therefore, we must have that $v = b - 3$, so $w = b - 3$ as well. However, in examining (4.46) again, we see that

$$\begin{aligned} b - 3 = l - 4 &= v_2(2^{l-4}E) \\ &= v_2(ef + fh + eh) = v_2(e(f + h) + fh) \\ &= v_2(e(f + h)) = v_2(f + h) \geq b - 3 + 1 \\ &= b - 2, \end{aligned}$$

a contradiction. Therefore, the possibility where $b = l - 1$, l (even)≥ 6 cannot occur.

Chapter 5

Main Case 1: The 2-parts of the conductor and the discriminant

Let $r, s, t \in \mathbb{Z}$ be the roots of the resolvent cubic $x^3 - Ax^2 - 4Cx + (4AC - B^2)$, and $r_1 x^2 = r - A$, $s_1 y^2 = s - A$, $t_1 z^2 = t - A$, where r_1, s_1, t_1 are square-free integers and x, y, and z are non-negative integers. Recall the following equations:

$$r + s + t = A \tag{5.1}$$

$$rs + st + rt = -4C, \tag{5.2}$$

$$rst = B^2 - 4AC, \tag{5.3}$$

$$(r - A) + (s - A) + (t - A) = -2A, \tag{5.4}$$

$$(r - A)(s - A) + (s - A)(t - A) + (r - A)(t - A) = A^2 - 4C, \tag{5.5}$$

$$(r - A)(s - A)(t - A) = B^2, \tag{5.6}$$

$$r_1 s_1 t_1 = \left(\frac{B}{xyz}\right)^2, \tag{5.7}$$

$$v_p(r - A) + v_p(s - A) + v_p(t - A) \equiv 0 \pmod 2 \text{ for any prime } p, \tag{5.8}$$

In determining the 2-part of the conductor $f(K)$ and of the discriminant $d(K)$, we recall Corollaries 2.1 and 2.2:

Corollary 2.1. When $B \neq 0$, let $r - A = r_1 x^2$, $s - A = s_1 y^2$, $t - A = t_1 z^2$ where r_1, s_1 and t_1 are square-free integers and x, y and z are non-negative integers. Then, up to a permutation of r, s and t, exactly one of the following must be true:

(a) $r_1 \equiv s_1 \equiv t_1 \equiv 1 \pmod 4$,

(b) $r_1 \equiv s_1 \equiv 3 \pmod 4$, $t_1 \equiv 1 \pmod 4$,

(c) $r_1 \equiv s_1 \equiv 2$ or $6 \pmod 8$, $t_1 \equiv 1 \pmod 4$,

(d) $r_1 \equiv 2 \pmod 8$, $s_1 \equiv 6 \pmod 8$, $t_1 \equiv 3 \pmod 4$.

Corollary 2.2. Let $r - A = r_1 x^2$, $s - A = s_1 y^2$, $t - A = t_1 z^2$ where r_1, s_1 and t_1 are square-free integers and x, y and z are non-negative integers. When $B \neq 0$, let $r - A = r_1 x^2$, $s - A = s_1 y^2$ and $t - A = t_1 z^2$ where r_1, s_1 and t_1 are square-free integers and x, y and z are non-negative integers. Then, up to a permutation of r, s and t, we have

(A) If $r_1 s_1 t_1 \equiv 0 \pmod 2$, then $\alpha = 3$. Furthermore, if we have $r_1 \equiv 1 \pmod 4$ or $s_1 \equiv t_1 \equiv 2$ or $6 \pmod 8$, then $\beta = 6$; otherwise, $r_1 \equiv 3 \pmod 4$, $(s_1, t_1) \equiv (2, 6) \pmod 8$ and $\beta = 8$.

(B) If all of r_1, s_1 or t_1 are odd and at most one of r_1, s_1 or t_1 is congruent to 1 modulo 4, then $\alpha = 2$.

(C) If $r_1 \equiv s_1 \equiv t_1 \equiv 1 \pmod 4$, then $\alpha = 0$.

Whenever $\alpha \neq 3$, we have from Theorem 1.2 that $\beta = 2\alpha$; we need only perform extra computations to determine β when $\alpha = 3$.

5.1 Cases 1-5

Whenever A is odd, we have that exactly one of r, s and t is odd because of (5.1) and (5.2); without loss of generality, we will always take this to be r.

Case 1: $A \equiv 1$ (**mod** 2), $B \equiv 2$ (**mod** 4), $C \equiv 1$ (**mod** 2)

As $B \equiv 2 \pmod 4$, we have $B^2 \equiv 4 \pmod 8$. As $A \equiv C \equiv 1 \pmod 2$, we have $4AC \equiv 4 \pmod 8$. Hence, by (5.3),

$$rst = B^2 - 4AC \equiv 0 \pmod 8,$$

so as r is odd we deduce that $st \equiv 0 \pmod 8$. By (5.2) we have $r(s+t) \equiv 4 \pmod 8$, hence $s + t \equiv 4 \pmod 8$. Therefore, $(s,t) \equiv (0,4)$ or $(4,0) \pmod 8$, thus $s \equiv t \equiv 0 \pmod 4$.

If $A \equiv 1 \pmod 4$, then $(s - A, t - A) \equiv (3,3) \pmod 4$, thus $\alpha = 2$. If $A \equiv 3 \pmod 4$, then $(s - A, t - A) \equiv (1,1) \pmod 4$, thus $\alpha = 0$.

Case 2: $A \equiv 1$ (**mod** 2), $B \equiv 2$ (**mod** 4), $C \equiv 0$ (**mod** 2)

Here $B^2 \equiv 4 \pmod 8$ and $4AC \equiv 0 \pmod 8$, so from (5.3) we have

$$rst = B^2 - 4AC \equiv 4 - 0 \equiv 4 \pmod 8,$$

so that $st \equiv 4 \pmod 8$. As $r \equiv A \equiv 1 \pmod 2$, we have from (5.1) that $s + t \equiv 0 \pmod 2$. Thus $(s,t) \equiv (2,2) \pmod 4$. If $A \equiv 1 \pmod 4$, then $(s - A, t - A) \equiv (1,1) \pmod 4$, thus $\alpha = 0$. If $A \equiv 3 \pmod 4$ then $(s - A, t - A) \equiv (3,3) \pmod 4$ and thus $\alpha = 2$.

Case 3: $A \equiv 1$ (**mod** 2), $B \equiv 0$ (**mod** 4), $C \equiv 1$ (**mod** 2)

Here we have $B^2 \equiv 0 \pmod{16}$ and $4AC \equiv 4 \pmod 8$, so from (5.3) we have

$$rst = B^2 - 4AC \equiv 4 \pmod 8$$

so that $st \equiv 4 \pmod 8$. By (5.1) we have $s + t \equiv 0 \pmod 2$, so $(s, t) \equiv (2, 2) \pmod 4$. If $A \equiv 1 \pmod 4$, then we have $s - A \equiv t - A \equiv 1 \pmod 4$, thus $\alpha = 0$. If $A \equiv 3 \pmod 4$, then we have $s - A \equiv t - A \equiv 3 \pmod 4$ and thus $\alpha = 2$.

Case 4: $A \equiv 1$ (**mod** 2), $B \equiv 0$ (**mod** 4), $C \equiv 0$ (**mod** 4)

Here we have $B^2 \equiv 0 \pmod{16}$ and $4AC \equiv 0 \pmod{16}$, so from (5.3) we have

$$rst = B^2 - 4AC \equiv 0 \pmod{16},$$

hence $st \equiv 0 \pmod{16}$. From (5.2) we have $r(s+t) \equiv 0 \pmod{16}$, thus $s+t \equiv 0 \pmod{16}$ as r is odd. Examining this congruence modulo 4, as $16 \mid st$ we must have $(s, t) \equiv (0, 0) \pmod 4$. If $A \equiv 1 \pmod 4$, then $(s - A, t - A) \equiv (3, 3) \pmod 4$, thus $\alpha = 2$. If $A \equiv 3 \pmod 4$ then $(s - A, t - A) \equiv (1, 1) \pmod 4$ and thus $\alpha = 0$.

Case 5: $A \equiv 2$ (**mod** 4), $B \equiv 4$ (**mod** 8), $C \equiv 2$ (**mod** 4)

From (5.1) and (5.2), as A and $-4C$ are both even, we have that r, s and t must all be even. Examining (5.1) and (5.3), we have that $r + s + t \equiv 2 \pmod 4$ and $rst = B^2 - 4AC \equiv 0 \pmod{32}$. Thus

$$\frac{r}{2} + \frac{s}{2} + \frac{t}{2} \equiv 1 \pmod 2, \quad \frac{r}{2} \cdot \frac{s}{2} \cdot \frac{t}{2} \equiv 0 \pmod 4.$$

Hence, up to a permutation of r, s and t, we have $\frac{r}{2} \equiv \frac{s}{2} \equiv 0 \pmod 2$ and $\frac{t}{2} \equiv 1 \pmod 2$, so that

$$(r, s, t) \equiv (0, 0, 2) \pmod 4.$$

From this, we have that $r - A \equiv s - A \equiv 2 \pmod 4$ and $t - A \equiv 0 \pmod 4$, thus $\alpha = 3$. Examining (5.6), as $B \equiv 4 \pmod 8$ we have that

$$2^4 \parallel (r - A)(s - A)(t - A).$$

As $r - A \equiv s - A \equiv 2 \pmod 4$, we have that $2^2 \parallel t - A$, so $t - A \equiv 4 \pmod 8$. From (5.4) we have

$$r - A + s - A + t - A \equiv -2A \equiv 4 \pmod 8,$$

so that

$$r - A + s - A \equiv 0 \pmod 8.$$

Therefore, up to permutation of r and s, we have

$$(r - A, s - A) \equiv (2, 6) \pmod 8,$$

hence $\beta = 8$.

5.2 Cases 7-13

For all of the following cases, A is even. Thus, by (5.1) and (5.2), $r + s + t$ and $rs + st + rt$ are even. Therefore r, s and t are even.

Case 7: $A \equiv 2$ (**mod** 4), $B \equiv 0$ (**mod** 8), $C \equiv 0$ (**mod** 4)

By (5.1) we have $r + s + t \equiv 2 \pmod 4$, so up to permutation of r, s, t we have, without loss of generality, that $(r, s, t) \equiv (0, 0, 2)$ or $(2, 2, 2) \pmod 4$. Appealing to (5.3), we have that $rst \equiv 0 \pmod{16}$, thus $(r, s, t) \equiv (2, 2, 2) \pmod 4$ cannot occur, hence we must have $(r, s, t) \equiv (0, 0, 2) \pmod 4$. Therefore, without loss of generality, $r - A \equiv 2 \pmod 4$, so $2 \parallel r - A$ and $2 \parallel s - A$, hence $\alpha = 3$. From (5.6) we see that $16 \mid t - A$. Therefore, (5.4) yields $r - A + s - A \equiv 4 \pmod 8$, thus we have $r - A \equiv s - A \equiv 2$ or $6 \pmod 8$. Hence, $\beta = 6$.

Cases 8, 9: $A \equiv 4$ (**mod** 8), $B \equiv 0$ (**mod** 4), $C \equiv 1$ (**mod** 2)

From equations (5.1) and (5.2) we have

$$r + s + t \equiv 4 \pmod 8,$$
$$rs + st + rt \equiv 4 \pmod 8.$$

If $r \equiv 0 \pmod 8$, then $s + t \equiv st \equiv 4 \pmod 8$, hence $(s, t) \equiv (2, 2)$ or $(6, 6) \pmod 8$. If $r \equiv 2 \pmod 8$, then $s + t \equiv 2 \pmod 8$ and $st \equiv 0 \pmod 8$, so

$$(s, t) \equiv (0, 2), (2, 0), (4, 6) \text{ or } (6, 4) \pmod 8.$$

If $r \equiv 4 \pmod 8$, then $s+t \equiv 0 \pmod 8$ and $st \equiv 4 \pmod 8$, so $(s, t) \equiv (2, 6)$ or $(6, 2) \pmod 8$. If $r \equiv 6 \pmod 8$ then $s + t \equiv 6 \pmod 8$ and $st \equiv 0 \pmod 8$, so

$$(s, t) \equiv (0, 6), (2, 4), (4, 2) \text{ or } (6, 0) \pmod 8.$$

Thus, permuting r, s and t if necessary, we have that

$$(r, s, t) \equiv (0, 2, 2), (0, 6, 6) \text{ or } (2, 4, 6) \pmod 8. \tag{5.9}$$

In all cases we have that $2 \parallel t - A$, therefore $\alpha = 3$. By (5.9), modulo 8 we have

$$(r - A, s - A, t - A) \equiv (4, 6, 6),\ (4, 2, 2),\ \text{or } (6, 0, 2) \pmod 8.$$

Note that the difference between Cases 8 and 9 is that in Case 8 we have $B \equiv 4 \pmod 8$ and in Case 9 we have $B \equiv 0 \pmod 8$. Hence, $2b = 4$ in Case 8 and $2b \geq 6$ in Case 9. Thus, in view of (5.6), we attribute

$$(r - A, s - A, t - A) \equiv (4, 6, 6) \text{ or } (4, 2, 2) \pmod 8$$

to Case 8 and $(r - A, s - A, t - A) \equiv (6, 0, 2) \pmod 8$ to Case 9. We then have $\beta = 6$ in Case 8 and $\beta = 8$ in Case 9.

Case 10: $A \equiv 4$ (**mod** 8), $B \equiv 0$ (**mod** 16), $C \equiv 4$ (**mod** 8)

As in Cases 8 and 9, the solutions to the congruence $r + s + t \equiv 4 \pmod 8$ are, up to permutations, $(r, s, t) \equiv (0, 0, 4), (0, 2, 2), (0, 6, 6), (2, 4, 6), (4, 4, 4) \pmod 8$. From (5.2) we have that

$$rs + st + rt \equiv 16 \pmod{32}.$$

Note that $(0, 0, 4) \pmod 8$ does not satisfy this congruence modulo 32, and $(0, 2, 2)$ and $(0, 6, 6) \pmod 8$ do not satisfy this congruence modulo 16. Appealing to equation (5.3), we have

$$rst \equiv 0 \pmod{64},$$

so $(2,4,6) \pmod 8$ does not satisfy this congruence. Thus $(r,s,t) \equiv (4,4,4) \pmod 8$. Therefore, $r - A \equiv s - A \equiv t - A \equiv 0 \pmod 8$. Appealing to (5.4), we have that $(r-A)+(s-A)+(t-A) = -2A$. As $-2A \equiv 8 \pmod{16}$, we have the congruence

$$(r-A)+(s-A)+(t-A) \equiv 8 \pmod{16},$$

which, without loss of generality, has solutions

$$(r-A, s-A, t-A) \equiv (0,0,8),\ (8,8,8) \pmod{16}$$

since $r-A, s-A, t-A \equiv 0 \pmod 8$. Note that the second possibility cannot occur as $(r-A, s-A, t-A) \equiv (8,8,8) \pmod{16}$ contradicts (5.8). Hence, we have $8 \| t - A$. Therefore, $\alpha = 3$.

The deduction of β in this case is much more involved and is treated in a separate section.

Cases 11, 12: $A \equiv 0$ (**mod** 8), $B \equiv 0$ (**mod** 4), $C \equiv 1$ (**mod** 2)

Appealing to (5.1) and (5.2), we have

$$r + s + t \equiv 0 \pmod 8,$$

$$rs + st + rt \equiv 4 \pmod 8.$$

The solutions to the first congruence, up to permutations, are

$$(r, s, t) \equiv (0, 0, 0), (2, 2, 4), (2, 6, 0), (4, 4, 0), (6, 6, 4) \pmod 8.$$

Clearly $(0, 0, 0)$ and $(4, 4, 0)$ do not satisfy the second congruence. In the remaining cases, we have $2 \| r - A$, so $\alpha = 3$.

Note the difference between Cases 11 and 12 is that in Case 11 we have $B \equiv 4 \pmod 8$ and in Case 12 we have $B \equiv 0 \pmod 8$. Hence, we have that $2b = 4$ in Case 11 and $2b \geq 6$ in Case 12. Thus, in view of (5.6), we attribute

$$(r - A, s - A, t - A) \equiv (2, 2, 4) \text{ or } (6, 6, 4) \pmod 8$$

to Case 11 and $(r - A, s - A, t - A) \equiv (2, 6, 0) \pmod 8$ to Case 12. We then have $\beta = 6$ in Case 11 and $\beta = 8$ in Case 12.

Case 13: $A \equiv 0$ (**mod** 8), $B \equiv 0$ (**mod** 16), $C \equiv 4$ (**mod** 16)

From (5.1), (5.2) and (5.3), we have

$$r + s + t \equiv 0 \pmod 8,$$

$$rs + st + rt \equiv 48 \pmod{64},$$

$$rst \equiv 0 \pmod{128}.$$

As in Cases 11 and 12, the solutions to the first congruence, up to permutations, are:

$$(r, s, t) \equiv (0, 0, 0), (2, 2, 4), (2, 6, 0), (4, 4, 0), (6, 6, 4) \pmod 8.$$

Clearly $(0, 0, 0)$ does not satisfy the second congruence, and $(2, 2, 4)$ and $(6, 6, 4)$ do not satisfy the third congruence.

For $(r, s, t) \equiv (2, 6, 0) \pmod 8$, we have

$$(r - A, s - A, t - A) \equiv (2, 6, 0) \pmod 8.$$

Appealing to (5.5), we deduce

$$(r - A)(s - A) + (s - A)(t - A) + (r - A)(t - A) = A^2 - 4C \equiv 0 \pmod 8$$

but

$$(r - A)(s - A) + (s - A)(t - A) + (r - A)(t - A) \equiv 4 + 0 + 0 \equiv 4 \pmod 8,$$

a contradiction. Therefore, $(r, s, t) \equiv (4, 4, 0) \pmod 8$.

Now, recall (5.8) for $p = 2$; namely, that

$$v_2(r - A) + v_2(s - A) + v_2(t - A) \equiv 0 \pmod 2.$$

Now, as $r, s \equiv 4 \pmod 8$, we have that $r - A, s - A \equiv 4 \pmod 8$, hence $4 \| r - A, s - A$. Therefore, $v_2(t - A) \equiv 0 \pmod 2$. Moreover, as $t - A \equiv 0 \pmod 8$, we then have in this case that $t - A \equiv 0 \pmod{16}$. Thus, as $v_2(r - A)$, $v_2(s - A)$ and $v_2(t - A)$ are all even, we have that $2 \nmid r_1, s_1, t_1$, thus $\alpha \neq 3$.

Define integers r_4, s_4 and t_4 such that $r - A = 4r_4$, $s - A = 4s_4$ and $t - A = 4t_4$. Note that r_4 and s_4 are odd as $4 \| (r - A), (s - A)$ and that $4 | t_4$ as $16 | t - A$. Thus

$$r - A = r_1 x^2 = 4r_4 \Rightarrow r_1 \left(\frac{x}{2}\right)^2 = r_4.$$

Therefore, $r_4 \equiv r_1 \pmod 4$. Similarly, $s_4 \equiv s_1 \pmod 4$.

Appealing to (5.4), we have

$$r - A + s - A + t - A = -2A \equiv 0 \pmod{16}.$$

Dividing this congruence by 4, we obtain

$$r_4 + s_4 + t_4 \equiv 0 \pmod 4.$$

However, $t_4 \equiv 0 \pmod 4$, thus

$$r_4 + s_4 + t_4 \equiv r_4 + s_4 \equiv 0 \pmod 4.$$

Therefore, $r_4 \not\equiv s_4 \pmod 4$ as r_4 and s_4 are odd. Thus, $r_1 \not\equiv s_1 \pmod 4$.

Without loss of generality, we may suppose that $r_1 \equiv 3 \pmod 4$ and $s_1 \equiv 1 \pmod 4$. Recalling (5.7), since r_1, s_1 and t_1 are all odd, we have that $\left(\frac{B}{xyz}\right)^2$ is odd. Thus

$$r_1 s_1 t_1 = \left(\frac{B}{xyz}\right)^2 \equiv 1 \pmod 4.$$

As $r_1 s_1 \equiv 3 \pmod 4$, we deduce that $t_1 \equiv 3 \pmod 4$. Therefore, at most one of r_1, s_1, t_1 is congruent to 1 modulo 4. Thus, $\alpha = 2$.

5.3 Case 6: $A \equiv 2 \pmod 4$, $B \equiv 0 \pmod 8$, $C \equiv 1 \pmod 4$

As A is even we have that r, s and t are all even. As $A \equiv 2 \pmod 4$, by (5.1) we have, up to permutations, that $(r, s, t) \equiv (2, 0, 0)$ or $(2, 2, 2) \pmod 4$. If $(r, s, t) \equiv (2, 0, 0) \pmod 4$, then by (5.2) we have $8 \mid 4C$, a contradiction as C is odd, so we have $(r, s, t) \equiv (2, 2, 2) \pmod 4$.

Therefore, we conclude

$$r - A \equiv s - A \equiv t - A \equiv 0 \pmod{4}.$$

This scenario presents some difficulty as it is not trivial to deduce the values of r_1, s_1 and t_1 modulo 4; thus, a more in-depth case analysis will be required in this section. Let

$$e = \frac{r-A}{4} = 2^u e_1,\ f = \frac{s-A}{4} = 2^v f_1,\ h = \frac{t-A}{4} = 2^w h_1,$$

where without loss of generality $u \leq v \leq w$ and e_1, f_1 and h_1 are odd, and notice that e, f and h generate the same quadratic subfields as $r - A, s - A$ and $t - A$, respectively. From (5.4)-(5.6) we obtain the following equations:

$$\begin{aligned}
&2^u e_1 + 2^v f_1 + 2^w h_1 = \frac{-A}{2},\\
&2^{u+v} e_1 f_1 + 2^{v+w} f_1 h_1 + 2^{u+w} e_1 h_1 = \frac{A^2 - 4C}{16} = 2^{l-4} E,\\
&2^{u+v+w} e_1 f_1 h_1 = \left(\frac{B}{8}\right)^2 = 2^{2b-6} B_1^2,
\end{aligned}$$

where

$$A^2 - 4C = 2^l E,\ E \equiv 1 \pmod{2},\ B = 2^b B_1,\ B_1^2 \equiv 1 \pmod{2}.$$

Note that as $\frac{-A}{2}$ is odd, we have that at least one of e, f and h must be odd; therefore, as we assume that $u \leq v \leq w$, we have that $e = e_1$ is odd and $u = 0$. Thus the above equations become

$$e_1 + 2^v f_1 + 2^w h_1 = \frac{-A}{2}, \tag{5.10}$$

$$2^v e_1 f_1 + 2^{v+w} f_1 h_1 + 2^w e_1 h_1 = \frac{A^2 - 4C}{16} = 2^{l-4} E, \tag{5.11}$$

$$2^{v+w} e_1 f_1 h_1 = \left(\frac{B}{8}\right)^2 = 2^{2b-6} B_1^2. \tag{5.12}$$

Recall from Lemma 4.11, which pertains to this case, that $b \geq 3$ and $l \geq 4$. By (5.12) we have

$$v + w = 2b - 6 \tag{5.13}$$

and

$$e_1 f_1 h_1 = B_1^2. \tag{5.14}$$

From (5.13) we have

$$v \equiv w \pmod 2. \tag{5.15}$$

As $B_1^2 \equiv 1 \pmod 8$, we deduce from (5.14) that

$$e_1 f_1 h_1 \equiv 1 \pmod 8, \tag{5.16}$$

so that up to permutation of e_1, f_1 and h_1 we have

$$(e_1, f_1, h_1) \equiv (1, 1, 1),\ (1, 3, 3) \pmod 4. \tag{5.17}$$

Then, from (5.10), we deduce:

$$\text{If } v = w = 0 \text{ then } A \equiv 2 \pmod 8. \tag{5.18}$$

From (5.11) and (5.13) we have:

$$\text{If } v = w = 0 \text{ then } b = 3,\ l = 4,\ \text{and } E \equiv 3 \pmod 4. \tag{5.19}$$

Also, from (5.11), we deduce:

$$\text{If } v < w \text{ then } v = l - 4. \tag{5.20}$$

From (5.15) we have $v \equiv w \pmod 2$. Thus, if $0 < v < w$, then $w \geq 2$ and $w - v \geq 2$ so that by (5.11), (5.16) and (5.20) we obtain:

$$\text{If } 0 < v < w \text{ then } e_1 f_1 \equiv h_1 \equiv E \pmod 4. \tag{5.21}$$

By (5.13) we have:

$$\text{If } v < w \text{ then } v < b - 3. \tag{5.22}$$

By (5.20) and (5.22) we deduce:

$$\text{If } v < w \text{ then } b > l - 1. \tag{5.23}$$

By (5.13) and (5.23) we have:

$$\text{If } b \leq l - 1 \text{ then } v = w = b - 3. \tag{5.24}$$

By (5.13) and (5.20) we deduce:

$$\text{If } v \equiv 0 \pmod 2 \text{ and } l \equiv 1 \pmod 2 \text{ then } b \equiv 1 \pmod 2 \text{ and } v = w = b - 3. \tag{5.25}$$

By (5.11) and (5.13) we have:

$$\text{If } v = w \geq 1 \text{ then } b \leq l - 2. \tag{5.26}$$

From (5.10) we deduce:

$$\text{If } v = w \geq 2 \text{ then } e_1 \equiv \frac{-A}{2} \pmod 8. \tag{5.27}$$

If $b = l - 2 \geq 5$, by (5.24) we have

$$v = w = b - 3 \geq 2,\ l = b + 2,$$

so (5.11) becomes

$$2^{b-3}e_1 f_1 + 2^{2b-6} f_1 h_1 + 2^{b-3} e_1 h_1 = 2^{b-2} E.$$

Dividing the above equation by 2^{b-3} yields

$$e_1(f_1 + h_1) + 2^{b-3} f_1 h_1 = 2E.$$

If $b \geq 6$, we deduce

$$e_1(f_1 + h_1) \equiv 2E \pmod 8.$$

Hence, as $e_1 \equiv \frac{-A}{2} \pmod 8$ by (5.27), multiplying the above congruence by e_1 yields

$$f_1 + h_1 \equiv e_1(2E) \equiv \frac{-A}{2} \cdot 2E \equiv -AE \pmod 8.$$

Therefore, we conclude:

$$\text{If } b = l - 2 \geq 6 \text{ then } f_1 + h_1 \equiv -AE \pmod 8 \text{ and } e_1 \equiv \frac{-A}{2} \pmod 8. \tag{5.28}$$

If $b = 5$, we deduce

$$e_1(f_1 + h_1) \equiv 2E + 4 \pmod 8.$$

Multiplying the above congruence by e_1 yields

$$f_1 + h_1 \equiv e_1(2E + 4) \equiv \frac{-A}{2}(2E + 4) \equiv -AE + 4 \equiv AE \pmod 8.$$

Therefore, we conclude:

$$\text{If } b = l - 2 = 5 \text{ then } f_1 + h_1 \equiv AE \pmod 8 \text{ and } e_1 \equiv \frac{-A}{2} \pmod 8. \tag{5.29}$$

Lemma 5.1.

1. If $\alpha = 0$, then v and w are even and $e_1 \equiv f_1 \equiv h_1 \equiv 1 \pmod 4$.
2. If $\alpha = 2$, then v and w are even and two of e_1, f_1, h_1 are congruent to 3 modulo 4 and the other is congruent to 1 modulo 4.
3. If $\alpha = 3$, then v and w are odd.
4. If $\alpha = 3$, then $\beta = 6$ if and only if $e_1 \equiv 1 \pmod 4$ or $f_1 \equiv h_1 \pmod 4$.
5. If $\alpha = 3$, then $\beta = 8$ if and only if $e_1 \equiv 3 \pmod 4$ or $f_1 \not\equiv h_1 \pmod 4$.

Proof: As e_1, f_1 and h_1 are odd, letting

$$e_1 = x^2 e_2, \quad f_1 = y^2 f_2, \quad h_1 = z^2 h_2,$$

where x, y, z are integers and e_2, f_2 and h_2 are square-free, we have that

$$e_1 \equiv e_2, \quad f_1 \equiv f_2, \quad h_1 \equiv h_2 \pmod 4.$$

Thus, we need only consider e_1, f_1, h_1 when examining the 2-part of $f(K)$ in this case (Case 6). From (5.12) we have that $v + w$ is even, thus either both of v and w are even or both are odd.

If $\alpha = 3$, then by Corollary 2.2 (A) at least one of v or w must be odd, therefore from above we have that both are. When $\alpha \neq 3$, the three quadratic subfields of K are $\mathbb{Q}\left(\sqrt{e_1}\right), \mathbb{Q}\left(\sqrt{f_1}\right)$ and $\mathbb{Q}\left(\sqrt{h_1}\right)$. If $\alpha = 0$, then appealing to Corollary 2.2 (C) we have that $e_1 \equiv f_1 \equiv h_1 \equiv 1 \pmod 4$. If $\alpha = 2$, then by Corollary 2.2 (B) at least one of e_1, f_1 and h_1 is congruent to 3 modulo 4. However, by (5.12), we see that $e_1 f_1 h_1 = B_1^2 \equiv 1 \pmod 4$, thus exactly two of e_1, f_1 and h_1 are congruent to 3 modulo 4, and the remaining one is necessarily congruent to 1 modulo 4. The results when $\beta = 6$ or 8 follow directly from Corollary 2.2 (A). □

We now address the subcases listed in Table 1 of Appendix A. The breakdown of Case 6 into these cases is justified by Lemma 4.11. The first thirteen subcases occur when l is odd, and the final six occur when l is even. Almost all of the following proofs will rely on Lemma 5.1, establishing a contradiction for two of the possible values for α in each subcase.

Subcase 6(i): l odd, $b \geq l - 1 \;\Rightarrow\; \alpha = 3$

Since $l \geq 4$ and l is odd, we have that $l \geq 5$. If $\alpha \neq 3$, then by Lemma 5.1 we have v and

w are even. By (5.25) we have $v = w = b - 3$. If $v = w = 0$, then by (5.19) we have $l = 4$, a contradiction as l is odd. If $v = w \geq 1$, then by (5.24) we have $b \leq l - 2$, a contradiction as $b \geq l - 1$. Therefore, $\alpha = 3$.

By (5.25), if $b = l - 1$ then $v = w = b - 3$; however, this is impossible as (5.26) states if $v = w \geq 1$ then $b \leq l - 2$. Therefore, $b > l - 1$ and $v \neq w$. Thus, without loss of generality, we will assume $v < w$.

Now, by (5.23) we have $v = l - 4$. From (5.10), we have

$$e_1 + 2^v f + 2^w h = \frac{-A}{2}.$$

If $l = 5$ then $v = 1$, thus $2^v f \equiv 2 \pmod 4$. If $l > 5$ then $v \geq 2$, so $2^v f \equiv 0 \pmod 4$. As $v < w$, we have for $l \geq 5$ that $2^w h \equiv 0 \pmod 4$. Therefore, from (5.4) we have

$$e_1 \equiv \begin{cases} \frac{A}{2} \pmod 4, & l = 5, \\ \frac{-A}{2} \pmod 4, & l > 5. \end{cases}$$

Note that $\frac{A}{2} \equiv 1 \pmod 4$ if and only if $A \equiv 2 \pmod 8$ and $\frac{A}{2} \equiv 3 \pmod 4$ if and only if $A \equiv 6 \pmod 8$. Recall that $\alpha = 3$ in this case, so v and w are both odd. Therefore,

$$\beta = \begin{cases} 6, & e_1 \equiv 1 \pmod 4, \\ 8, & e_1 \equiv 3 \pmod 4. \end{cases}$$

Hence, by Lemma 5.1, for $l = 5$, we have

$$\beta = \begin{cases} 6, & A \equiv 2 \pmod 8, \\ 8, & A \equiv 6 \pmod 8, \end{cases}$$

and for $l > 5$, we have

$$\beta = \begin{cases} 6, & A \equiv 6 \pmod 8, \\ 8, & A \equiv 2 \pmod 8. \end{cases}$$

Subcase 6(ii): $l = 7, b = 5,\ A \equiv 6 \pmod{16},\ E \equiv 1 \pmod 4\ \Rightarrow\ \alpha = 0$

By (5.24) we have that $v = w = b - 3 = 2$, so by Lemma 5.1 we have that $\alpha \neq 3$. By (5.29) we have that $f_1 + h_1 \equiv AE \equiv 6 \pmod 8$ and $e_1 \equiv \frac{-A}{2} \equiv 5 \pmod 8$. If $\alpha = 2$ then by Lemma 5.1 we have $f_1 \equiv h_1 \equiv 3 \pmod 4$. As $f_1 + h_1 \equiv 6 \pmod 8$, we then conclude that $f_1 \equiv h_1 \pmod 8$. But then $e_1 f_1 h_1 \equiv 5 \pmod 8$, contradicting (5.16). Therefore, $\alpha \neq 2$. Thus, $\alpha = 0$.

Subcase 6(iii): $l = 7,\ b = 5,\ A \equiv 6 \pmod{16},\ E \equiv 3 \pmod 4\ \Rightarrow\ \alpha = 2$

By (5.24) we have that $v = w = b - 3 = 2$, so by Lemma 5.1 we have that $\alpha \neq 3$. By (5.29) we have that $f_1 + h_1 \equiv AE \equiv 2 \pmod 8$ and $e_1 \equiv \frac{-A}{2} \equiv 5 \pmod 8$. If $\alpha = 0$ then by Lemma 5.1 we have $f_1 \equiv h_1 \equiv 1 \pmod 4$. As $f_1 + h_1 \equiv 2 \pmod 8$, we conclude that $f_1 \equiv h_1 \pmod 8$. But then $e_1 f_1 h_1 \equiv 5 \pmod 8$, contradicting (5.16). Therefore, $\alpha \neq 0$. Thus, $\alpha = 2$.

Subcase 6(iv): $l = 7,\ b = 5,\ A \equiv 14 \pmod{16}, E \equiv 1 \pmod 4\ \Rightarrow\ \alpha = 2$

By (5.24) we have that $v = w = b - 3 = 2$, so by Lemma 5.1 we have that $\alpha \neq 3$. By (5.29) we have that $f_1 + h_1 \equiv AE \equiv 6 \pmod 8$ and $e_1 \equiv \frac{-A}{2} \equiv 1 \pmod 8$. If $\alpha = 0$ then by Lemma 5.1 we have $f_1 \equiv h_1 \equiv 1 \pmod 4$. As $f_1 + h_1 \equiv 6 \pmod 8$, we conclude, up to a permutation of f_1 and h_1, that $f_1 \equiv 1 \pmod 8$ and $h_1 \equiv 5 \pmod 8$. But then $e_1 f_1 h_1 \equiv 5 \pmod 8$, contradicting (5.16). Therefore, $\alpha \neq 0$. Thus, $\alpha = 2$.

Subcase 6(v): $l = 7,\ b = 5,\ A \equiv 14 \pmod{16},\ E \equiv 3 \pmod 4 \ \Rightarrow\ \alpha = 0$

By (5.24) we have that $v = w = b - 3 = 2$, so by Lemma 5.1 we have that $\alpha \neq 3$. By (5.29) we have that $f_1 + h_1 \equiv AE \equiv 2 \pmod 8$ and $e_1 \equiv \frac{-A}{2} \equiv 1 \pmod 8$. If $\alpha = 2$ then by Lemma 5.1 we have $f_1 \equiv h_1 \equiv 3 \pmod 4$. As $f_1 + h_1 \equiv 2 \pmod 8$, we then conclude, up to a permutation of f_1 and h_1, that $f_1 \equiv 3 \pmod 8$ and $h_1 \equiv 7 \pmod 8$. But then $e_1 f_1 h_1 \equiv 5 \pmod 8$, contradicting (5.16). Therefore, $\alpha \neq 2$. Thus, $\alpha = 0$.

Subcase 6(vi): l odd, $b = l - 2$, $l \geq 9$, $A \equiv 6 \pmod{16}$, $E \equiv 1 \pmod 4 \ \Rightarrow\ \alpha = 2$

By (5.24) we have that $v = w = b - 3 \geq 4$, so by Lemma 5.1 we have that $\alpha \neq 3$. By (5.28) we have that $f_1 + h_1 \equiv -AE \equiv 2 \pmod 8$ and $e_1 \equiv \frac{-A}{2} \equiv 5 \pmod 8$. If $\alpha = 0$ then by Lemma 5.1 we have $f_1 \equiv h_1 \equiv 1 \pmod 4$. As $f_1 + h_1 \equiv 2 \pmod 8$, we conclude $f_1 \equiv h_1 \pmod 8$. But then $e_1 f_1 h_1 \equiv 5 \pmod 8$, contradicting (5.16). Therefore, $\alpha \neq 0$. Thus, $\alpha = 2$.

Subcase 6(vii): l odd, $b = l - 2$, $l \geq 9$, $A \equiv 6 \pmod{16}$, $E \equiv 3 \pmod 4 \ \Rightarrow\ \alpha = 0$

By (5.24) we have that $v = w = b - 3 \geq 4$, so by Lemma 5.1 we have that $\alpha \neq 3$. By (5.28) we have that $f_1 + h_1 \equiv -AE \equiv 6 \pmod 8$ and $e_1 \equiv \frac{-A}{2} \equiv 5 \pmod 8$. If $\alpha = 2$ then by Lemma 5.1 we have $f_1 \equiv h_1 \equiv 3 \pmod 4$. As $f_1 + h_1 \equiv 6 \pmod 8$, we conclude $f_1 \equiv h_1 \pmod 8$. But then $e_1 f_1 h_1 \equiv 5 \pmod 8$, contradicting (5.16). Therefore, $\alpha \neq 2$. Thus, $\alpha = 0$.

<u>**Subcase 6(viii):** l odd, $b = l - 2, l \geq 9, A \equiv 14 \pmod{16},\ E \equiv 1 \pmod 4 \ \Rightarrow\ \alpha = 0$</u>

By (5.24) we have that $v = w = b - 3 \geq 4$, so by Lemma 5.1 we have that $\alpha \neq 3$. By (5.28) we have that $f_1 + h_1 \equiv -AE \equiv 2 \pmod 8$ and $e_1 \equiv \frac{-A}{2} \equiv 1 \pmod 8$. If $\alpha = 2$ then by Lemma 5.1 we have $f_1 \equiv h_1 \equiv 3 \pmod 4$. As $f_1 + h_1 \equiv 2 \pmod 8$, we conclude, up to permutation of f_1 and h_1, that $f_1 \equiv 3 \pmod 8$ and $h_1 \equiv 7 \pmod 8$. But then $e_1 f_1 h_1 \equiv 5 \pmod 8$, contradicting (5.16). Therefore, $\alpha \neq 2$. Thus, $\alpha = 0$.

<u>**Subcase 6(ix):** l odd, $b = l - 2, l \geq 9, A \equiv 14 \pmod{16},\ E \equiv 3 \pmod 4 \ \Rightarrow\ \alpha = 2$</u>

By (5.24) we have that $v = w = b - 3 \geq 4$, so by Lemma 5.1 we have that $\alpha \neq 3$. By (5.28) we have that $f_1 + h_1 \equiv -AE \equiv 6 \pmod 8$ and $e_1 \equiv \frac{-A}{2} \equiv 1 \pmod 8$. If $\alpha = 0$ then by Lemma 5.1 we have $f_1 \equiv h_1 \equiv 1 \pmod 4$. As $f_1 + h_1 \equiv 6 \pmod 8$, we conclude, up to permutation of f_1 and h_1, that $f_1 \equiv 1 \pmod 8$ and $h_1 \equiv 5 \pmod 8$. But then $e_1 f_1 h_1 \equiv 5 \pmod 8$, contradicting (5.16). Therefore, $\alpha \neq 0$. Thus, $\alpha = 2$.

<u>**Subcase 6(x):** l odd, $b \leq l - 3$, b even $\ \Rightarrow\ \alpha = 3$</u>

If $\alpha \neq 3$, then by Lemma 5.1 we have that v and w are even. However, by (5.24) we have that $v = w = b - 3$, a contradiction as b is even. Therefore, $\alpha = 3$. By (5.24) we have $v = w = b - 3$. Also, from (5.27), we have $e_1 \equiv \frac{-A}{2} \pmod 8$. Similar to the $l > 5$ case in subcase (i), we have from Lemma 5.1that

$$\beta = \begin{cases} 6, & A \equiv 6 \pmod 8, \\ 8, & A \equiv 2 \pmod 8). \end{cases}$$

<u>**Subcase 6(xi):** l odd, $b < l-3$, $b = 5$, $A \equiv 10 \pmod{16} \;\Rightarrow\; \alpha = 2$</u>

By (5.24) we have that $v = w = b - 3 = 2$, so $\alpha \neq 3$. Supposing that $\alpha = 0$, then by Lemma 5.1 we have that $f_1 + h_1 \equiv 2 \pmod 4$. Thus, from (5.11) we deduce that $2^3 \parallel 2^{l-4}E$, so $l = 7$. Therefore, $b < 4$, a contradiction as $b = 5$. Thus, $\alpha \neq 0$. Hence $\alpha = 2$.

<u>**Subcase 6(xii):** l odd, $b < l-3$, $b = 7$, $A \equiv 2 \pmod{16} \;\Rightarrow\; \alpha = 2$</u>

As $b < l-3$ we have by (5.24) that $v = w = b-3 = 4$. Hence, as v and w are both even, we deduce from Lemma 5.1 that $\alpha \neq 3$. From (5.11) we have

$$2^4 e_1(f_1 + h_1) + 2^8 f_1 h_1 = 2^{l-4}E,$$

where $l - 4 > b - 1 = 6$, so $4|f_1 + h_1$. Thus $(f_1, h_1) \not\equiv (1,1) \pmod 4$, so by Lemma 5.1 we have $\alpha \neq 0$. Therefore, $\alpha = 2$.

<u>**Subcase 6(xiii):** l odd, $b < l-3$, b (odd) ≥ 9, $A \equiv 2 \pmod{16} \;\Rightarrow\; \alpha = 2$</u>

As $b < l - 3$ we have by (5.24) that $v = w = b - 3$. As b is odd, v and w are both even, so by Lemma 5.1 we have $\alpha \neq 3$. From (5.11) we have

$$2^{b-3} e_1(f_1 + h_1) + 2^{2b-6} f_1 h_1 = 2^{l-4}E.$$

Dividing by 2^{b-3}, we obtain

$$e_1(f_1 + h_1) + 2^{b-3} f_1 h_1 = 2^{l-b-1}E.$$

As $b - 3 \geq 6$ and $l - b - 1 > 2$, we have $4|f_1 + h_1$. Thus $(f_1, h_1) \not\equiv (1,1) \pmod 4$, so by

Lemma 5.1 we have $\alpha \neq 0$. Therefore, $\alpha = 2$.

Subcase 6(xiv): l even, $b \geq l$, $l \geq 6$, $A \equiv 6 \pmod 8$, $E \equiv 1 \pmod 4$ $\Rightarrow$ $\alpha = 0$

If $\alpha = 3$ then by Lemma 5.1 we have that v and w are odd. If $v \neq w$, then $v < w$ and by (5.20) we have that $v = l - 4$, a contradiction as l is even. Thus, $v = w$. But from (5.26), as $v \geq 1$ and $v = w$ we have $b \leq l - 2$, a contradiction. Therefore, $\alpha \neq 3$.

If $\alpha = 2$, then by Lemma 5.1 we have that v and w are even. If $v \neq w$, then $v < w$ and by (5.20) we have that $v = l - 4 \geq 2$. Thus, by (5.10), we have $e_1 \equiv \frac{-A}{2} \equiv 1 \pmod 4$. Hence, as we are supposing that $\alpha = 2$, we have that $f_1 \equiv h_1 \equiv 3 \pmod 4$. However, by (5.21), we have $e_1 f_1 \equiv h_1 \equiv E \equiv 1 \pmod 4$, a contradiction. Therefore, $v = w$. From (5.13) we have that $v = b - 3 \geq l - 3 \geq 3$. However, we then have again from (5.26) that $b \leq l - 2$, a contradiction. Thus $\alpha \neq 2$. Therefore, $\alpha = 0$.

Subcase 6(xv): l even, $b \geq l$, $l \geq 6$, $A \equiv 2 \pmod 8$ or $E \equiv 3 \pmod 4$ $\Rightarrow$ $\alpha = 2$

If $\alpha = 3$ then by Lemma 5.1 we have that v and w are odd. If $v \neq w$ then $v < w$, thus by (5.20) we have that $v = l - 4$, a contradiction as l is even. Therefore, $v = w \geq 1$. But from (5.26) we have that $b \leq l - 2$, a contradiction. Therefore, $\alpha \neq 3$.

Suppose $\alpha = 0$. By Lemma 5.1 we have that v and w are even and $e_1 \equiv f_1 \equiv h_1 \equiv 1 \pmod 4$. If $v = w = 0$ then by (5.19) we have that $b = 3$, a contradiction. If $v = w \geq 2$ we have from (5.26) that $b \leq l - 2$, a contradiction. Thus $v < w$ and from (5.20) we have that $v = l - 4 \geq 2$. As $2 \leq v < w$ we deduce from (5.10) that

$$1 \equiv e_1 \equiv \frac{-A}{2} \pmod 4,$$

so that $A \equiv 6 \pmod 8$. Therefore, $E \equiv 3 \pmod 4$ by the hypothesis of this subcase. From

(5.21) we have that $h_1 \equiv E \equiv 3 \pmod 4$, a contradiction. Thus $\alpha \neq 0$. Therefore, $\alpha = 2$.

Subcase 6(xvi): $b = 3, l = 4, A \equiv 2 \pmod{16} \;\Rightarrow\; \alpha = 2$

As $b = 3$ we have $2b - 6 = 0$, so by (5.13) we have that $v = w = 0$, thus $\alpha \neq 3$. If $\alpha = 0$ then by Lemma 5.1 we have that $e_1 \equiv f_1 \equiv h_1 \equiv 1 \pmod 4$. From (5.10) we have that $e_1 + f_1 + h_1 = \frac{-A}{2} \equiv 7 \pmod 8$. The only solutions to this congruence, up to permutation of e_1, f_1 and h_1, are $(e_1, f_1, h_1) \equiv (1,1,5),\ (5,5,5) \pmod 8$, contradicting (5.16). Thus $\alpha \neq 0$. Therefore, $\alpha = 2$.

Subcase 6(xvii): $b = 3, l = 4, A \equiv 10 \pmod{16} \;\Rightarrow\; \alpha = 0$

Again, as in subcase 6(xvi), $v = w = 0$ and $\alpha \neq 3$. If $\alpha = 2$, then by (5.10) we have that $e_1 + f_1 + h_1 \equiv 3 \pmod 8$. By Lemma 5.1 we may suppose without loss of generality that $e_1 \equiv 1 \pmod 4$ and $f_1 \equiv h_1 \equiv 3 \pmod 4$. Thus, the solutions of $e_1 + f_1 + h_1 \equiv 3 \pmod 8$ up to permutation of f_1 and h_1 are $(e_1, f_1, h_1) \equiv (1,3,7),\ (5,3,3),\ (5,7,7) \pmod 8$, contradicting (5.16). Thus $\alpha \neq 2$. Therefore, $\alpha = 0$.

Subcase 6(xviii): b even, l even, $b \leq l - 2$, $l \geq 6$, $b \geq 4 \;\Rightarrow\; \alpha = 3$

From (5.24) as $b \leq l - 2$ we have that $v = w = b - 3 \geq 1$. As b is even we have that v and w are odd, therefore $\alpha = 3$ by Lemma 5.1. We have $e_1 \equiv \frac{-A}{2} \pmod 8$. Therefore, by Lemma 5.1 we deduce

$$\beta = \begin{cases} 6, & A \equiv 6 \pmod 8, \\ 8, & A \equiv 2 \pmod 8. \end{cases}$$

<u>**Subcase(xix):** b odd, l even, $b \le l-2$, $l \ge 8$, $b \ge 5 \;\Rightarrow\; \alpha = 2$</u>

From (5.24) as $b \le l-2$ we have that $v = w = b-3 \ge 2$. As b is odd we have that v and w are even, therefore $\alpha \ne 3$ by Lemma 5.1.

If $\alpha = 0$, then by Lemma 5.1 we have that $e_1 \equiv f_1 \equiv h_1 \equiv 1 \pmod 4$. From (5.11) we then have that $v+1 = l-4$, a contradiction as l and v are even. Thus $\alpha \ne 0$. Therefore, $\alpha = 2$.

5.4 Case 10: $A \equiv 4 \pmod 8$, $B \equiv 0 \pmod{16}$, $C \equiv 4 \pmod 8$

We have from the conductor argument that $\alpha = 3$ and

$$(r-A, s-A, t-A) \equiv (0,0,8) \pmod{16}.$$

In order to determine β, we need to understand the values r_1 and s_1 modulo 8. Given $r-A \equiv s-A \equiv 0 \pmod{16}$, this will require a more detailed analysis. Let

$$r_2 = v_2(r-A),\; s_2 = v_2(s-A),\; t_2 = v_2(t-A) \tag{5.30}$$

so that

$$r_2 \ge 4,\; s_2 \ge 4,\; t_2 = 3. \tag{5.31}$$

Next, define the odd integers r_0, s_0 and t_0 by

$$r_0 = \frac{r-A}{2^{r_2}},\; s_0 = \frac{s-A}{2^{s_2}},\; t_0 = \frac{t-A}{2^{t_2}}. \tag{5.32}$$

Recall that $b = v_2(B)$ and set

$$B_0 = \frac{B}{2^b} \equiv 1 \pmod 2. \tag{5.33}$$

Recall (5.6), namely

$$(r - A)(s - A)(t - A) = B^2. \tag{5.34}$$

From (5.32), (5.33) and (5.34) we deduce

$$r_2 + s_2 + t_2 = 2b \tag{5.35}$$

and dividing (5.34) by 2^{2b} yields

$$r_0 s_0 t_0 = B_0^2 \equiv 1 \pmod 4. \tag{5.36}$$

From (5.31) and (5.35) we deduce

$$r_2 + s_2 = 2b - 3 \equiv 1 \pmod 2 \tag{5.37}$$

so that

$$r_2 \neq s_2. \tag{5.38}$$

In view of (5.38), without loss of generality, we may assume that $r_2 > s_2$ so that

$$r_2 \geq s_2 + 1. \tag{5.39}$$

By (5.30) and (5.31) we have

$$v_2(s-A+t-A)=3. \tag{5.40}$$

Therefore, by (5.30) and (5.40), we obtain

$$v_2((r-A)(s-A+t-A))=r_2+3. \tag{5.41}$$

Also, by (5.30) and (5.31), we have

$$v_2\left((s-A)(t-A)\right)=s_2+3. \tag{5.42}$$

Recalling (5.5), we have

$$\begin{aligned} 2^l E &= (r-A)(s-A)+(s-A)(t-A)+(r-A)(t-A) \\ &= (r-A)(s-A+t-A)+(s-A)(t-A). \end{aligned} \tag{5.43}$$

From (5.39), (5.41), (5.42), and (5.43) we deduce that $l=s_2+3$. Therefore,

$$s_2=l-3. \tag{5.44}$$

Appealing to (5.37) and (5.44), we have

$$r_2=2b-l. \tag{5.45}$$

Then, from (5.39), (5.44) and (5.45), we deduce

$$b\geq l-1. \tag{5.46}$$

From (5.31) and (5.44) we have

$$l \geq 7.$$

From (5.45) we deduce that

$$r_2 \equiv l \pmod{2}. \tag{5.47}$$

From (5.45) and (5.46) we have

$$r_2 \geq l - 2. \tag{5.48}$$

If $b = l - 1$, then from (5.45) we have that $r_2 = l - 2$. If $b \geq l$, we have from (5.45) that $r_2 \geq l$. Hence, we have

$$\begin{cases} r_2 = l - 2, & \text{if } b = l - 1, \\ r_2 \geq l, & \text{if } b \geq l. \end{cases} \tag{5.49}$$

Dividing (5.43) by 2^l, we deduce from (5.31), (5.32), (5.44) and (5.45) that

$$E = r_0 2^{2(b-l)+3} \left(2^{l-6} s_0 + t_0\right) + s_0 t_0. \tag{5.50}$$

Appealing to (5.36), we have

$$r_0 \equiv s_0 t_0 \pmod{4} \tag{5.51}$$

and

$$s_0 \equiv r_0 t_0 \pmod{4}. \tag{5.52}$$

Subcase (a): l odd

If l is odd, then by (5.47) we have that

$$r_2 \equiv 1(\bmod 2). \tag{5.53}$$

As $t_2 = 3$, we have that

$$t_1 z^2 = t - A = 2^3 t_0$$

with t_0 odd, so $2 \| t_1$ and $2 \| z$. Hence,

$$t_1 \equiv 2 \pmod 4. \tag{5.54}$$

Next, we have

$$r_1 x^2 = r - A = 2^{r_2} r_0. \tag{5.55}$$

By (5.53) r_2 is odd, hence (5.55) implies $2 | r_1$. As r_1 is square-free, we have

$$r_1 \equiv 2 \pmod 4. \tag{5.56}$$

As $\alpha = 3$, conditions (5.54) and (5.56) allow us to deduce from Corollary 2.2 (A) that

$$\beta = \begin{cases} 6, & \text{if } r_1 \equiv t_1 \pmod 8, \\ 8, & \text{if } r_1 \not\equiv t_1 \pmod 8. \end{cases} \tag{5.57}$$

From (5.55) and (5.56) we deduce that $2^{\frac{r_2-1}{2}} \| x$, thus (5.55) gives

$$2r_0 = r_1 \left(\frac{x}{2^{\frac{r_2-1}{2}}} \right)^2,$$

and hence

$$2r_0 \equiv r_1 \pmod 8. \tag{5.58}$$

Similarly, as $t_1 \equiv 2 \pmod 4$, we have that

$$2t_0 \equiv t_1 \pmod 8. \tag{5.59}$$

Appealing to (5.58) and (5.59), we can reformulate (5.57) as

$$\beta = \begin{cases} 6, & \text{if } r_0 \equiv t_0 \pmod 4, \\ 8, & \text{if } r_0 \not\equiv t_0 \pmod 4. \end{cases} \tag{5.60}$$

Subcase (a) (i): l odd, $b = l - 1$

If $l = 7$ then $b = l - 1 = 6$, thus by (5.44) and (5.45) we have

$$r_2 = 2 \cdot 6 - 7 = 5, \;\; s_2 = 7 - 3 = 4. \tag{5.61}$$

Then (5.4), (5.31), (5.32) and (5.61) yield

$$-2A = 2^5 r_0 + 2^4 s_0 + 2^3 t_0. \tag{5.62}$$

Reducing (5.62) modulo 32, we obtain

$$-2A \equiv 16 + 8t_0 \pmod{32}. \tag{5.63}$$

As $A \equiv 4 \pmod 8$, (5.63) gives

$$t_0 \equiv \begin{cases} 1 \pmod 4, & \text{if } A \equiv 4 \pmod{16}, \\ 3 \pmod 4, & \text{if } A \equiv 12 \pmod{16}. \end{cases} \tag{5.64}$$

If $l > 7$ then $l \geq 9$ as l is odd, so from (5.44) and (5.45) we have

$$r_2 = l - 2 \geq 7, \;\; s_2 = l - 3 \geq 6. \tag{5.65}$$

Then (5.4), (5.31), (5.32) and (5.65) give

$$-2A = 2^{r_2} r_0 + 2^{s_2} s_0 + 2^{t_2} t_0 \equiv 8t_0 \pmod{32},$$

so

$$A \equiv -4t_0 \pmod{16}. \tag{5.66}$$

Thus, as $A \equiv 4 \pmod 8$, (5.66) yields

$$t_0 \equiv \begin{cases} 3 \pmod 4, & \text{if } A \equiv 4 \pmod{16}, \\ 1 \pmod 4, & \text{if } A \equiv 12 \pmod{16}. \end{cases} \tag{5.67}$$

Suppose that $E \equiv 1 \pmod 4$. In this case, (5.50) gives

$$E = r_0 2\left(2^{l-6} s_0 + t_0\right) + s_0 t_0 \equiv 1 \pmod 4. \tag{5.68}$$

As $l \geq 7$, we obtain

$$s_0t_0 \equiv 3 \pmod{4},$$

so by (5.51) we have that

$$r_0 \equiv 3 \pmod{4}. \tag{5.69}$$

Therefore, if $E \equiv 1 \pmod{4}$ and $l = 7$, we deduce from (5.60), (5.64) and (5.69) that

$$\beta = \begin{cases} 6, & \text{if } A \equiv 12 \pmod{16}, \\ 8, & \text{if } A \equiv 4 \pmod{16}, \end{cases} \tag{5.70}$$

whereas, if $E \equiv 1 \pmod{4}$ and $l > 7$, we deduce from (5.60),(5.67) and (5.69) that

$$\beta = \begin{cases} 6, & \text{if } A \equiv 4 \pmod{16}, \\ 8, & \text{if } A \equiv 12 \pmod{16}. \end{cases} \tag{5.71}$$

Now suppose that $E \equiv 3 \pmod{4}$. From (5.50), as $E \equiv 3 \pmod{4}$ and $l \geq 7$ we obtain

$$s_0t_0 \equiv 1 \pmod{4},$$

so by (5.51) we have that

$$r_0 \equiv 1 \pmod{4}. \tag{5.72}$$

Therefore, if $E \equiv 3 \pmod{4}$ and $l = 7$, appealing to (5.60) we have from (5.64) and (5.72) that

$$\beta = \begin{cases} 6, & \text{if } A \equiv 4 \pmod{16}, \\ 8, & \text{if } A \equiv 12 \pmod{16}, \end{cases} \tag{5.73}$$

whereas, if $E \equiv 3 \pmod 4$ and $l > 7$, appealing to (5.60) we have from (5.67) and (5.72) that

$$\beta = \begin{cases} 6, & \text{if } A \equiv 12 \pmod{16}, \\ 8, & \text{if } A \equiv 4 \pmod{16}. \end{cases} \tag{5.74}$$

Subcase (a) (ii): l odd, $b \geq l$

As $b - l \geq 0$, examining (5.50) modulo 4, we have from (5.51) that

$$E \equiv s_0 t_0 \equiv r_0 \pmod 4. \tag{5.75}$$

Our analysis of (5.4) will proceed almost exactly as it did in Subcase (a) (i). We have at all times that $r_2 \geq 7$ by (5.49). From (5.44) we have $s_2 = 4$ when $l = 7$ and $s_2 \geq 6$ when $l > 7$. Therefore, using the same arguments from Subcase (a) (i), we have when $l = 7$ that

$$t_0 \equiv \begin{cases} 1 \pmod 4, & \text{if } A \equiv 4 \pmod{16}, \\ 3 \pmod 4, & \text{if } A \equiv 12 \pmod{16}, \end{cases} \tag{5.76}$$

and when $l > 7$, we have

$$t_0 \equiv \begin{cases} 3 \pmod 4, & \text{if } A \equiv 4 \pmod{16}, \\ 1 \pmod 4, & \text{if } A \equiv 12 \pmod{16}. \end{cases} \tag{5.77}$$

If $E \equiv 1 \pmod 4$, when $l = 7$ we have from (5.60), (5.75) and (5.76) that

$$\beta = \begin{cases} 6, & \text{if } A \equiv 4 \pmod{16}, \\ 8, & \text{if } A \equiv 12 \pmod{16}, \end{cases} \tag{5.78}$$

and when $l > 7$ we have from (5.60), (5.75) and (5.77) that

$$\beta = \begin{cases} 6, & \text{if } A \equiv 12 \pmod{16}, \\ 8, & \text{if } A \equiv 4 \pmod{16}. \end{cases} \tag{5.79}$$

If $E \equiv 3 \pmod 4$, when $l = 7$ we have from (5.60), (5.75) and (5.76) that

$$\beta = \begin{cases} 6, & \text{if } A \equiv 12 \pmod{16}, \\ 8, & \text{if } A \equiv 4 \pmod{16}, \end{cases} \tag{5.80}$$

and when $l > 7$ we have from (5.60), (5.75) and (5.77) that

$$\beta = \begin{cases} 6, & \text{if } A \equiv 4 \pmod{16}, \\ 8, & \text{if } A \equiv 12 \pmod{16}. \end{cases} \tag{5.81}$$

This concludes our analysis in the case where l is odd. Note that, for $m, n \in \mathbb{Z}$, if $m = 16k + 4m_1$ and $n = 4j + n_1$ for $k, j \in \mathbb{Z}$ and $m_1 \equiv 1 \pmod 2$, that $mn = 64jk + 16kn_1 + 16jm_1 + 4m_1n_1 \equiv 4m_1n_1 \pmod{16}$. Using this fact, we are able to summarize the above results for β using $AE \pmod{16}$ in Table 2 of Appendix A.

Subcase (b): l even

From (5.47) and (5.37), we have that

$$s_2 \equiv 1 \pmod 2,\ r_2 \equiv 0 \pmod 2.$$

Since $K = \mathbb{Q}\left(\sqrt{s_1},\ \sqrt{t_1}\right)$, we may thus construct the analogue of (5.60) for s_0 and t_0; that is,

$$\beta = \begin{cases} 6, & \text{if } s_0 \equiv t_0 \pmod 4, \\ 8, & \text{if } s_0 \not\equiv t_0 \pmod 4. \end{cases} \tag{5.82}$$

As l is even, since $l \geq 7$ we have that

$$l \geq 8.$$

<u>Subcase (b) (i): l even, $b = l - 1$</u>

We have from (5.68) that

$$E = r_0 2\left(2^{l-6} s_0 + t_0\right) + s_0 t_0,$$

so as $l \geq 8$, we have

$$-E \equiv s_0 t_0 \pmod 4. \tag{5.83}$$

Suppose that $E \equiv 1 \pmod 4$. Then from (5.83) we have $s_0 t_0 \equiv 3 \pmod 4$, thus

$$s_0 \not\equiv t_0 \pmod 4.$$

Therefore, by (5.82), if $E \equiv 1 \pmod 4$ we have

$$\beta = 8. \tag{5.84}$$

Suppose that $E \equiv 3 \pmod 4$. Then from (5.83) we have $s_0t_0 \equiv 1 \pmod 4$, thus

$$s_0 \equiv t_0 \pmod 4.$$

Therefore, by (5.82), if $E \equiv 3 \pmod 4$ we have

$$\beta = 6. \tag{5.85}$$

<u>Subcase (b) (ii): l even, $b \geq l$</u>

As $b - l \geq 0$, examining (5.50) modulo 4, we have from (5.51) that

$$E \equiv s_0t_0 \pmod 4. \tag{5.86}$$

Suppose that $E \equiv 1 \pmod 4$. Then from (5.86) we have $s_0t_0 \equiv 1 \pmod 4$, thus

$$s_0 \equiv t_0 \pmod 4.$$

Therefore, by (5.82), if $E \equiv 1 \pmod 4$ we have

$$\beta = 6. \tag{5.87}$$

Suppose that $E \equiv 3 \pmod 4$. Then from (5.86) we have $s_0 t_0 \equiv 3 \pmod 4$, thus

$$s_0 \not\equiv t_0 \pmod 4.$$

Therefore, by (5.82), if $E \equiv 1 \pmod 4$ we have

$$\beta = 8. \tag{5.88}$$

This completes our treatment of Main Case 1: $AB(A^2 - 4C) \neq 0$.

Chapter 6

Main Case 2: $AB \neq 0,\ A^2 - 4C = 0$

6.1 The Odd Part of the conductor

As $A^2 - 4C = 0$ we have that $A^2 = 4C$, thus $A \equiv 0 \pmod 2$ and $C = \left(\frac{A}{2}\right)^2$ is a square. We note that all results in Chapter 2 hold for this case. In particular, $r-A, s-A, t-A$ remain as generators for the three distinct quadratic subfields of K, and equations (2.20)-(2.22) and (5.1)-(5.6) are valid. Using $A^2 - 4C = 0$, these relations become:

$$(r-A)^3 + 2A(r-A)^2 = B^2, \tag{6.1}$$

$$(s-A)^3 + 2A(s-A)^2 = B^2, \tag{6.2}$$

$$(t-A)^3 + 2A(t-A)^2 = B^2, \tag{6.3}$$

$$r + s + t = A, \tag{6.4}$$

$$rs + st + rt = -4C, \tag{6.5}$$

$$rst = B^2 - 4AC, \tag{6.6}$$

$$(r-A) + (s-A) + (t-A) = -2A, \tag{6.7}$$

$$-(r-A)(s-A+t-A) = (s-A)(t-A), \tag{6.8}$$

$$(r-A)(s-A)(t-A) = B^2. \tag{6.9}$$

Let p be an odd prime. Recall for an odd prime p that

$$a_p = v_p(A),\ b_p = v_p(B),\ c_p = v_p(C),$$

and let

$$r_p = v_p(r - A),\ s_p = v_p(s - A),\ t_p = v_p(t - A).$$

From $A^2 = 4C$ we deduce

$$2a_p = c_p. \tag{6.10}$$

From (6.1) we deduce

$$v_p\left((r - A)^3 + 2A(r - A)^2\right) = 2b_p. \tag{6.11}$$

From (6.11) we see that

$$\text{if } r_p > a_p,\ a_p + 2r_p = 2b_p, \tag{6.12}$$

$$\text{if } r_p < a_p,\ 3r_p = 2b_p, \tag{6.13}$$

$$\text{if } r_p = a_p,\ 2b_p \geq 3r_p = 3a_p. \tag{6.14}$$

From (6.8), we have

$$r_p + v_p(s - A + t - A) = s_p + t_p. \tag{6.15}$$

From (6.15) we deduce

$$\text{if } s_p > t_p,\ r_p = s_p, \tag{6.16}$$

$$\text{if } s_p < t_p,\ r_p = t_p, \tag{6.17}$$

$$\text{if } s_p = t_p,\ r_p \leq s_p = t_p. \tag{6.18}$$

From (6.9), we have

$$r_p + s_p + t_p = 2b_p. \tag{6.19}$$

If r_p is odd, then by (6.19) we have

$$s_p + t_p = 2b_p - r_p \equiv 1 \pmod 2.$$

We conclude that $s_p \neq t_p$ when r_p is odd. Therefore, without loss of generality, we shall assume that $s_p > t_p$ when r_p is odd. Thus, using (6.15) and (6.16), we deduce:

$$\text{If } r_p \text{ is odd, then } s_p > t_p,\ v_p(s - A + t - A) = t_p \text{ and } r_p = s_p. \tag{6.20}$$

Lemma 6.1. Let p be an odd prime. If $r_p,\ s_p$ or t_p is odd, then b_p is odd and $a_p = 0$.

Proof: Without loss of generality, let r_p be odd. For an odd prime p, we wish to examine $2b_p$ using (6.11). Depending on the values of a_p and r_p, three cases arise:

Case 1: $r_p < a_p$.

Case 2: $r_p = a_p$.

Case 3: $r_p > a_p$.

<u>Case 1:</u> If $r_p < a_p$ then by (6.13) we have that $3r_p = 2b_p$, which is impossible as r_p is odd. Therefore, Case 1 cannot occur.

<u>Case 2:</u> Here, $r_p = a_p$. Then we have a_p is odd and from (6.14) we have that $2b_p \geq 3a_p$.

Thus $2b_p \geq 3$, so $b_p \geq 2$ and $2b_p \geq 4$. By (6.10), we have that $c_p = 2a_p$. Therefore, if $a_p \geq 3$, then we have $c_p \geq 6$ and $2b_p \geq 9$, thus $b_p \geq 5$. This contradicts our simplifying assumption (1.6) that there is no prime p such that $a_p \geq 2$, $b_p \geq 3$ and $c_p \geq 4$. Thus $a_p = r_p = 1$. From (6.14) we deduce $s_p = 1$ and $1 > t_p$. Hence $t_p = 0$. Therefore, from (6.19) we deduce $b_p = 1$. Clearly, having $r_p = s_p = a_p = 1$ and $t_p = 0$ contradicts (6.7). Therefore, Case 2 cannot occur.

Case 3: If $r_p > a_p$, then $3r_p > a_p + 2r_p = v_p(2A(r-A)^2)$. Thus, by (6.11), we have $2b_p = a_p + 2r_p$, and hence a_p is even. By way of contradiction, assume that $a_p \neq 0$. Then $a_p \geq 2$, hence $2b_p = a_p + 2r_p > 2r_p$, so $b_p > r_p$. From (6.19) we have that $r_p + s_p + t_p = 2b_p > 2r_p$, so $s_p + t_p > r_p$. From (6.20) we have $r_p = s_p$. Then, from $s_p + t_p > r_p$, we deduce that $t_p > 0$.

Now, as $a_p \geq 2$ and $2a_p = c_p$, we have $c_p \geq 4$. Hence, by our simplifying assumption (1.6), $b_p \leq 2$. Therefore, from (6.19), we have $r_p + s_p + t_p \leq 4$. As $r_p = s_p$ and $t_p \geq 1$ we deduce that $2r_p \leq 3$. As r_p is odd, we have $r_p = 1$. Thus $s_p = 1$, which contradicts $s_p > t_p$. Therefore, $a_p = 0$. Thus, $2b_p = a_p + 2r_p = 2r_p$, so $b_p = r_p \equiv 1 \pmod 2$. □

Lemma 6.2. If p is an odd prime and b_p is odd then one of r_p, s_p and t_p is odd.

Proof: By way of contradiction, assume that all of r_p, s_p and t_p are even. From (6.9) we have

$$r_p + s_p + t_p = 2b_p \equiv 2 \pmod 4,$$

so without loss of generality we may suppose that $r_p \equiv 2 \pmod 4$. Then $s_p \equiv t_p \pmod 4$. From (6.8), as $r_p > 0$, we have that $s_p + t_p > 0$, so at least one of s_p and t_p is non-zero. Without loss of generality we may suppose that $s_p > 0$. Moreover, since

$s_p \equiv t_p \pmod 4$, we have from (6.15) that

$$r_p + v_p(s - A + t - A) \equiv 2 + v_p(s - A + t - A) \equiv 0 \pmod 4,$$

thus $v_p(s-A+t-A) \equiv 2 \pmod 4$ and is therefore non-zero. If $t_p = 0$ then $v_p(s-A+t-A) = 0$, a contradiction, so $t_p > 0$. By (6.7),

$$r - A + s - A + t - A = -2A,$$

hence, as r_p, s_p and t_p are all even and non-zero, we have that $p^2|A$, so $a_p \geq 2$. Then, by (6.10), we have that $c_p \geq 4$. We also have from (6.9) that

$$2b_p = r_p + s_p + t_p \geq 2 + 2 + 2 = 6,$$

so $b_p \geq 3$. Having $a_p \geq 2$, $b_p \geq 3$ and $c_p \geq 4$ contradicts our simplifying assumption (1.6). Therefore, at least one of r_p, s_p, and t_p is odd. □

From Lemmas 6.1 and 6.2, we have the following:

Lemma 6.3. If p is an odd prime, then one of r_p, s_p or t_p is odd if and only if b_p is odd.

The proof of the following theorem follows exactly as in Theorem 3.1, simply replacing Lemma 3.4 with Lemma 6.3 in the proof.

Theorem 6.1. Let K be a bicyclic quartic field. Suppose that $K = \mathbb{Q}(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$ and A, B, C are integers satisfying (1.3), (1.4), (1.5), (1.6), $AB \neq 0$ and $A^2 - 4C = 0$. Then the odd part $f_0(K)$ of the conductor $f(K)$ is given by

$$f_0(K) = \prod_{\substack{p \neq 2 \text{ (prime)} \\ b_p \text{ odd}}} p.$$

Proof: By (3.5) we have

$$K = \mathbb{Q}\left(\sqrt{r_1},\ \sqrt{s_1}\right).$$

By (3.6) we have

$$|r_1| = \prod_{\substack{p \text{ (prime)} \\ r_p \text{ odd}}} p, \quad |s_1| = \prod_{\substack{p \text{ (prime)} \\ s_p \text{ odd}}} p.$$

By (1.8) and (1.9) we have $f(K) = (1 \text{ or } 4)\mathrm{lcm}(r_1, s_1)$, hence

$$\begin{aligned} f_0(K) &= \mathrm{lcm}\left(\prod_{\substack{p \text{ (prime)} \neq 2 \\ r_p \text{ odd}}} p \quad \prod_{\substack{p \text{ (prime)} \neq 2 \\ s_p \text{ odd}}} p \right) \\ &= \prod_{\substack{p \text{ (prime)} \neq 2 \\ r_p \text{ or } s_p \text{ odd}}} p \\ &= \prod_{\substack{p \text{ (prime)} \neq 2 \\ \text{at least one of} \\ r_p, s_p, t_p \text{ odd}}} p, \end{aligned}$$

by (3.14). By Lemma 6.3 we have

$$\prod_{\substack{p \text{ (prime)} \neq 2 \\ b_p \text{ odd}}} p,$$

which is the asserted formula for $f_0(K)$. $\square$

6.2 The 2-Parts of the conductor and the discriminant

Recall that $a = v_2(A),\ b = v_2(B)$, and $c = v_2(C)$. We will denote

$$r_2 = v_2(r - A),\ s_2 = v_2(s - A) \text{ and } t_2 = v_2(t - A).$$

Also recall that A is even and $C = \left(\frac{A}{2}\right)^2$ is a square, so $C \equiv 0$ or $1 \pmod 4$. As $A^2 = 4C$, we have

$$2a = c + 2. \tag{6.21}$$

Similar to (6.11), we have

$$v_2\left((r - A)^3 + 2A(r - A)^2\right) = 2b. \tag{6.22}$$

From (6.22) we deduce

$$\text{if } r_2 > a + 1,\ a + 2r_2 + 1 = 2b, \tag{6.23}$$

$$\text{if } r_2 < a + 1, 3r_2 = 2b, \tag{6.24}$$

$$\text{if } r_2 = a + 1,\ 2b \geq 3r_2 = 3a + 3. \tag{6.25}$$

Similar to (6.15), we have

$$r_2 + v_2(s - A + t - A) = s_2 + t_2. \tag{6.26}$$

First, we address the case $C \equiv 0 \pmod 4$. We establish that this case cannot occur. As $A^2 = 4C$, we have that $16|A^2$, thus $4|A$, so $a \geq 2$. Moreover, by (6.21) we have $c = 2a - 2$. If $a \geq 3$, then $c \geq 6 - 2 = 4$. From (6.4) and (6.5) we have $r + s + t \equiv 0 \pmod 8$ and $rs + st + rt \equiv 0 \pmod 8$. By Proposition (4.1) (iii) we have $r \equiv s \equiv t \equiv 0 \pmod 4$, so

$r - A \equiv s - A \equiv t - A \equiv 0 \pmod 4$. By (6.9) we then have $2b \geq 6$, so $b \geq 3$. This contradicts our simplifying assumption (1.6), thus a cannot be at least 3. Therefore, $a = 2$.

We again address the three cases that arise from (6.22):

Case 1: $r_2 > 3$.

Case 2: $r_2 < 3$.

Case 3: $r_2 = 3$.

If $r_2 > 3$, then by (6.23) $2b = 3 + 2r_2$, a contradiction. If $r_2 < 3$, then by (6.24) we have $3r_2 = 2b$. By (6.9), we have that

$$s_2 + t_2 = 2r_2. \tag{6.27}$$

From (6.26) we then have that

$$v_2(s - A + t - A) = s_2 + t_2 - r_2 = r_2. \tag{6.28}$$

If $s_2 \neq t_2$, then without loss of generality we may suppose that $s_2 > t_2$. Then, by (6.28) we have

$$r_2 = v_2(s - A + t - A) = t_2.$$

Then, from (6.27), we have $s_2 = r_2$. Hence $s_2 = t_2$, contradicting $s_2 > t_2$. Thus $s_2 = t_2$. But then from (6.28) we have $r_2 = v_2(s - A + t - A) > s_2$. On the other hand, by (6.27) we have

$$2r_2 = s_2 + t_2 = 2s_2,$$

so $r_2 = s_2$. This is clearly a contradiction. Therefore, the case where $r_2 < 3$ cannot occur.

If $r_2 = 3$, then by (6.25) we have that

$$2b \geq 3r_2 = 9,$$

so $2b \geq 10$. From (6.9) we have

$$r_2 + s_2 + t_2 = 2b,$$

so as r_2 is odd, we deduce

$$s_2 + t_2 \equiv 1 \pmod{2}.$$

Without loss of generality, we may assume that $s_2 > t_2$, so $v_2(s - A + t - A) = t_2$. From (6.26) we have

$$r_2 + t_2 = s_2 + t_2,$$

so $s_2 = r_2 = 3$ and $3 > t_2$. Therefore, from (6.9) we have

$$10 \leq 2b = r_2 + s_2 + t_2 = 6 + t_2 < 9,$$

a contradiction. As each possible value for r_2 results in a contradiction when $C \equiv 0 \pmod{4}$, we conclude that the case $C \equiv 0 \pmod{4}$ cannot occur.

Now we examine the case $C \equiv 1 \pmod{4}$. Recall Corollary 2.2:

Corollary 2.2. Let $r - A = r_1x^2$, $s - A = s_1y^2$ and $t - A = t_1z^2$ where r_1, s_1 and t_1 are square-free integers and x, y and z are non-negative integers. When $B \neq 0$, let $r - A = r_1x^2$, $s - A = s_1y^2$, $t - A = t_1z^2$ where r_1, s_1 and t_1 are square-free integers and x, y and z are non-negative integers. Then, up to a permutation of r, s and t, we have

(A) If $r_1s_1t_1 \equiv 0 \pmod 2$, then $\alpha = 3$. Furthermore, if we have $r_1 \equiv 1 \pmod 4$ or $s_1 \equiv t_1 \equiv 2$ or $6 \pmod 8$, then $\beta = 6$; otherwise, $r_1 \equiv 3 \pmod 4$, $(s_1, t_1) \equiv (2, 6) \pmod 8$ and $\beta = 8$.

(B) If all of r_1, s_1 or t_1 are odd and at most one of r_1, s_1 or t_1 is congruent to 1 modulo 4, then $\alpha = 2$.

(C) If $r_1 \equiv s_1 \equiv t_1 \equiv 1 \pmod 4$, then $\alpha = 0$.

As $A^2 = 4C \equiv 4 \pmod{16}$, we have $A \equiv 2 \pmod 4$. From (6.4) and (6.5), we have the following congruences:

$$r + s + t = A \equiv 2 \pmod 4,$$
$$rs + st + rt = -4C \equiv 12 \pmod{16}.$$

Thus $r, s, t \equiv 2 \pmod 4$ by Proposition 4.1(viii).

We need to examine r, s and t modulo higher powers of 2 as, since we have that $r - A, s - A, t - A \equiv 0 \pmod 4$, we cannot obtain the relevant information about r_1, s_1 and t_1 required to determine α without knowing the parity of r_2, s_2 and t_2. If $A \equiv 2 \pmod 8$ then (6.4) gives

$$r + s + t \equiv 2 \pmod 8.$$

As $r \equiv s \equiv t \equiv 2 \pmod 4$, we deduce up to a permutation of r, s and t that

$$(r, s, t) \equiv (2, 2, 6) \text{ or } (6, 6, 6) \pmod 8.$$

Similarly, if $A \equiv 6 \pmod 8$, we have

$$(r, s, t) \equiv (2, 2, 2) \text{ or } (6, 6, 2) \pmod 8.$$

From (6.8) and (6.9), we have

$$-(t - A)(r - A + s - A) = (r - A)(s - A) = \frac{B^2}{t - A},$$

so that

$$-(r - A + s - A) = \left(\frac{B}{t - A}\right)^2.$$

Therefore, $v_2(r - A + s - A)$ is even. We now dispose of some of the subcases that do not occur.

If $A \equiv 2 \pmod 8$ and $(r, s, t) \equiv (6, 6, 6) \pmod 8$, then

$$r - A \equiv s - A \equiv t - A \equiv 2 \pmod 4.$$

By (6.8) we have

$$-(t - A)(r - A + s - A) = (r - A)(s - A), \tag{6.29}$$

$$-(r - A)(s - A + t - A) = (s - A)(t - A), \tag{6.30}$$

$$-(s - A)(r - A + t - A) = (r - A)(t - A). \tag{6.31}$$

Since $r - A \equiv s - A \equiv 4 \pmod 8$, we have that $8|(r - A + s - A)$, therefore we conclude that $32|(t - A)(r - A + s - A)$. However, $16\|(r - A)(s - A)$, thus (6.29) gives a contradiction. Therefore this case cannot occur.

If $A \equiv 6 \pmod 8$, $(r, s, t) \equiv (2, 2, 2) \pmod 8$, then we again have

$$r - A \equiv s - A \equiv t - A \equiv 4 \pmod 8,$$

and the same contradiction as above arises. Therefore, we have exactly two cases to consider, namely:

Case (i): $A \equiv 2 \pmod 8$, $(r, s, t) \equiv (2, 2, 6) \pmod 8$, and
Case (ii): $A \equiv 6 \pmod 8$, $(r, s, t) \equiv (6, 6, 2) \pmod 8$.

In both cases, we note that $r - A \equiv s - A \equiv 0 \pmod 8$ and that $t_2 = 2$. From (6.29), we have that

$$v_2(r - A + s - A) = r_2 + s_2 - t_2. \tag{6.32}$$

If $r_2 > s_2$, then $v_2(r - A + s - A) = s_2$. But then we have $r_2 - t_2 = 0$, a contradiction as $r_2 > t_2$. Thus $r_2 = s_2$. By (6.9), we then have $2 + 2r_2 = 2b$. Since $r - A \equiv 0 \pmod 8$, we have $r_2 \geq 3$, thus $2b \geq 2 + 6 = 8$, so $b \geq 4$ and $b = r_2 + 1$. If b is even, then r_2 is odd, thus $\alpha = 3$. Otherwise, when b is odd we have $b \geq 5$.

We wish to deduce β when b is even and $\alpha = 3$. In both cases (i) and (ii), we have that $r \equiv s \pmod{16}$; were this not the case, then up to permutation of r and s we would have $r - A \equiv 0 \pmod{16}$ and $s - A \equiv 8 \pmod{16}$, a contradiction as $r_2 = s_2$. Therefore, $r \equiv s \pmod{16}$. Note in both cases that $t - A \equiv 4 \pmod 8$, so $\frac{t-A}{4} \equiv t_1 \pmod 4$. Thus, determining $t - A$ modulo 16 will allow us to deduce β by Corollary 2.2 (A). From (6.7), if $A \equiv 2 \pmod 8$, then

$$r - A + s - A + t - A \equiv 12 \pmod{16}.$$

As $r \equiv s \equiv 2 \pmod 8$ we have $r - A \equiv s - A \equiv 0$ or $8 \pmod{16}$. In either case, (6.7) yields $t - A \equiv 12 \pmod{16}$, so $\frac{t-A}{4} \equiv 3 \pmod 4$, thus $\beta = 8$. If $A \equiv 6 \pmod 8$, then (6.7) yields

$$r - A + s - A + t - A \equiv 4 \pmod{16}.$$

As $r \equiv s \equiv 6 \pmod 8$ we have $r - A \equiv s - A \equiv 0$ or $8 \pmod{16}$. In either case, (6.7) yields $t - A \equiv 12 \pmod{16}$, so $\frac{t-A}{4} \equiv 3 \pmod 4$, thus $\beta = 8$. Therefore, if b is even, we have that $\beta = 8$.

Suppose now that b is odd and $b \geq 5$.

Case (i): As $A \equiv 2 \pmod 8$, we have that $r - A \equiv s - A \equiv 0 \pmod 8$ and $t - A \equiv 4 \pmod 8$. As $-2A \equiv 12 \pmod{16}$, analyzing (6.7), up to permutation of r and s we have that

$$(r - A, s - A, t - A) \equiv (0, 0, 12),\ (0, 8, 4) \text{ or } (8, 8, 12) \pmod{16}.$$

Since b is odd, $b = r_1 + 1$, and $r_2 = s_2$, we have that r_2 and s_2 are even. Thus the possibilities $(0, 8, 4)$ and $(8, 8, 12)$ modulo 16 do not occur as $s_2 = 3$ in these cases. Therefore,

$$(r - A, s - A, t - A) \equiv (0, 0, 12) \pmod{16}.$$

Since $\frac{t-A}{4} \equiv 3 \pmod 4$, we have by Corollary 2.2 (C) that $\alpha \neq 0$. Since $r_2, s_2 \equiv 0 \pmod 2$ and $t_2 = 2$, we have by Corollary 2.2 (A) that $\alpha \neq 3$. Therefore, $\alpha = 2$.

Case (ii): If $A \equiv 6 \pmod 8$ then $-2A \equiv 4 \pmod{16}$. With $t - A \equiv 4 \pmod 8$ and

$r - A \equiv s - A \equiv 0 \pmod 8$, analyzing (6.7) yields solutions

$$(r - A, s - A, t - A) \equiv (0, 0, 4),\ (0, 8, 12),\ (8, 8, 4) \pmod{16}.$$

Again, solutions with $s_2 \equiv 1 \pmod 2$ are invalid as $b = r_2 + 1$ is odd and $r_2 = s_2$. Thus

$$(r - A, s - A, t - A) \equiv (0, 0, 4) \pmod{16}.$$

Letting $k = r_2$, $r_0 = \frac{r-A}{2^k}$, $s_0 = \frac{s-A}{2^k}$, we have from (6.29) that

$$-(t - A)(r_0 + s_0) = r_0(s - A).$$

Since $t_2 \equiv s_2 \equiv 0 \pmod 2$, we have that $v_2(r_0 + s_0) \equiv 0 \pmod 2$. Since r_0 and s_0 are both odd, we have that $r_0 \not\equiv s_0 \pmod 4$. Letting $t_0 = \frac{t-A}{2^{t_2}}$, since $t - A \equiv 4 \pmod{16}$ we have that $t_0 \equiv 1 \pmod 4$. Thus, we have from (6.9) that

$$3 \equiv r_0 s_0 t_0 \equiv 1 \pmod 4,$$

a contradiction. Thus, this case does not occur.

Using the above analysis of the 2-part of $f(K)$ and Theorem 6.1, we deduce our desired result.

Theorem 6.2 (Main Case 2)**.** Let K be a bicyclic quartic field. Suppose that $K = \mathbb{Q}(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$ and A, B, C are integers satisfying (1.3), (1.4), (1.5), (1.6), $AB \neq 0$ and $A^2 - 4C = 0$. Then C is odd and $f(K) = 2^\alpha f_0(K)$, where

$$f_0(K) = \prod_{\substack{p \text{ (prime)} \neq 2 \\ v_p(B) \text{ odd}}} p,$$

such that

$$\alpha = \begin{cases} 2, & \text{if } v_2(B) \equiv 1 \pmod{2}, \\ 3, & \text{if } v_2(B) \equiv 0 \pmod{2}. \end{cases}$$

Moreover, $d(K) = 2^{\beta}\,(f_0(K))^2$, where

$$\beta = \begin{cases} 4, & \text{if } v_2(B) \equiv 1 \pmod{2}, \\ 8, & \text{if } v_2(B) \equiv 0 \pmod{2}, \end{cases}$$

Chapter 7

Main Case 3: $A \neq 0,\ B = 0$

The resolvent cubic of $x^4 + Ax^2 + Bx + C$ is $x^3 - Ax^2 - 4Cx + (4AC - B^2)$. With $B = 0$, the resolvent cubic becomes

$$x^3 - Ax^2 - 4Cx + 4AC = (x - A)(x^2 - 4C).$$

Denoting the roots of the resolvent cubic as r, s and t, without loss of generality we have

$$r = A,\ s = 2\sqrt{C},\ t = -2\sqrt{C}, \tag{7.1}$$

so that $t = -s$. From (1.13) we have $C \neq 0$, thus $s \neq 0$. As s is a non-zero integer, we deduce

$$C = \left(\frac{s}{2}\right)^2 > 0.$$

As C is an integer which is the square of a rational number, it must be the square of an integer.

We next show that

$$A^2 - 4C \neq 0. \tag{7.2}$$

Suppose $A^2 = 4C$. Then A is even and $C = \dfrac{A^2}{4}$. Therefore,

$$g(x) = x^4 + Ax^2 + \frac{A^2}{4} = \left(x^2 + \frac{A}{2}\right)^2$$

is reducible in $\mathbb{Z}[X]$, contradicting (1.4). As a consequence of (7.2), we have

$$A \neq \pm 2\sqrt{C}. \tag{7.3}$$

Let

$$\tau = \frac{1}{2}\left(\sqrt{-A + 2\sqrt{C}} - \sqrt{-A - 2\sqrt{C}}\right).$$

Then

$$\tau^2 = \frac{1}{2}\left(-A - \sqrt{-A + 2\sqrt{C}}\,\sqrt{-A - 2\sqrt{C}}\right)$$

so that for some $\varepsilon = \pm 1$ we have

$$\begin{aligned}\tau^2 &= \frac{1}{2}\left(-A + \varepsilon\sqrt{\left(-A + 2\sqrt{C}\right)\left(-A - 2\sqrt{C}\right)}\right)\\ &= \frac{1}{2}\left(-A + \varepsilon\sqrt{A^2 - 4C}\right).\end{aligned}$$

Hence

$$\begin{aligned}4\tau^4 + 4A\tau^2 + A^2 &= (2\tau^2 + A)^2\\ &= \left(\varepsilon\sqrt{A^2 - 4C}\right)^2\\ &= A^2 - 4C,\end{aligned}$$

and thus

$$\tau^4 + A\tau^2 + C = 0.$$

Hence τ is a root of $g(x)$. All four roots of $g(x)$ are

$$\tau_1 = \frac{1}{2}\left(\sqrt{-A + 2\sqrt{C}} - \sqrt{-A - 2\sqrt{C}}\right),$$
$$\tau_2 = \frac{1}{2}\left(\sqrt{-A + 2\sqrt{C}} + \sqrt{-A - 2\sqrt{C}}\right),$$
$$\tau_3 = \frac{1}{2}\left(-\sqrt{-A + 2\sqrt{C}} - \sqrt{-A - 2\sqrt{C}}\right),$$
$$\tau_4 = \frac{1}{2}\left(-\sqrt{-A + 2\sqrt{C}} + \sqrt{-A - 2\sqrt{C}}\right).$$

As $g(x)$ is irreducible of degree 4, we have

$$\text{neither } -A + 2\sqrt{C} \text{ nor } -A - 2\sqrt{C} \text{ is the square of an integer.} \tag{7.4}$$

This agrees with the deduction of Kappe and Warren [33, Theorem 2].

We now need to determine the subfield lattice of K.

Lemma 7.1. When $A \neq 0$ and $B = 0$, $\mathbb{Q}\left(\sqrt{-A + 2\sqrt{C}}\right)$ and $\mathbb{Q}\left(\sqrt{-A - 2\sqrt{C}}\right)$ are distinct quadratic subfields of K.

Proof: As $A \neq 0$ and C is a non-zero perfect square, we have that $-A+2\sqrt{C}$ and $-A-2\sqrt{C}$ are distinct integers, neither of which is a perfect square by (7.4). Thus $\mathbb{Q}\left(\sqrt{-A + 2\sqrt{C}}\right)$ and $\mathbb{Q}\left(\sqrt{-A - 2\sqrt{C}}\right)$ are quadratic fields. We now show that they are distinct fields. By way of contradiction, we assume that

$$\mathbb{Q}\left(\sqrt{-A + 2\sqrt{C}}\right) = \mathbb{Q}\left(\sqrt{-A - 2\sqrt{C}}\right).$$

Then there exist non-zero integers j and k such that

$$j^2\left(-A+2\sqrt{C}\right)=k^2\left(-A-2\sqrt{C}\right).$$

Equivalently, $-A+2\sqrt{C} = \frac{k^2}{j^2}\left(-A-2\sqrt{C}\right)$. But then $\tau_1 = \frac{1-k}{2j}\sqrt{-A+2\sqrt{C}}$, which is algebraic of degree 2 over $\mathbb{Q}$, a contradiction as the minimal polynomial of τ_1 is of degree 4. Thus $\mathbb{Q}\left(\sqrt{-A+2\sqrt{C}}\right) \neq \mathbb{Q}\left(\sqrt{-A-2\sqrt{C}}\right)$. As $\sqrt{-A+2\sqrt{C}} = \tau_1+\tau_2 \in K$ and $\sqrt{-A-2\sqrt{C}} = \tau_1-\tau_2 \in K$, we have that these elements lie in K, thus they generate two distinct quadratic subfields of K. $\square$

Corollary 7.1. Let $l = v_2(A^2-4C)$, $K_1=\mathbb{Q}\left(\sqrt{-A+2\sqrt{C}}\right)$, $K_2=\mathbb{Q}\left(\sqrt{-A-2\sqrt{C}}\right)$, $-A+2\sqrt{C} = c_+x^2$ and $-A-2\sqrt{C} = c_-y^2$ where c_+ and c_- are square-free. When $A \neq 0$ and $B=0$, then

(A) If $l \equiv 0 \pmod 2$ then $\mathbb{Q}\left(\sqrt{E}\right)$ is a quadratic subfield of K different from K_1 and K_2.

(B) If $l \equiv 1 \pmod 2$ then $\mathbb{Q}\left(\sqrt{2E}\right)$ is a quadratic subfield of K different from K_1 and K_2. Moreover, exactly one of c_+ and c_- is odd.

Proof: As K_1 and K_2 are distinct quadratic subfields of K by Lemma 7.1, we have that $\sqrt{(-A-2\sqrt{C})(-A+2\sqrt{C})} = \sqrt{A^2-4C}$ generates the third distinct quadratic subfield of K, hence $K_3 = \mathbb{Q}\left(\sqrt{A^2-4C}\right)$ is the third distinct quadratic subfield of K. Let $A^2-4C = x^2E_1$ where E_1 is square-free and x is an integer. Clearly $K_3 = \mathbb{Q}\left(\sqrt{E_1}\right)$. We have

$$x^2E_1 = A^2-4C = 2^lE. \tag{7.5}$$

If l is even, then as $v_2(x^2)$ is even and $v_2(E_1) \leq 1$, we have that $v_2(E_1)=0$ and $v_2(x^2)=l$.

Dividing (7.5) by 2^l yields

$$\left(\frac{x}{2^{\frac{l}{2}}}\right)^2 E_1 = E$$

Therefore, we have that $E \equiv E_1 \pmod 8$, hence $K_3 = \mathbb{Q}\left(\sqrt{E}\right)$. If l is odd, then as $v_2(x^2)$ is even and $v_2(E_1) \leq 1$, we have $v_2(E_1) = 1$ and $v_2(x^2) = l - 1$. Dividing (7.5) by 2^{l-1} yields

$$\left(\frac{x}{2^{\frac{l-1}{2}}}\right)^2 E_1 = 2E.$$

Therefore, we have that $2E \equiv E_1 \pmod 8$, hence $K_3 = \mathbb{Q}\left(\sqrt{2E}\right)$. As $2E_1$ is even, squarefree and $K_3 = \mathbb{Q}\left(\sqrt{2E}\right)$, we have by Lemma 1.4 that exactly one of c_+ and c_- is odd. □

The Conductor $f(K)$ and Discriminant $d(K)$

From Lemma 7.1, note that

$$f_0(K) = \prod_{v_p\left(-A+2\sqrt{C}\right) \text{ or } v_p\left(-A-2\sqrt{C}\right) \text{ odd}} p$$

since $v_p(A^2 - 4C)$ is odd if and only if exactly one of $v_p\left(-A + 2\sqrt{C}\right)$ or $v_p\left(-A - 2\sqrt{C}\right)$ is odd by (1.8) and $A^2 - 4C$, $-A + 2\sqrt{C}$ and $-A - 2\sqrt{C}$ generate the three distinct quadratic subfields of K.

In determining $\alpha = v_2(f(K))$, we again search for the following conditions as per Theorem 1.2: if at least one of $v_2\left(-A + 2\sqrt{C}\right), v_2\left(-A - 2\sqrt{C}\right)$ or $v_2(A^2-4C)$ is odd, then $\alpha = 3$; otherwise, if one of the odd parts of $-A+2\sqrt{C}$ or $-A-2\sqrt{C}$ are congruent to 3 modulo 4, then $\alpha = 2$, but if both are congruent to 1 modulo 4, then $\alpha = 0$.

Let A be odd. If $\sqrt{C}$ is even, then $-A + 2\sqrt{C} \equiv -A - 2\sqrt{C} \equiv -A \pmod 4$, thus

$$\alpha = \begin{cases} 2, & A \equiv 1 \pmod 4, \\ 0, & A \equiv 3 \pmod 4. \end{cases}$$

If C is odd, then $2\sqrt{C} \equiv 2 \pmod 4$, thus $-A + 2\sqrt{C} \equiv -2\sqrt{C} - 4 \equiv 2 - A \pmod 4$. Therefore,

$$\alpha = \begin{cases} 0, & A \equiv 1 \pmod 4, \\ 2, & A \equiv 3 \pmod 4. \end{cases}$$

Let A and $\sqrt{C}$ be even. Note that if A and $\sqrt{C}$ are 0 modulo 4, then $2^2|A$ and $2^4|C$, contradicting our simplifying assumption. Thus, for the following scenarios, we have that $2\sqrt{C} \equiv 4 \pmod 8$.

If $A \equiv 2 \pmod 4$, then $-A + 2\sqrt{C} \equiv -A \equiv 2 \pmod 4$, thus $\alpha = 3$. As $-A + 2\sqrt{C} \equiv -A - 2\sqrt{C} \equiv 2 \pmod 4$ and

$$-A + 2\sqrt{C} + -A - 2\sqrt{C} = -2A \equiv 4 \pmod 8,$$

we have $-A + 2\sqrt{C} \equiv -A - 2\sqrt{C} \pmod 8$. Therefore, by Theorem 1.2 and Lemma 7.1, we have that $\beta = 6$.

If $A \equiv 0 \pmod 8$, then $-A + 2\sqrt{C} \equiv 4 \pmod 8$. If $-A + 2\sqrt{C} \equiv 4 \pmod{16}$, then $2\sqrt{C} \equiv A + 4 \pmod{16}$, thus $-A - 2\sqrt{C} \equiv -2A - 4 \equiv -4 \equiv 12 \pmod{16}$. Thus, $\frac{-A-2\sqrt{C}}{4} \equiv 3 \pmod 4$ and $\frac{-A+2\sqrt{C}}{4} \equiv 1 \pmod 4$, hence $\alpha = 2$. If we have that $-A + 2\sqrt{C} \equiv 12 \pmod{16}$, then a similar argument will establish that $\frac{-A-2\sqrt{C}}{4} \equiv 1 \pmod 4$ and clearly $\frac{-A+2\sqrt{C}}{4} \equiv 3 \pmod 4$, therefore $\alpha = 2$ in either scenario.

If $A \equiv 4 \pmod 8$, then $-A + 2\sqrt{C} \equiv 0 \pmod 8$. If $-A + 2\sqrt{C} \equiv 0 \pmod{16}$, then

$2\sqrt{C} \equiv A \pmod{16}$, thus $-A - 2\sqrt{C} \equiv 2A \equiv 8 \pmod{16}$, thus $v_2\left(-A - 2\sqrt{C}\right)$ is odd, hence $\alpha = 3$. If $-A + 2\sqrt{C} \equiv 8 \pmod{16}$, we have that $v_2\left(-A + 2\sqrt{C}\right)$ is odd and so $\alpha = 3$ in either scenario. We may then assume, without loss of generality, that $-A + 2\sqrt{C} \equiv 0 \pmod{16}$ and $-A - 2\sqrt{C} \equiv 8 \pmod{16}$. By Lemma 7.1, if l is odd, we have that c_+ is odd as c_- is even, thus

$$\beta = \begin{cases} 6, & c_+ \equiv 1 \pmod 4, \\ 8, & c_+ \equiv 3 \pmod 4. \end{cases}$$

When l is even, we have

$$\beta = \begin{cases} 6, & E \equiv 1 \pmod 4, \\ 8, & E \equiv 3 \pmod 4. \end{cases}$$

Now, let C be odd while A is even. If $A \equiv 0 \pmod 4$, we have that $-A + 2\sqrt{C} \equiv -A - 2\sqrt{C} \equiv 2 \pmod 4$, thus $\alpha = 3$. As

$$-A + 2\sqrt{C} + -A - 2\sqrt{C} = -2A \equiv 0 \pmod 8,$$

we have $-A + 2\sqrt{C} \not\equiv -A - 2\sqrt{C} \pmod 8$. Therefore, by Lemma 7.1 and Theorem 1.2, we have that $\beta = 8$.

Finally, we address the case where $A \equiv 2 \pmod 4$ and C is odd. Note that $-A + 2\sqrt{C} \equiv -A - 2\sqrt{C} \equiv 0 \pmod 4$. If $v_2\left(-A + 2\sqrt{C}\right) \equiv 1 \pmod 2$ or $v_2\left(-A - 2\sqrt{C}\right) \equiv 1 \pmod 2$, then $\alpha = 3$ by Theorem 1.2 and Lemma 7.1. We have that $-A + 2\sqrt{C} \equiv -A - 2\sqrt{C} \equiv 0 \pmod 4$ and

$$-A + 2\sqrt{C} + -A - 2\sqrt{C} \equiv -2A \equiv 4 \pmod 8. \tag{7.6}$$

Without loss of generality, suppose that $v_2\left(-A - 2\sqrt{C}\right) \equiv 1 \pmod 2$, so that

$-A+2\sqrt{C} \equiv 4 \pmod 8$ and $-A-2\sqrt{C} \equiv 0 \pmod 8$. By Theorem 1.2 and Lemma 7.1, we have

$$\beta = \begin{cases} 6, & \frac{-A+2\sqrt{C}}{4} \equiv 1 \pmod 4, \\ 8, & \frac{-A+2\sqrt{C}}{4} \equiv 3 \pmod 4; \end{cases}$$

that is,

$$\beta = \begin{cases} 6, & -A+2\sqrt{C} \equiv 4 \pmod{16}, \\ 8, & -A+2\sqrt{C} \equiv 12 \pmod{16}. \end{cases}$$

Now, suppose that $v_2\left(-A+2\sqrt{C}\right) \equiv v_2\left(-A-2\sqrt{C}\right) \equiv 0 \pmod 2$. If $-A+2\sqrt{C} \equiv 0 \pmod 8$, then $2\sqrt{C} \equiv A \pmod 8$, hence

$$-A-2\sqrt{C} \equiv -2A \equiv 4 \pmod 8.$$

Similarly, if $-A+2\sqrt{C} \equiv 4 \pmod 8$, we have that $-A-2\sqrt{C} \equiv 0 \pmod 8$. Thus, our arguments for when $-A+2\sqrt{C} \equiv 0 \pmod 8$ and $-A+2\sqrt{C} \equiv 4 \pmod 8$ will be identical, where the second case is simply the first case with $2\sqrt{C}$ interchanged with $-2\sqrt{C}$.

Assume $-A+2\sqrt{C} \equiv 0 \pmod 8$. Modulo 16, as $v_2\left(-A+2\sqrt{C}\right)$ is even, we must have that $-A+2\sqrt{C} \equiv 0 \pmod{16}$. Thus, as $A \equiv 2\sqrt{C} \pmod{16}$, we have that $-A-2\sqrt{C} \equiv -2A \pmod{16}$. If $A \equiv 2 \pmod 8$, then we have that $-2A \equiv 12 \pmod{16}$, thus $\alpha = 2$. If $A \equiv 6 \pmod 8$, then $-A-2\sqrt{C} \equiv 4 \pmod{16}$, thus $c_- \equiv 1 \pmod 4$. Thus, α is explicitly determined by c_+ as follows:

$$\alpha = \begin{cases} 0, & c_+ \equiv 1 \pmod 4, \\ 2, & c_+ \equiv 3 \pmod 4. \end{cases}$$

Therefore, we have the following result:

Theorem 7.1 (Main Case 3)**.** Let K be a bicyclic quartic field. Suppose that $K = \mathbb{Q}(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$ and A, B, C are integers satisfying (1.3), (1.4), (1.5), (1.6) and $A \neq 0,\ B = 0$. Then C is the square of a non-zero integer and $f(K) = 2^\alpha f_0(K)$, where

$$f_0(K) = \prod_{\substack{p \text{ (prime)} \neq 2 \\ v_p(-A+2\sqrt{C}) \text{ or } v_p(-A-2\sqrt{C}) \text{ odd}}} p$$

and the values of α are given in Tables 3 and 4 in Appendix A. Moreover, $d(K) = 2^\beta\,(f_0(K))^2, \beta$ is given in Tables 3 and 4 in Appendix A.

Main Case 3 is a special case of the trinomials $x^n + Ax^s + B$ ($n = 4$ and $s = 2$) considered by Llorente, Nart and Vila [36]. Theorem 7.1 agrees numerically with the results of [36].

Example 1: $g(x) = x^4 + 2x^2 + 4$. Here, we have that $A = 2$, $C = 4$ and $A^2 - 4C = -12 = -2^2 \cdot 3$. Thus Theorem 7.1 yields $f_0(K) = 3$ and $\beta = 6$ from Table 3 in Appendix A, so $d(K) = 2^6 \cdot 3^2 = 576$. In the notation of [36], we have $D = 9216 = 2^{10} \cdot 3^2$, so the only primes which need checking are 2 and 3. We perform this check in the table below.

$p = 2$	$p = 3$
$A_2 = 1$	$A_3 = 2$
$B_2 = 1$	$B_3 = 4$
$t_2 = 0$	$t_3 = 1$
$M_2 = 0$	$M_3 = 0$
$a_2 = 1$	$a_3 = 2$
$b_2 = 2$	$b_3 = 4$
$c_2 = 1$	$c_3 = 2$
$z_2 = 1$	$z_3 = 2$
$\delta = b_2 = 2$	$\delta = b_3 - z_3 = 2$
$v_2(d) = 4 \cdot 1 + 4 - 2 = 6$	$v_3(d) = 4 \cdot 0 + 4 - 2 = 2$

from which [36] concludes $d(K) = 2^6 \cdot 3^2 = 576$, agreeing with Theorem 7.1.

Example 2: $g(x) = x^4 + 10x^2 + 36$. Here $A = 10$, $C = 36$ and $A^2 - 4C = -44 = -4 \cdot 11$. Thus Theorem 7.1 implies $11 \mid f_0(K)$ and $\beta = 6$ from Table 3 in Appendix A, therefore $d(K) = 2^6 \cdot 11^2 = 7744$. In the notation of [36], we have $D = 1115136 = 2^{10} \cdot 3^2 \cdot 11^2$, so we need only check the primes 2, 3 and 11.

$p = 2$	$p = 3$	$p = 11$
$A_2 = 5$	$A_3 = 10$	$A_{11} = 10$
$B_2 = 9$	$B_3 = 4$	$B_{11} = 36$
$t_2 = 0$	$t_3 = 1$	$t_{11} = 1$
$M_2 = 0$	$M_3 = 4$	$M_{11} = 0$
$a_2 = 1$	$a_3 = 2$	$a_{11} - 2$
$b_2 = 2$	$b_3 = 2$	$b_{11} = 4$
$c_2 = 1$	$c_3 = 2$	$c_{11} = 2$
$z_2 = 1$	$z_3 = 2$	$z_{11} = 2$
$\delta = b_2 = 2$	$\delta = 2 + 2 - \inf\{4, \max\{0, 0\}\} = 4$	$\delta = b_{11} - z_{11} = 2$
$v_2(d) = 4 \cdot 1 + 4 - 2 = 6$	$v_3(d) = 4 \cdot 0 + 4 - 4 = 0$	$v_1 1(d) = 4 \cdot 0 + 4 - 2 = 2$

Therefore, this method concludes that $d(K) = 2^6 \cdot 11^2 = 7744$, which agrees with our result.

As it is noted in the literature (see, for example, [2]), the results of [36] do not cover all cases of quartic trinomials of the form $x^4 + Ax + B$; it is indeed the case here as well. We present two further examples to illustrate this and compute the discriminants in these examples.

Example 3: $g(x) = x^4 + 6x^2 + 1$. For the prime $p = 2$, in the notation of [36] we have

$$M_2 = -4,\ a_2 = 1,\ b_2 = 4,\ c_2 = 1,\ z_2 = 1.$$

From here, as $M_2 < -0$, we have that $2 \mid b_2$, $b_2 = -M_2$ and $2 \nmid \frac{n}{b_2}$, so the hypothesis of [36, Theorem 1] is not satisfied by $p = 2$. Therefore, the results of [36] cannot be used here.

From our result, we have that $A = 6$, $C = 1$ and $A^2 - 4C = 32 = 2^5$, so no odd primes divide $d(K)$. From Table 4 of Appendix A, since $-A + 2\sqrt{C} = -4$ and $-A - 2\sqrt{C} = -6$, $v_2(-A - 2\sqrt{C})$ is odd and we have $-A + 2\sqrt{C} = -1 \equiv 3 \pmod 4$, so $\beta = 8$. Therefore, $d(K) = 2^8 = 256$. We obtain the same result in Maple.

Example 4: $g(x) = x^4 + 3x^2 + 16$. For the prime $p = 2$, in the notation of [36] we have

$$M_2 = 8,\ a_2 = 2,\ b_2 = 4,\ c_2 = 2,\ z_2 = 2.$$

From here, as $M_2 > 0$, we have that as $2 \mid b_2$ the hypothesis of [36, Theorem 1] is not satisfied by $p = 2$. Therefore, the results of [36] cannot be used here.

In using our results, we have that $A = 3$, $C = 16$ and $A^2 - 4C = -55 = -5 \cdot 11$. Thus Theorem 7.1 implies $5, 11 \mid f_0(K)$ and $\beta = 0$ from Table 3 in Appendix A, therefore $d(K) = 5^2 \cdot 11^2 = 3025$.

Chapter 8

Main Case 4: $A = 0,\ B \neq 0$

With $A = 0$, we have $g(x) = x^4+Bx+C$, thus we have that the resolvent is $q(x) = x^3 - 4Cx - B^2$. From this, we restate (2.2)-(2.4) as

$$r + s + t = 0, \tag{8.1}$$

$$rs + st + rt = -4C, \tag{8.2}$$

$$rst = B^2. \tag{8.3}$$

First, note that if $B \equiv 1 \pmod 2$, then by (8.3) we have $r \equiv s \equiv t \equiv 1 \pmod 2$, which contradicts (8.1). Therefore, B is even. From (8.1), we have

$$t = -r - s. \tag{8.4}$$

Substituting (8.4) into (8.2) yields

$$r^2 + s^2 + rs = 4C. \tag{8.5}$$

Let $r = r_1x^2$, $s = s_1y^2$, $t = t_1z^2$ for square-free integers r_1, s_1 and t_1 and positive integers x, y and z. For a given prime p, we denote $v_p(r) = r_p$, $v_p(s) = s_p$ and $v_p(t) = t_p$. As well, recall that $b_p = v_p(B)$, $c_p = v_p(C)$ and when $p = 2$ we may also write $b = v_2(B)$ and $c = v_2(C)$.

Given $A = 0$, we restate equations (2.20)-(2.22) as

$$r^3 - 4Cr = B^2, \tag{8.6}$$

$$s^3 - 4Cs = B^2, \tag{8.7}$$

$$t^3 - 4Ct = B^2. \tag{8.8}$$

We have from (8.6) that

$$r(r^2 - 4C) = B^2. \tag{8.9}$$

Comparing this with (8.3) yields

$$st = r^2 - 4C. \tag{8.10}$$

Recall from Theorems 1.2 and 2.2 and Corollary 2.2 (A) that for an odd prime p, $p \mid f(K)$ if and only if $p|r_1s_1t_1$. Moreover, $\alpha = 3$ if and only if $2 \mid r_1s_1t_1$.

Suppose that p is a prime where, without loss of generality, $p \mid r_1$. Then $p|r$ and from (8.3) we have that $p \mid B$. Since r_1 is square-free, $p \parallel r_1$ and thus r_p is odd. From (8.9) we have that

$$r_p + v_p(r^2 - 4C) = 2b_p. \tag{8.11}$$

Since r_p is odd, we must have that $v_p(r^2 - 4C)$ is odd, so $p \mid r^2 - 4C$. From here, we now split into cases for $p \geq 3$ and $p = 2$.

Lemma 8.1. Let p be an odd prime. Then $p \mid f(K)$ if and only if $p^2 \mid B$ and $p^2 \parallel C$.

Proof: $\underline{\Longrightarrow}$: Without loss of generality, we may assume $p \mid r_1$. Since $p \mid r$ and p is odd, $p \mid r^2 - 4C$ implies $p \mid C$. From (8.5), we deduce that $p \mid s$. Therefore, from (8.5) we see that $c_p \geq 2$. Moreover, since $v_p(r^2 - 4C) \geq 2$ and is odd, we have from (8.11) that $2b_p \geq 4$, so $b_p \geq 2$ and $p^2 \mid B$.

By way of contradiction, suppose that c_p is odd, so $c_p \geq 3$. Rewriting (8.9) using $r = r_1 x^2$, we obtain

$$r_1 x^2 (r_1^2 x^4 - 4C) = B^2. \tag{8.12}$$

Denote $x_p = v_p(x)$. As $v_p(r^2 - 4C)$ and c_p are odd and $v_p(r^2)$ is even, we must have that

$$c_p < 2r_p = 2 + 4x_p, \tag{8.13}$$

hence $v_p(r^2 - 4C) = c_p$. Note from (8.13) that if $x_p = 0$ then $c_p < 2$, a contradiction as $c_p \geq 2$. Therefore, $x_p \geq 1$. We have from (8.12) that

$$1 + 2x_p + c_p = 2b_p. \tag{8.14}$$

If $c_p \geq 5$, then from (8.14) we have that $2b_p \geq 1 + 2 + 5 = 8$, so $b_p \geq 4$. But then $p^3 \mid B$ and $p^4 \mid C$, contradicting our simplifying assumption (1.6). Therefore, $c_p = 3$. As $x_p \geq 1$ and $p \mid r_1$ we have that $r_p \geq 3$. As $p \mid s$ and $c_p = 3$, we have that

$$3 = v_p(r^2 + s^2 + rs).$$

As $v_p(r^2) \geq 6$ and $v_p(rs) \geq 4$, we must have that $3 = v_p(s^2)$, which is impossible. Therefore, c_p cannot be odd.

We now have that $c_p \geq 2$, c_p is even and $r_p \geq 1$. If $c_p \geq 4$ then $2r_p \geq 4$, otherwise

$v_p(r^2 - 4C)$ is even. As r_p is odd, we deduce that $r_p \geq 3$. But then from (8.11) we have that

$$2b_p = r_p + v_p(r^2 - 4C) \geq 3 + 5 = 8,$$

so $b_p \geq 4$. Therefore $p^3 \mid B$ and $p^4 \mid C$, contradicting our simplifying assumption (1.6). Therefore, $c_p = 2$, as desired.

$\underline{\Longleftarrow}$: If one of $r_p,\ s_p$ or t_p is odd, then the result holds. By way of contradiction, suppose that all of $r_p,\ s_p$ and t_p are even. From (8.6) and (8.7), we see that as $p \mid C$ and $p \mid B$, we must have $p \mid r$ and $p \mid s$, so $r_p \geq 2$ and $s_p \geq 2$. From (8.5), we see that

$$2 = v_p(4C) = v_p(r^2 + s^2 + rs) \geq 4,$$

a contradiction. Therefore, at least one of r_p, s_p and t_p is odd and thus $p \mid f(K)$. $\square$

Lemma 8.2. $\alpha = 3$ if and only if C is odd.

Proof: $\underline{\Longrightarrow}$: Without loss of generality, we may assume that $2 \mid r_1$ when $\alpha = 3$. We examine cases based on the parity of x in view of (8.12).

Case 1: x is even. We have from above that $v_2(r_1^2 x^4 - 4C)$ is odd. Therefore, as

$$v_2(r_1^2 x^4) \geq 2 + 4 = 6,$$

we must have that $v_2(4C) = 3, 5$ or $v_2(4C) \geq 6$ as $v_2(4C) \geq 2$.

If $v_2(4C) \geq 6$, then $c \geq 4$. Note from (8.12) that we have $2b \geq 3 + 7 = 10$, so $b \geq 5$. But then $2^3 \mid B$ and $2^4 \mid C$, contradicting our simplifying assumption (1.6). Therefore, $v_2(4C) < 6$.

If $v_2(4C) = 5$, examining (8.5) we have

$$v_2(r^2 + s^2 + rs) = 5.$$

As $v_2(r^2) = v_2(r_1^2 x^4) \geq 6$, we have that $v_2(s^2 + rs) = 5$. Clearly s cannot be odd in this scenario. If $v_2(s) \leq 2$, then $v_2(s^2 + rs) = v_2(s^2) \leq 4$, a contradiction. If $v_2(s) \geq 3$, then $v_2(s^2 + rs) \geq 6$, again a contradiction. Therefore, $v_2(4C) \neq 5$.

If $v_2(4C) = 3$, again examining (8.5) we have that $v_2(s^2 + rs) = 3$ as $v_2(r^2) \geq 6$. Again, clearly s is even. If $v_2(s) = 1$, then $v_2(s^2 + rs) = 2$, a contradiction. If $v_2(s) \geq 2$ then $v_2(s^2 + rs) \geq 4$, again a contradiction.

Therefore, the case where x is even cannot occur when $\alpha = 3$.

<u>Case 2: x is odd.</u> Then $v_2(r) = 1$. As $v_2(r^2 - 4C)$ must be odd, $v_2(r^2) = 2$ and $v_2(4C) \geq 2$, we must have that $v_2(4C) = 2$, otherwise $v_2(r^2 - 4C) = 2$, a contradiction. Therefore $v_2(4C) = 2$, thus C must be odd.

<u>$\Longleftarrow$:</u> As B is even, we have from (8.9) that r is even or $r^2 - 4C$ is even. Since

$$r^2 - 4C \equiv r^2 \equiv r \pmod 2,$$

we have that r must be even. From (8.10), we then have that st is even. Therefore, by (8.1), we have that all of r, s and t are even. Examining (8.5) modulo 8, we have

$$r^2 + s^2 + rs \equiv 4 \pmod 8.$$

If $4 \mid r$ and $4 \mid s$, the above congruence would yield $0 \equiv 4 \pmod 8$, a contradiction. Thus, as both r and s are even, we conclude that $v_2(r) = 1$ or $v_2(s) = 1$, so $\alpha = 3$, as desired. □

Lemma 8.3. If $\alpha \neq 3$ then $\alpha = 2$.

Proof: As $\alpha \neq 3$, we have $v_2(r_1) = v_2(s_1) = v_2(t_1) = 0$ and $v_2(r)$, $v_2(s)$ and $v_2(t)$ are all even. Let

$$\gamma = \min\{v_2(r), v_2(s), v_2(t)\}.$$

Analyzing (8.1) using $r_2 = \frac{r}{2^\gamma}$, $s_2 = \frac{s}{2^\gamma}$ and $t_2 = \frac{t}{2^\gamma}$, we have

$$r_2 + s_2 + t_2 = 0.$$

Without loss of generality, let $\gamma = v_2(t)$. Then t_2 is odd. Thus, for the above equation to hold, we must have exactly one of r_2 and s_2 odd. Without loss of generality, let s_2 be odd, so $v_2(s) = v_2(t) = \gamma$ and $v_2(r) > \gamma$.

Revisiting (8.3), we have $v_2(r) + v_2(s) + v_2(t) = 2b$, where $b = v_2(B)$. Thus, $v_2(r) = 2(b - \gamma)$, so $v_2(r) \equiv 0 \pmod 2$. Examining (8.1) again, note that since $v_2(s_1) = v_2(t_1) = 0$, we have that $s_2 = u^2 s_1$ and $t_2 = v^2 t_1$ for odd integers u and v. Therefore, $s_2 \equiv s_1$ and $t_2 \equiv t_1$ modulo 4. Since γ is even and $v_2(r_2) > 0$, we have that $v_2(r_2) \geq 2$. Therefore, (8.1) yields

$$0 = r_2 + s_2 + t_2 \equiv s_2 + t_2 \pmod 4,$$

thus $s_2 \not\equiv t_2 \pmod 4$. Therefore, without loss of generality, $s_2 \equiv 3 \pmod 4$, so $\alpha \neq 0$ by Corollary 2.2 (C). Therefore, $\alpha = 2$ by Corollary 2.2 (B). □

Lemma 8.4. When $\alpha = 3$,

$$\beta = \begin{cases} 6, & \text{if } b = 2, \\ 8, & \text{if } b \geq 3. \end{cases}$$

Proof: Suppose $\alpha = 3$, so C is odd by Lemma 8.2. As $\alpha = 3$, by Corollary 2.2 (A) we have that exactly two of $v_2(r)$, $v_2(s)$ and $v_2(t)$ are odd. From the proof of Lemma 8.4, we have without loss of generality that

$$v_2(r) > \gamma = \min\{v_2(r), v_2(s), v_2(t)\} = v_2(s) = v_2(t),$$

so γ must be odd and $v_2(r)$ must be even. From (8.2), we have

$$rs + st + rt = -4C,$$

so $r(s+t)+st = -4C$. As $v_2(r) > v_2(s)$ and $v_2(s+t) > v_2(t)$, we have that $v_2(r(s+t)) > v_2(st)$. Therefore, we conclude that

$$2\gamma = v_2(st) = v_2(-4C) = 2.$$

Thus, $\gamma = 1$. From (8.3) we have that

$$2b = v_2(r) + v_2(st) = v_2(r) + 2\gamma = v_2(r) + 2,$$

so $v_2(r) = 2(b-1)$. As $v_2(r) > 1$, we have that $b \geq 2$.

We have $v_2(r) = 2$ if and only if $b = 2$. If $b = 2$, then examining (8.1) modulo 8, we have

$$4 + s + t \equiv 0 \pmod 8,$$

so

$$s + t \equiv 4 \pmod 8.$$

As $2 \parallel s$ and $2 \parallel t$, we conclude that

$$s \equiv t \pmod 8,$$

therefore $\beta = 6$ by Corollary 2.2 (A).

If $b \geq 3$, then $v_2(r) \geq 4$ as $v_2(r)$ is even. Examining (8.1) again modulo 8, we have

$$s + t \equiv 0 \pmod 8.$$

As $2 \parallel s$ and $2 \parallel t$, we conclude that, up to a permutation of s and t,

$$(s, t) \equiv (2, 6) \pmod 8,$$

therefore $\beta = 8$ by Corollary 2.2 (A). □

The above lemmas establish the following result:

Theorem 8.1. Let K be a bicyclic quartic field. Suppose that $K = \mathbb{Q}(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$ and A, B, C are integers satisfying (1.3), (1.4), (1.5), (1.6), $A = 0$, $B \neq 0$ and $b = v_2(B)$. Then $f(K) = 2^{\alpha} f_0(K)$, where

$$f(K) = 2^{\alpha} \prod_{\substack{p \text{ (prime)} \neq 2 \\ p^2 \mid B \text{ and } p^2 \parallel C}} p$$

where

$$\alpha = \begin{cases} 2, & \text{if } C \text{ is even,} \\ 3, & \text{if } C \text{ is odd,} \end{cases}$$

and $d(K) = 2^{\beta} f_0(K)^2$, where

$$\beta = \begin{cases} 4, & \text{if } C \text{ is even,} \\ 6, & \text{if } C \text{ is odd and } b = 2, \\ 8, & \text{if } C \text{ is odd and } b \geq 3. \end{cases}$$

Comparing with the findings of Alaca and Williams in [4, Theorem 3.1], we see that there is clear theoretical agreement in all cases except where $\beta = 6$. We deduced that $\beta = 6$ or 8 (i.e. $\alpha = 3$) if and only if C is odd. Comparing this with the result of [4], we see that $\beta = 6$ if and only if we have both $b = 2$ and $C \equiv 7 \pmod 8$ or $b = 2$ and $C \equiv 3 \pmod{16}$ and $v_2(\Delta)$ is even where $\Delta = 256C^3 - 27B^4$ is the discriminant of $g(x)$.

We can demonstrate some theoretical agreement insofar that $C \equiv 3 \pmod 4$ when $\beta = 6$. Note if $\beta = 6$ then $b = 2$, $v_2(r) = 2$ and $v_2(s) = v_2(t) = 1$ from the proof of Lemma 8.4. From Corollary 1.3 we have that $s \equiv t \equiv 2$ or $6 \pmod 8$. We have from (8.2) that $st \equiv -4C \pmod{16}$. Since $st \equiv 4 \pmod{16}$, we have that $C \equiv 12 \pmod{16}$, hence $C \equiv 3 \pmod 4$. We illustrate numerical agreement with the following examples.

Example: $g(x) = x^4 + 36x + 63$. Here C is odd and $b = 2$, so from Theorem 8.1 we have $\beta = 6$. Referring to [4], we have since $b = 2$ and $C \equiv 7 \pmod 8$, that $\beta = 6$.

Example 2: $g(x) = x^4 + 588x + 3283$. Here C is odd and $b = 2$, so from Theorem 8.1 we have $\beta = 6$. Referring to [4], as $b = 2$, $C \equiv 3 \pmod{16}$ and $v_2(\Delta) = v_2(5830872678400) = 14$ is even, we have that $\beta = 6$.

Chapter 9

Main Case 5: $A = B = 0$

Given that the resolvent of $x^4 + Ax^2 + Bx + C$ is $x^3 - Ax^2 - 4Cx + (4AC - B^2)$, we have that the resolvent cubic of $g(x) = x^4 + C$ is $q(x) = x^3 - 4Cx = x(x^2 - 4C)$. Therefore, when $x^4 + C$ is irreducible, we have that $\mathrm{Gal}(x^4 + C) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if and only if C is a square. As such, we will examine the quartics of the form $x^4 + n^2$. As before, if there is a prime p with $p^4|n^2$ (ie n is not square-free), we would then have $\left(\frac{\theta}{p}\right)^4 + \frac{n^2}{p^4} = 0$ for any root θ of $x^4 + n^2$. Thus, we will assume that n is square-free and positive. We note that $g(x)$ is reducible in the case where $n = 2$: $g(x) = x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$.

From here, we simply factor $x^4 + n^2$ as

$$x^4 + n^2 = (x^2 + in)(x^2 - in) = \left(x + i\sqrt{in}\right)\left(x - i\sqrt{in}\right)\left(x - \sqrt{in}\right)\left(x + \sqrt{in}\right).$$

Note that

$$i\sqrt{in} = \sqrt{2n}\left(\frac{-1}{2} + \frac{i}{2}\right) = -\overline{\left(\sqrt{in}\right)},$$

so we see that all four rots of $x^4 + n^2$ lie in $\mathbb{Q}\left(\sqrt{in}\right)$.

Let $K = \mathbb{Q}\left(\sqrt{in}\right)$ and $n \neq 2$. Note that $\sqrt{in} + \overline{\sqrt{in}} = \sqrt{2n}$ and $\frac{\left(\sqrt{in}\right)^2}{n} = i$, so

$\mathbb{Q}\left(\sqrt{2n}\right), \mathbb{Q}(i) \subset K$, so $K = \mathbb{Q}\left(i, \sqrt{2n}\right)$. As $n \neq 2$ and is square-free, we have $[K : \mathbb{Q}] = 4$, thus $x^4 + n^2$ is irreducible over $\mathbb{Z}$, hence we may use (1.9) to determine the conductor of K. If n is odd, then as $2n$ is even we automatically have $f(K) = 2^3 \operatorname{lcm}(-1, n) = 8|n|$ by Theorem 1.2. When n is even, as n is square-free we have $2^2 \| 2n$, thus $\mathbb{Q}\left(\sqrt{2n}\right) = \mathbb{Q}\left(\sqrt{\frac{n}{2}}\right)$, hence by Theorem 1.2 we have $f(K) = 2^2 \operatorname{lcm}\left(-1, \frac{n}{2}\right) = 2|n|$. As $\mathbb{Q}\left(\sqrt{-1}\right) \subset K$, by Theorem 1.2 we have that $\beta = 8$ when n is odd and $\beta = 4$ when n is even. Thus, we have the following result:

Theorem 9.1 (Main Case 5)**.** Let K be a bicyclic quartic field. Suppose that $K = \mathbb{Q}(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$ and A, B, C are integers satisfying (1.3), (1.4), (1.5), (1.6), and $A = B = 0$. Then $C = n^2$ for some square-free $n \in \mathbb{Z}$,

$$f(K) = \begin{cases} 8|n|, & \text{if } n \text{ is odd,} \\ 2|n|, & \text{if } n \text{ is even,} \end{cases}$$

and

$$d(K) = \begin{cases} 256n^2, & \text{if } n \text{ is odd,} \\ 4n^2, & \text{if } n \text{ is even.} \end{cases}$$

We conclude with expressing this result in the form of the previous Main Cases. Letting $v_2(f(K)) = \alpha$, $v_2(d(K)) = \beta$, $f(K) = 2^\alpha f_0(K)$ and $d(K) = 2^\beta (f_0(K))^2$, we have

$$\alpha = \begin{cases} 3, & \text{if } n \text{ is odd,} \\ 2, & \text{if } n \text{ is even,} \end{cases} \qquad \beta = \begin{cases} 8, & \text{if } n \text{ is odd,} \\ 4, & \text{if } n \text{ is even,} \end{cases} \qquad f_0(K) = \begin{cases} |n|, & \text{if } n \text{ is odd,} \\ \left|\frac{n}{2}\right|, & \text{if } n \text{ is even.} \end{cases}$$

Chapter 10

Future Work

10.1 Integral Bases and Prime Ideal Decomposition of Bicyclic Quartic Fields

Integral bases. In this section, we aim to combine our results with previous work on integral bases in bicyclic quartic fields and explore where it is possible and where more is required to express an integral basis of K defined by $g(x) = x^4 + Ax^2 + Bx + C$ in terms of A, B and C. The integral bases of bicyclic quartic fields K have been known since 1970 due to the work of Williams [53]. However, the construction of these integral bases is entirely dependent on having a representation of K as $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ where m and n are square-free, $m, n \neq 1$ and $m \neq n$. We state the result of Williams with respect to $\beta = v_2(d(K))$ and $\gcd(m, n)$:

Theorem 10.1. Let $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ be a bicyclic quartic field, where m and n are square-free integers with $m \neq 1,\ n \neq 1,\ m \neq n$, and $\rho = \dfrac{mn}{\gcd(m, n)^2}$. Then an integral basis for K is given by

(i) $\left\{1, \dfrac{1+\sqrt{m}}{2}, \dfrac{1+\sqrt{n}}{2}, \dfrac{1+\sqrt{m}+\sqrt{n}+\sqrt{\rho}}{4}\right\}$, if $\beta = 0$ and $\gcd(m, n) \equiv 1 \pmod 4$,

(ii) $\left\{1, \dfrac{1+\sqrt{m}}{2}, \dfrac{1+\sqrt{n}}{2}, \dfrac{1-\sqrt{m}+\sqrt{n}+\sqrt{\rho}}{4}\right\}$, if $\beta = 0$ and $\gcd(m, n) \equiv 3 \pmod 4$,

(iii) $\left\{1, \dfrac{1+\sqrt{m}}{2}, \sqrt{n}, \dfrac{\sqrt{n}+\sqrt{\rho}}{2}\right\}$, if $\beta = 4$,

(iv) $\left\{1, \sqrt{m}, \sqrt{n}, \dfrac{\sqrt{m}+\sqrt{\rho}}{2}\right\}$, if $\beta = 6$,

(v) $\left\{1, \sqrt{m}, \dfrac{\sqrt{m}+\sqrt{n}}{2}, \dfrac{1+\sqrt{\rho}}{2}\right\}$, if $\beta = 8$.

It is worth noting that integral bases of the forms (iii) and (v) are the equivalent given the permutation $m \mapsto \rho \mapsto n \mapsto m$, which was shown to be permissible in the discussion preceding Lemma 1.3 in Section 1.2. However, it is useful to recall that the values of m, n and ρ modulo 8 differ between these cases.

In view of this thesis and the above theorem, the following question naturally arises:

"Is it possible to find an integral basis of $\mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ explicitly in terms of the coefficients of a defining irreducible quartic polynomial $g(x) = x^4 + Ax^2 + Bx + C$?"

In Main Cases 3 ($A \neq 0,\ B = 0$) and 5 ($A = B = 0$), the answer is immediately yes, as in both of these cases we are able to explicitly determine the quadratic subfields of K in terms of the coefficients of $g(x)$. Below are modified versions of Tables 3 and 4 of Appendix A, where c_+ and c_- are the square-free parts of $-A + 2\sqrt{C}$ and $-A - 2\sqrt{C}$, respectively, $l = v_2(A^2 - 4C)$, $E = \frac{A^2-4C}{2^l}$ and **NR** indicates a value not required for deduction. The integral basis column refers to cases (i)-(v) of Theorem 10.1 where $m = c_+$ and $n = c_-$ and distinguishing between when integral bases of the form (i) and (ii) occur is determined by the value of $\gcd(c_+, c_-)$ modulo 4.

A	C (2)	l	E	c_+	c_-	β	integral basis
1 (4)	0	**NR**	**NR**	3 (4)	3 (4)	4	(*iii*)
1 (4)	1	**NR**	**NR**	1 (4)	1 (4)	0	(*i*) or (*ii*)
3 (4)	0	**NR**	**NR**	1 (4)	1 (4)	0	(*i*) or (*ii*)
3 (4)	1	**NR**	**NR**	3 (4)	3 (4)	4	(*iii*)
0 (4)	1	**NR**	**NR**	2 (4)	2 (4)	8	(*v*)
2 (4)	0	**NR**	**NR**	2 or 6 (8)	c_+ (8)	6	(*iv*)
0 (8)	0	**NR**	**NR**	1 (4)	3 (4)	4	(*iii*)
4 (8)	0				2 (4)		
		1 (2)	**NR**	1 (4)		6	(*iv*)
		1 (2)	**NR**	3 (4)		8	(*v*)
		0 (2)	1 (4)	**NR**		6	(*iv*)
		0 (2)	1 (4)	**NR**		8	(*v*)

For the case where $A \equiv 2 \pmod 4$ and $C \equiv 1 \pmod 2$, up to permutation of c_+ and c_- we have the following table:

$v_2(c_+)$ or $v_2(c_-)$ odd?	A (mod 8)	c_+ (mod 4)	β	integral basis
yes	**NR**	1	6	(*iv*)
yes	**NR**	3	8	(*v*)
no	2	**NR**	4	(*iii*)
no	6	3	4	(*iii*)
no	6	1	0	(*i*) or (*ii*)

In Main Case 5, we determined the defining quartic polynomial of K to be of the form $g(x) = x^4 + n^2$ where $n \neq 2$ is square-free and that $\mathbb{Q}\left(\sqrt{-1}\right)$ and $\mathbb{Q}\left(\sqrt{2n}\right)$ were two of the three quadratic subfields of K. From Theorem 9.1, we have

$$d(K) = \begin{cases} 256n^2, & \text{if } n \text{ is odd,} \\ 4n^2, & \text{if } n \text{ is even,} \end{cases}$$

so

$$\beta = \begin{cases} 8, & \text{if } n \text{ is odd,} \\ 4, & \text{if } n \text{ is even.} \end{cases}$$

In the case where n is even, we had $\mathbb{Q}\left(\sqrt{2n}\right) = \mathbb{Q}\left(\sqrt{\frac{n}{2}}\right)$. Therefore, when a bicyclic quartic field K has a defining irreducible quartic polynomial of the form $g(x) = x^4 + n^2$ where n is square-free, Theorems 9.1 and 10.1 imply that K has an integral basis of the following form:

$$\begin{cases} \left\{1, \sqrt{-1}, \dfrac{\sqrt{-1} + \sqrt{2n}}{2}, \dfrac{1 + \sqrt{-2n}}{2}\right\}, & \text{if } n \text{ is odd,} \\ \left\{1, \dfrac{1 + \sqrt{-1}}{2}, \sqrt{\dfrac{n}{2}}, \dfrac{\sqrt{\frac{n}{2}} + \sqrt{\frac{-n}{2}}}{2}\right\}, & \text{if } n \text{ is even.} \end{cases}$$

As noted in Chapter 8, $g(x) = x^4 + Bx + C$ in Main Case 4 is of the same form as given by Alaca and Williams in [6] and [4]. However, in both papers, the integral bases provided are in terms of a root θ of $g(x)$ and are not presented as an expression in radicals involving A and B. We do know that the resolvent roots r, s and t are solvable in radicals via Cardano's formula for cubics [18, p.632], though such an expression of the roots and, consequently, an integral basis of K via [53], would likely not be useful for theoretical purposes. We will not display the result of using Cardano's formula here but we do note that it is possible.

Finally, in the most complicated cases, Main Cases 1 and 2, there is no immediately-clear path to determine an integral basis from the coefficients of $g(x) = x^4 + Ax^2 + Bx + C$.

Further research on these two cases and Main Case 4 would likely involve a focus on the conductor or discriminant of K, especially given the connection between the discriminant and any integral basis. With knowledge of the discriminant of K and the behaviour of $r, s, t, r - A, s - A$ and $t - A$ in these cases, it would seem to be feasible to explore this direction for future research.

Prime Ideal Factorization. A classical topic of algebraic number theory is the arithmetic surrounding principal ideals of integer primes in the ring of integers $\mathcal{O}_K$ of a number field K. Students are often exposed to the factoring of $p\mathcal{O}_K$ in number fields which are **monogenic** - that is, whose ring of integers can be expressed as $\mathbb{Z}[\theta]$ for some $\theta \in \mathcal{O}_K \backslash \mathbb{Z}$. In this scenario, it is possible to construct the prime ideal factorization of $p\mathcal{O}_K$ by examining the factorization of the minimal polynomial of θ modulo p [5, Theorem 10.3.1]. The bicyclic quartic fields which are monogenic have been completely determined by [20], a result which has been reproduced by Nyul in [43] with a case analysis more in line with that of [53]. Knowing the discriminant of a bicyclic quartic field K from a defining irreducible quartic means that we know which primes will ramify in K. It would be interesting to explore the relationship between the irreducible quartic polynomial and the decomposition of principal ideals of integer primes p which ramify in a monogenic bicyclic quartic field K.

We close by examining two examples.

Example 1: Let $g(x) = x^4 + 2x^2 + 4x + 2$, where $A^2 - 4C = 4 - 8 = -4 \neq 0$, so this example belongs to Main Case 1, Case 5. The resolvent cubic of $g(x)$ is

$$q(x) = x^3 - Ax^2 - 4Cx + 4AC - B^2 = x^3 - 2x^2 - 8x = x(x - 4)(x + 2),$$

so $r = 0,\ s = 4,\ t = -2$. From here, $r - A = -2,\ s - A = 2,\ t - A = -4$, so by Theorem

2.2 we have that $K = \mathbb{Q}\left(\sqrt{-1}, \sqrt{2}\right)$. From Theorem 1.3, we had that $\beta = 8$, which agrees with Corollary 1.3 given $m = -1 \equiv 3 \pmod 4$ and $n = 2 \equiv 2 \pmod 4$. From Theorem 10.1 above, an integral basis of K is

$$\left\{1, \sqrt{-1}, \frac{\sqrt{-1}+\sqrt{2}}{2}, \frac{1+\sqrt{-2}}{2}\right\}.$$

Since no odd primes divide $r - A$, $s - A$ nor $t - A$, we have that $d(K) = 2^8 = 256$. The only prime which ramifies in K is 2. From [43], we have that K is monogenic. We note that the element $\zeta_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$ exhibits a power basis for O_K. From here, since the minimal polynomial of ζ_8 is $x^4 + 1 \equiv (x+1)^4 \pmod 2$, we have that

$$2O_K = \langle 2, \zeta_8 + 1\rangle^4 = \left\langle 2, \frac{3+\sqrt{2}+i\sqrt{2}}{2}\right\rangle^4.$$

Therefore, 2 totally ramifies in K.

Example 2: Let $g(x) = x^4 + 3x^2 + 16$, which belongs to Main Case 3. We have $-A - 2\sqrt{C} = -11$, $-A + 2\sqrt{C} = 5$, so $K = \mathbb{Q}\left(\sqrt{-11}, \sqrt{5}\right)$. Since both of these quantities are square-free, from the first table of this section we have that $\beta = 0$ and the integral basis is of form (i) as $\gcd(-11, 5) = 1$. Therefore, an integral basis of K is

$$\left\{1, \frac{1+\sqrt{-11}}{2}, \frac{1+\sqrt{5}}{2}, \frac{1+\sqrt{-11}+\sqrt{5}+\sqrt{-55}}{4}\right\}.$$

As $d(K) = 5^2 \cdot 11^2$, we have that 5 and 11 ramify in K. We note that K is not monogenic according to [43]. Instead, we'll examine the index of a root of $g(x)$ in hopes of being able to use the same technique as above to determine the prime ideal decompositions in this case. As stated in [36], the discriminant of a root θ of $g(x)$ is

$$d(\theta) = (-1)^{\frac{4(4-1)}{2}} \cdot 2^4 \cdot 16^{2-1}\left((2)^2 \cdot 16^{2-1} - (2-1)^{2-1} \cdot (1)^1 \cdot 3^2\right)^2$$

$$= 256 \cdot 55^2.$$

We then have that

$$i(\theta)^2 = \frac{d(\theta)}{d(K)} = 256.$$

Therefore, since $5 \nmid i(\theta)$ and $11 \nmid i(\theta)$, we may proceed [5, Theorem10.5.1]. From our discussion in Chapter 7, we have that $\theta = \frac{1}{2}\left(\sqrt{5} + \sqrt{-11}\right)$ is a root of $g(x)$. For $p = 5$, we obtain

$$g(x) \equiv x^4 + 3x^2 + 1 \equiv (x+1)^2(x+4)^2 \pmod{5}.$$

Therefore, we have

$$5\mathcal{O}_K = \left\langle 5, \frac{\sqrt{5} + \sqrt{-11}}{2} + 1 \right\rangle^2 \left\langle 5, \frac{\sqrt{5} + \sqrt{-11}}{2} + 4 \right\rangle^2.$$

For $p = 11$, we obtain

$$g(x) \equiv x^4 + 3x^2 + 5 \equiv (x+2)^2(x+9)^2 \pmod{11}.$$

Therefore, we have

$$11\mathcal{O}_K = \left\langle 11, \frac{\sqrt{5} + \sqrt{-11}}{2} + 2 \right\rangle^2 \left\langle 11, \frac{\sqrt{5} + \sqrt{-11}}{2} + 9 \right\rangle^2.$$

If it had been the case that $5 \mid i(\theta)$ or $11 \mid i(\theta)$, there is an alternate route we could use. It is well-known that if we have a quartic extension $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$, then $K = \mathbb{Q}\left(\sqrt{m} + \sqrt{n}\right)$. Provided that $\mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ is a quartic extension, we have that

$$h(x) = x^4 - (2m + 2n)x^2 + m^2 + n^2 - 2mn$$

is the minimal polynomial of $\sqrt{m} + \sqrt{n}$. Applying this here with $m = 5$ and $n = -11$ yields the polynomial

$$h(x) = x^4 + 12x^2 + 256.$$

From here, we compute $d\left(\sqrt{5} + \sqrt{-11}\right) = 2^{28} \cdot 13^2 \cdot 19^2$, so we may use this polynomial to create our prime ideals. For $p = 5$, we obtain

$$h(x) \equiv x^4 + 2x^2 + 1 \equiv (x + 2)^2(x + 3)^2 \pmod{5}.$$

Therefore, we have

$$5\mathcal{O}_K = \left\langle 5, \sqrt{5} + \sqrt{-11} + 2\right\rangle^2 \left\langle 5, \sqrt{5} + \sqrt{-11} + 3\right\rangle^2.$$

For $p = 11$, we obtain

$$h(x) \equiv x^4 + x^2 + 3 \equiv (x + 4)^2(x + 7)^2 \pmod{11}.$$

Therefore, we have

$$11\mathcal{O}_K = \left\langle 11, \sqrt{5} + \sqrt{-11} + 4\right\rangle^2 \left\langle 11, \sqrt{5} + \sqrt{-11} + 7\right\rangle^2.$$

10.2 Dihedral Octic Fields

The candidates for the Galois group of splitting fields of irreducible quartic polynomials are isomorphic to C_4, V, D_4, A_4 and S_4. Through the completion of this thesis the cases of C_4 (see [49]) and V are now completed. One striking difference between the currently-completed cases and the currently-open cases is that C_4 and V are abelian groups, whereas D_4, A_4 and S_4 are non-abelian. Given that all subfields of cyclotomic extensions of $\mathbb{Q}$

which are Galois over $\mathbb{Q}$ must be abelian extensions, splitting fields of quartic polynomials in $\mathbb{Q}[x]$ with Galois group D_4, A_4 or S_4 have no conductor. Consequently, the search for the conductor of splitting fields of quartic polynomials ends with the completion of this thesis.

Spearman and Williams have determined the discriminant and an integral basis for octic fields of the form $K = \mathbb{Q}(\theta)$ where $\theta^8 + A\theta^4 + 1 = 0$ and $\mathrm{Gal}\,(K/\mathbb{Q}) \cong D_4$ [48]. Let K be a number field with $G = \mathrm{Gal}(K/\mathbb{Q}) \cong D_4$ and present the group as

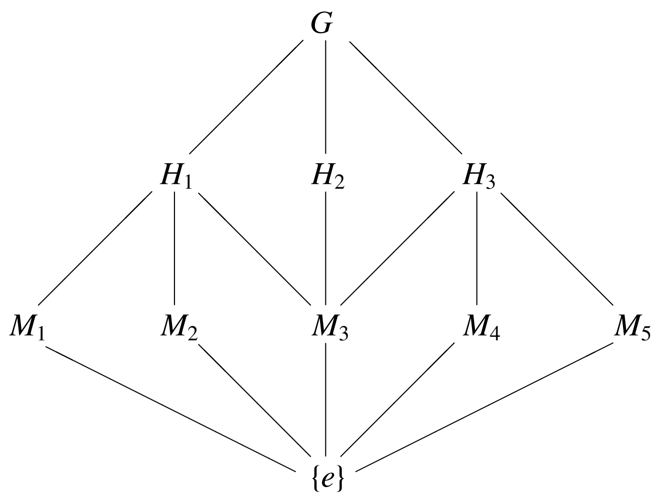
$$G = \langle\, a, b \mid a^4 = b^2 = e,\ ba = a^3 b\, \rangle.$$

As all finite extensions of $\mathbb{Q}$ are separable, we can express K as $K = \mathbb{Q}(\theta)$ for some $\theta \in K$ so that θ is an element of degree 8 over $\mathbb{Q}$. The non-trivial subgroups of G are:

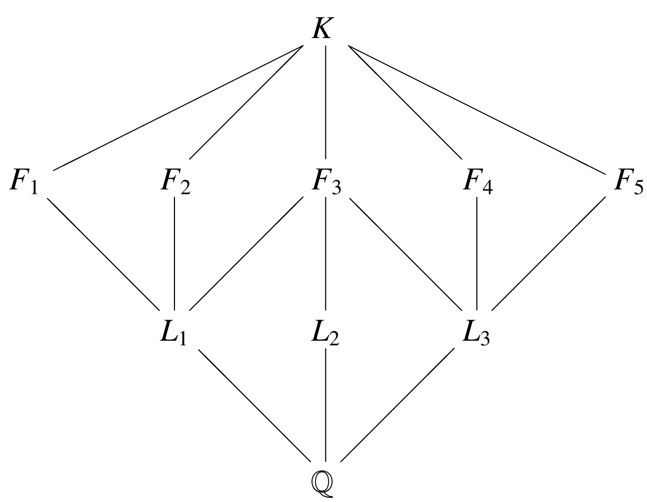
Order 4: $H_1 = \langle a^2, b\rangle,\ H_2 = \langle a\rangle,\ H_3 = \langle a^2, ab\rangle$

Order 2: $M_1 = \langle b\rangle,\ M_2 = \langle a^2 b\rangle,\ M_3 = \langle a^2\rangle,\ M_4 = \langle ab\rangle,\ M_5 = \langle a^3 b\rangle$.

This gives the following subgroup lattice:



From the Fundamental Theorem of Galois Theory, we know that the fixed fields $K^{\{e\}}$ and K^G are K and $\mathbb{Q}$, respectively and setting $L_i = K^{H_i}$ and $F_j = K^{M_j}$ for $i \in \{1, 2, 3\}$ and $j \in \{1, 2, 3, 4, 5\}$, we have the following subfield lattice of K:



We can make several observations simply from elementary Galois theory and knowledge of the field lattices of quartic Galois extensions. Firstly, by the Fundamental Theorem of Galois Theory, we have that K is Galois over every one of its subfields, $[K : L_i] = 4$ and $[K : F_j] = 2$ for each i and j. Secondly, from the field lattice structure, we have that K/L_1 and K/L_3 are relative bicyclic quartic extensions and K/L_2 is a relative cyclic quartic extension. Furthermore, $F_3/\mathbb{Q}$ is a bicyclic quartic extension.

Finally, we establish that F_1, F_2, F_4 and F_5 are **not** Galois extensions of $\mathbb{Q}$. Let

$F \in \{F_1, F_2, F_4, F_5\}$. As $F \neq F_3$, we have that the composite field $FF_3 = K$. Moreover, if F is Galois over $\mathbb{Q}$ and since $[F : \mathbb{Q}] = 4$, then $\mathrm{Gal}(F/\mathbb{Q})$ would be a group of order 4 and thus abelian. Since F_3 is an abelian extension of $\mathbb{Q}$, we would have that $FF_3 = K$ is abelian, a contradiction. Therefore, F cannot be Galois over $\mathbb{Q}$.

We now conclude this section with an example provided by Kappe and Warren [33] to gain some insight into the nature of the dihedral case. Let $g(x) = x^4 + 3x + 3$. From [33], we have the following result:

Theorem 10.2. Let $g(x) = x^4 + Ax^2 + Bx + C \in \mathbb{Z}[x]$ be an irreducible quartic polynomial, let $r(x) \in \mathbb{Z}[x]$ be its cubic resolvent and let E be the splitting field of $r(x)$. Then $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$ if and only if $r(x)$ has exactly one root $t \in \mathbb{Z}$ and $h(x) = (x^2 - tx + C)(x^2 + A - t)$ does not split over E.

So for $g(x) = x^4 + 3x + 3$, $r(x) = x^3 - 12x - 9 = (x+3)(x^2 - 3x - 3)$. The complex roots of $r(x)$ are $\frac{3 \pm \sqrt{21}}{2}$, so

$$E = \mathbb{Q}\left(\sqrt{21}\right).$$

As $t = -3$, we have that $h(x) = (x^2 + 3x + 3)(x^2 + 3)$, which has roots $\frac{-3 \pm i\sqrt{3}}{2}$ and $\pm i\sqrt{3}$, so $h(x)$ clearly not split over E. Therefore, we have that $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$.

We now wish to determine all of the subfields of K. First, we require the roots of $g(x)$, which Maple gives as

$$\frac{1}{2}\left(-i\sqrt{3} \pm \sqrt{3 - 2i\sqrt{3}}\right) \text{ and } \frac{1}{2}\left(i\sqrt{3} \pm \sqrt{3 + 2i\sqrt{3}}\right).$$

Set

$$\theta = \frac{-1}{2}i\sqrt{3} - \frac{1}{2}\sqrt{3 - 2i\sqrt{3}}.$$

Then

$$(\theta^2 - \theta)^2 = \frac{3 + 5i\sqrt{3}}{2},$$

so $i\sqrt{3} \in K$. Therefore, $-2\theta - i\sqrt{3} = \sqrt{3 - 2i\sqrt{3}} \in K$. Similarly, we have that $\sqrt{3 + 2i\sqrt{3}} \in K$. Thus,

$$\sqrt{3 - 2i\sqrt{3}}\sqrt{3 + 2i\sqrt{3}} = \sqrt{21} \in K.$$

As a result, we must have $\mathbb{Q}\left(\sqrt{-3}, \sqrt{21}\right) \subset K$. Given that this is a bicyclic quartic extension of $\mathbb{Q}$ and the only such subfield of K is F_3, we have that

$$F_3 = \mathbb{Q}\left(\sqrt{-3}, \sqrt{21}\right) = \mathbb{Q}\left(\sqrt{-3}, \sqrt{-7}\right) = \mathbb{Q}\left(\sqrt{-7}, \sqrt{21}\right).$$

Set

$$\begin{aligned}
\tau_1 &= \sqrt{3 - 2i\sqrt{3}}, \\
\tau_2 &= \sqrt{3 + 2i\sqrt{3}}, \\
\tau_4 &= \tau_1 + \tau_2 = \sqrt{6 + 2\sqrt{21}}, \\
\tau_5 &= \tau_1 - \tau_2 = \sqrt{6 - 2\sqrt{21}}.
\end{aligned}$$

Claim: The fields $\mathbb{Q}(\tau_1)$, $\mathbb{Q}(\tau_2)$, F_3, $\mathbb{Q}(\tau_4)$ and $\mathbb{Q}(\tau_5)$ are the distinct quartic subfields of K.

Proof: First, we show that τ_1 and τ_2 have degree 4 over $\mathbb{Q}$. Since $\tau_1^2 = 3 - 2i\sqrt{3}$ and $\tau_1^4 = -3 - 12i\sqrt{3}$, we have that τ_1 satisfies $x^4 - 6x + 21$. By Eisenstein's Criterion with respect to $p = 3$, we have that this polynomial is irreducible over $\mathbb{Q}$ and thus $\deg_{\mathbb{Q}}(\tau_1) = 4$. This is also the minimal polynomial of τ_2, so $\deg_{\mathbb{Q}}(\tau_2) = 4$ as well. We now establish that $\mathbb{Q}(\tau_1)$ and $\mathbb{Q}(\tau_2)$ are distinct. The radicals τ_1 and τ_2 cannot be de-nested as $3^2 - 2^2 \cdot (-3) = 21$

is not a rational square [8, Theorem 1]. From this, we conclude that $\sqrt{21} \notin \mathbb{Q}(\tau_1)$. Since

$$\frac{\tau_1}{\tau_2} = \frac{1}{\sqrt{21}}\left(3 - 2i\sqrt{3}\right) \notin \mathbb{Q}(\tau_1),$$

we have $\tau_2 \notin \mathbb{Q}(\tau_1)$. Therefore, we have $K = \mathbb{Q}(\tau_1, \tau_2)$. Since $\pm\tau_1$ and $\pm\tau_2$ are the roots of the irreducible quartic $x^4 - 6x + 2$, K is the splitting field of $x^4 - 6x + 2$ and $\mathbb{Q}(\tau_1)$, $\mathbb{Q}(\tau_2)$ are not Galois over $\mathbb{Q}$, thus $\mathbb{Q}(\tau_1), \mathbb{Q}(\tau_2) \neq F_3$.

We next show that τ_4 and τ_5 have degree 4 over $\mathbb{Q}$. Since we have $\tau_4^2 = 6 + 2\sqrt{21}$ and $\tau_4^4 = 120 + 24\sqrt{21}$, we deduce that τ_4 satisfies $x^4 - 12x^2 + 48$. By Eisenstein's Criterion with respect to 3, we have that this polynomial is irreducible over $\mathbb{Q}$ and thus $\deg_{\mathbb{Q}}(\tau_4) = 4$. This is also the minimal polynomial for τ_5, so $\deg_{\mathbb{Q}}(\tau_5) = 4$. Furthermore, $\tau_5 \notin \mathbb{Q}(\tau_4)$, as we would have $\tau_1, \tau_2 \in \mathbb{Q}(\tau_4)$, therefore $K = \mathbb{Q}(\tau_1, \tau_2) \subseteq \mathbb{Q}(\tau_4) \subseteq K$ and $K = \mathbb{Q}(\tau_4)$, a contradiction. Similarly, $\tau_4 \notin \mathbb{Q}(\tau_5)$. Again, $\mathbb{Q}(\tau_4)$ and $\mathbb{Q}(\tau_5)$ are not Galois over $\mathbb{Q}$, so $\mathbb{Q}(\tau_4), \mathbb{Q}(\tau_5) \neq F_3$.

Since $\mathbb{Q}(\tau_4) \subset \mathbb{R}$ and $\mathbb{Q}(\tau_1), \mathbb{Q}(\tau_2) \subset \mathbb{C}\backslash\mathbb{R}$, we conclude that $\mathbb{Q}(\tau_4) \neq \mathbb{Q}(\tau_1), \mathbb{Q}(\tau_2)$. If $\tau_1 \in \mathbb{Q}(\tau_5)$ or $\tau_2 \in \mathbb{Q}(\tau_5)$, then as $\tau_4 = \tau_5 + \tau_2 = 2\tau_1 - \tau_5$, in both cases we have $\tau_4 \in \mathbb{Q}(\tau_5)$, a contradiction. Therefore, $\mathbb{Q}(\tau_1)$, $\mathbb{Q}(\tau_2)$, $\mathbb{Q}(\tau_4)$ and $\mathbb{Q}(\tau_5)$ are pairwise-distinct non-Galois quartic subfields of K. $\square$

With this established, we can claim $\mathbb{Q}(\tau_i)$ corresponds to F_i for $i \in \{1, 2, 4, 5\}$. In closing, we note the connection between these subfields and the examination of Theorem 10.2. It seems reasonable to conjecture that the splitting field E of $q(x)$ and the splitting field of $h(x)$ are directly related to the subfields of K, which is certainly the case in the example above. The connection between the resolvent cubic and splitting fields was also prevalent throughout this thesis and in [49], so it would not be surprising to see the same kinds of connections in the dihedral case. Finally, results on relative extensions and the results of this thesis would likely play some role in pursuing this avenue of research.

10.3 Other Applications and Concluding Remarks

Number Field Cryptography. The application of number theory to the theory and implementation of public-key cryptography is an ever-growing and relevant field. Some popular cryptosystems rooted in number theory include RSA, Diffie-Hellman key exchange and elliptic curve cryptography. However, there are also cryptosystems rooted in algebraic number theory involving the class group of number fields, often involving quadratic number fields (see, for example, [11] and [45]). With the advent of practical quantum computing on the horizon, it is of crucial importance to develop cryptosystems which can withstand a quantum computer attack. There appears to be some potential for number fields of higher degree to provide stronger cryptosystems, with an emphasis on those with subfields providing some unpredictability for an attacker. [12]. Even as advancements in this field continue to be made, the use of low-degree number fields remains prevalent [16]. It would be interesting to explore this area in greater detail with an emphasis on bicyclic quartic fields, which have degree greater than 2, contain non-trivial subfields and, more specifically, contain multiple quadratic subfields. A mention of using imaginary bicyclic quartic fields appears in [39].

In closing, while bicyclic quartic fields are the simplest example of a non-cyclic Galois extension of $\mathbb{Q}$, there is still much more to learn about them. Whether a bicyclic quartic field K is expressed as the splitting field of an irreducible quartic polynomial or presented as $K = \mathbb{Q}\left(\sqrt{m}, \sqrt{n}\right)$ for the usual conditions on m and n, there is more work to be done in understanding these fields and in exploiting the known properties of these fields in further research in mathematics and cyber-security.

Appendix A Tables of Values for α and β

Recall that $\alpha = v_2(f(K)), \beta = v_2(d(K))$ and $a = v_2(A)$, $b = v_2(B)$ and $l = v_2(A^2 - 4C)$.

Theorem 1.3. Let K be a bicyclic quartic field. Suppose that $K = \mathbb{Q}(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$ and A, B, C are integers satisfying (1.3), (1.4), (1.5), (1.6), and $AB(A^2 - 4C) \neq 0$. Then $f(K) = 2^{\alpha} f_0(K)$ where

$$f_0(K) = \prod_{\substack{p \text{ (prime)} \neq 2 \\ e_p \text{ odd}}} p \prod_{\substack{p \text{ (prime)} \neq 2 \\ e_p \geq 2 \text{ even} \\ p|A}} p$$

and the values of α are given in Table 1 below. Moreover, $d(K) = 2^{\beta} (f_0(K))^2$ where the values of β are given in Tables 1 and 2 below.

Table 1: α and β values for subcases of Main Case 1

Case		α	β
1	$A \equiv 1 \pmod 2$, $B \equiv 2 \pmod 4$, $C \equiv 1 \pmod 2$		
	$A \equiv 1 \pmod 4$	2	4
	$A \equiv 3 \pmod 4$	0	0
2	$A \equiv 1 \pmod 2$, $B \equiv 2 \pmod 4$, $C \equiv 0 \pmod 2$		
	$A \equiv 1 \pmod 4$	0	0
	$A \equiv 3 \pmod 4$	2	4
3	$A \equiv 1 \pmod 2$, $B \equiv 0 \pmod 4$, $C \equiv 1 \pmod 2$		
	$A \equiv 1 \pmod 4$	0	0
	$A \equiv 3 \pmod 4$	2	4

Case		α	β
4	$A \equiv 1 \pmod 2,\ B \equiv 0 \pmod 4,\ C \equiv 0 \pmod 4$		
	$A \equiv 1 \pmod 4$	2	4
	$A \equiv 3 \pmod 4$	0	0
5	$A \equiv 2 \pmod 4,\ B \equiv 4 \pmod 8,\ C \equiv 2 \pmod 4$	3	8
6	$A \equiv 2 \pmod 4,\ B \equiv 0 \pmod 8,\ C \equiv 1 \pmod 4$		
	l **odd**		
	$(i)\ b \geq l-1$	3	
	$l = 5,\ A \equiv 2 \pmod 8$		6
	$l = 5,\ A \equiv 6 \pmod 8$		8
	$l > 5,\ A \equiv 2 \pmod 8$		8
	$l > 5,\ A \equiv 6 \pmod 8$		6
	$(ii)\ b = l-2,\ l = 7,\ A \equiv 6 \pmod{16},\ E \equiv 1 \pmod 4$	0	0
	$(iii)\ b = l-2,\ l = 7,\ A \equiv 6 \pmod{16},\ E \equiv 3 \pmod 4$	2	4
	$(iv)\ b = l-2,\ l = 7,\ A \equiv 14 \pmod{16},\ E \equiv 1 \pmod 4$	2	4
	$(v)\ b = l-2,\ l = 7,\ A \equiv 14 \pmod{16},\ E \equiv 3 \pmod 4$	0	0
	$(vi)\ b = l-2,\ l \geq 9,\ A \equiv 6 \pmod{16},\ E \equiv 1 \pmod 4$	2	2
	$(vii)\ b = l-2,\ l \geq 9,\ A \equiv 6 \pmod{16},\ E \equiv 3 \pmod 4$	0	0
	$(viii)\ b = l-2,\ l \geq 9,\ A \equiv 14 \pmod{16},\ E \equiv 1 \pmod 4$	0	0
	$(ix)\ b = l-2,\ l \geq 9,\ A \equiv 14 \pmod{16},\ E \equiv 3 \pmod 4$	2	4
	$(x)\ b \leq l-3,\ b$ even	3	
	$A \equiv 2 \pmod 8$		8
	$A \equiv 6 \pmod 8$		6
	$(xi)\ b < l-3,\ b = 5,\ A \equiv 10 \pmod{16}$	2	4
	$(xii)\ b < l-3,\ b = 7,\ A \equiv 2 \pmod{16}$	2	4
	$(xiii)\ b < l-3,\ b \text{ (odd)} \geq 9,\ A \equiv 2 \pmod{16}$	2	4

Case		α	β
6	$A \equiv 2 \pmod 4,\ B \equiv 0 \pmod 8,\ C \equiv 1 \pmod 4$		
	l **even**		
	(xiv) $b \geq l,\ l \geq 6,\ A \equiv 6 \pmod 8,\ E \equiv 1 \pmod 4$	0	0
	(xv) $b \geq l,\ l \geq 6,\ A \equiv 2 \pmod 8$ or $E \equiv 3 \pmod 4$	2	4
	(xvi) $b = l - 1,\ l = 4,\ b = 3,\ A \equiv 2 \pmod{16}$	2	4
	($xvii$) $b = l - 1,\ l = 4,\ b = 3,\ A \equiv 10 \pmod{16}$	0	0
	($xviii$) $b \leq l - 2,\ l \geq 6,\ b$ (even) ≥ 4	3	
	$A \equiv 2 \pmod 8$		8
	$A \equiv 6 \pmod 8$		6
	(xix) $b \leq l - 2,\ l \geq 8,\ b$ (odd) ≥ 5	2	4
7	$A \equiv 2 \pmod 4,\ B \equiv 0 \pmod 8,\ C \equiv 0 \pmod 4$	3	6
8	$A \equiv 4 \pmod 8,\ B \equiv 4 \pmod 8,\ C \equiv 3 \pmod 4$	3	6
9	$A \equiv 4 \pmod 8,\ B \equiv 0 \pmod 8,\ C \equiv 1 \pmod 4$	3	8
10	$A \equiv 4 \pmod 8,\ B \equiv 0 \pmod{16},\ C \equiv 4 \pmod 8$	3	**Table 2**
11	$A \equiv 0 \pmod 8,\ B \equiv 4 \pmod 8,\ C \equiv 3 \pmod 4$	3	6
12	$A \equiv 0 \pmod 8,\ B \equiv 0 \pmod 8,\ C \equiv 1 \pmod 4$	3	8
13	$A \equiv 0 \pmod 8,\ B \equiv 0 \pmod{16},\ C \equiv 4 \pmod{16}$	2	4

Table 2: β values for Main Case 1, Case 10: $A \equiv 4 \pmod 8$, $B \equiv 0 \pmod{16}$ and $C \equiv 4 \pmod 8$.

l even	
$b,\ l$	β
$b = l - 1$	8, if $E \equiv 1 \pmod 4$ 6, if $E \equiv 3 \pmod 4$
$b \geq l$	6, if $E \equiv 1 \pmod 4$ 8, if $E \equiv 3 \pmod 4$
l odd	
$b = l - 1,\ l = 7$	8, if $AE \equiv 4 \pmod{16}$ 6, if $AE \equiv 12 \pmod{16}$
$b = l - 1,\ l > 7$	6, if $AE \equiv 4 \pmod{16}$ 8, if $AE \equiv 12 \pmod{16}$
$b \geq l,\ l = 7$	6, if $AE \equiv 4 \pmod{16}$ 8, if $AE \equiv 12 \pmod{16}$
$b \geq l,\ l > 7$	8, if $AE \equiv 4 \pmod{16}$ 6, if $AE \equiv 12 \pmod{16}$

Theorem 1.5. Let K be a bicyclic quartic field. Suppose that $K = \mathbb{Q}(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$ and A, B, C are integers satisfying (1.3), (1.4), (1.5), (1.6) and $A \neq 0,\ B = 0$. Then C is the square of a non-zero integer,

$$f(K) = 2^{\alpha} \prod_{\substack{p \text{ (prime)} \neq 2 \\ v_p(-A+2\sqrt{C}) \text{ or } v_p(-A-2\sqrt{C}) \text{ odd}}} p$$

and $d(K) = 2^{\beta}\,(f_0(K))^2$, where α and β are given in Tables 3 and 4 below.

Recall that c_+ and c_- are the square-free parts of $-A+2\sqrt{C}$ and $-A-2\sqrt{C}$, respectively.

Table 3: Most α and β values for Main Case 3 *(up to permutation of c_+ and c_-)*

NR indicates a value which was not required for the deduction and $a \pmod{n}$ is abbreviated as a (n).

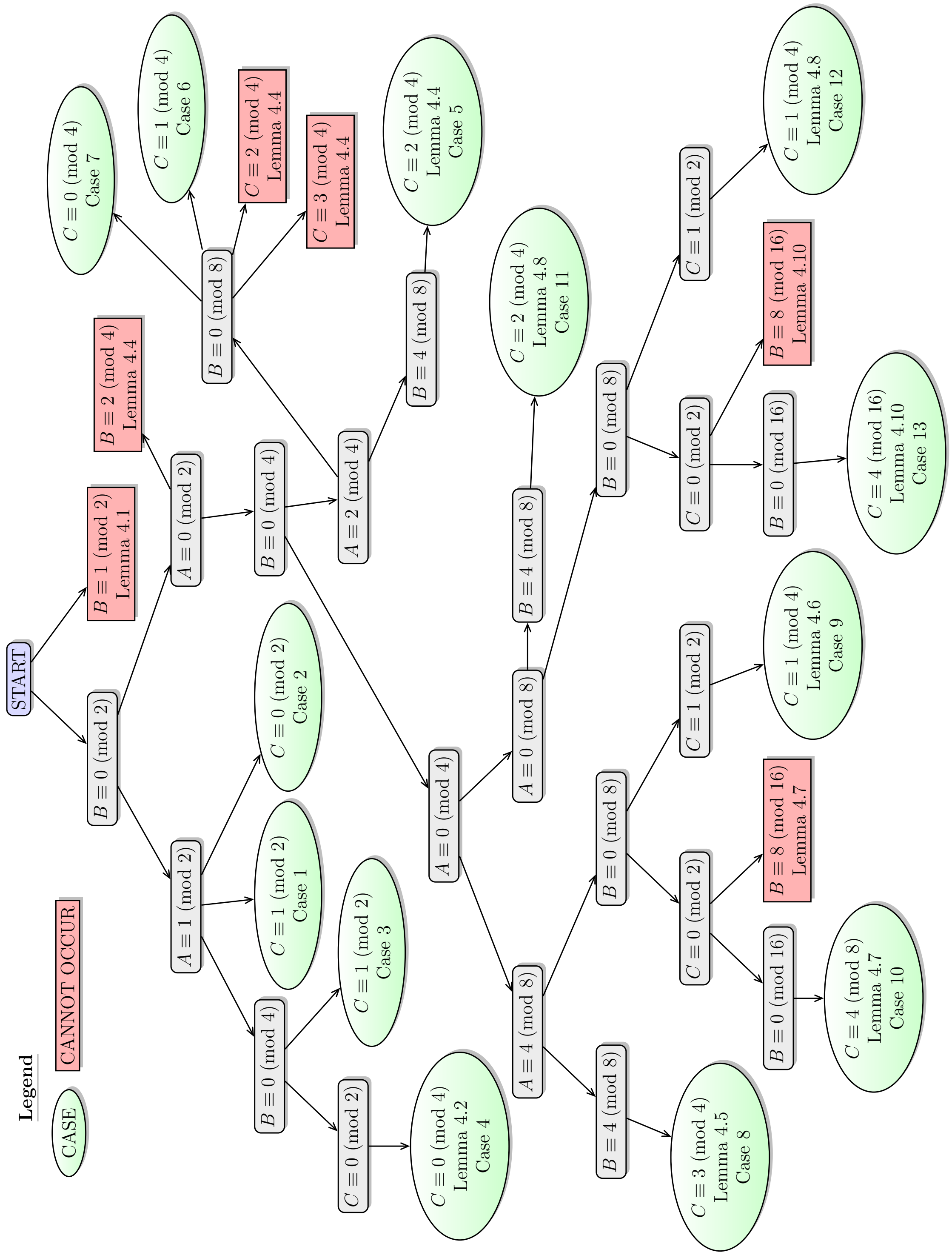
A	C (2)	l	E	c_+	c_-	α	β
1 (4)	0	**NR**	**NR**	3 (4)	3 (4)	2	4
1 (4)	1	**NR**	**NR**	1 (4)	1 (4)	0	0
3 (4)	0	**NR**	**NR**	1 (4)	1 (4)	0	0
3 (4)	1	**NR**	**NR**	3 (4)	3 (4)	2	4
0 (4)	1	**NR**	**NR**	2 (4)	2 (4)	3	8
2 (4)	0	**NR**	**NR**	2 or 6 (8)	c_+ (8)	3	6
0 (8)	0	**NR**	**NR**	1 (4)	3 (4)	2	4
4 (8)	0				2 (4)	3	
		1 (2)	**NR**	1 (4)			6
		1 (2)	**NR**	3 (4)			8
		0 (2)	1 (4)	**NR**			6
		0 (2)	1 (4)	**NR**			8

For the case where $A \equiv 2 \pmod{4}$ and $C \equiv 1 \pmod{2}$, up to permutation of c_+ and c_- we have the following table:

Table 4: α and β values for Main Case 3 when $A \equiv 2 \pmod 4$ and $C \equiv 1 \pmod 2$

$v_2(c_+)$ or $v_2(c_-)$ odd?	$A \pmod 8$	$c_+ \pmod 4$	α	β
yes	**NR**	1	3	6
yes	**NR**	3	3	8
no	2	**NR**	2	4
no	6	3	2	4
no	6	1	0	0

Appendix B Flowchart for Main Case 1



Appendix C Examples

Main Case 1

Case 1

$A \equiv 1 \pmod 4$	$x^4 - 3x^2 + 30x + 61$	$f(K) = 20,\ d(K) = 400$
$A \equiv 3 \pmod 4$	$x^4 - x^2 + 42x + 79$	$f(K) = 21,\ d(K) = 441$

Case 2

$A \equiv 1 \pmod 4$	$x^4 + 17x^2 + 126x + 172$	$f(K) = 21,\ d(K) = 441$
$A \equiv 3 \pmod 4$	$x^4 + 11x^2 + 14x + 74$	$f(K) = 28,\ d(K) = 784$

Case 3

$A \equiv 1 \pmod 4$	$x^4 + 37x^2 + 156x + 157$	$f(K) = 39,\ d(K) = 1521$
$A \equiv 3 \pmod 4$	$x^4 + 35x^2 + 60x + 61$	$f(K) = 12,\ d(K) = 144$

Case 4

$A \equiv 1 \pmod 4$	$x^4 + 65x^2 + 140x + 596$	$f(K) = 28,\ d(K) = 784$
$A \equiv 3 \pmod 4$	$x^4 + 59x^2 + 252x + 844$	$f(K) = 21,\ d(K) = 441$

Case 5	$x^4 + 2x^2 + 4x + 2$	$f(K) = 8,\ d(K) = 256$

Case 6

6(i)

$l = 5,\ A \equiv 2 \pmod 8$	$x^4 + 2x^2 - 96x + 217$	$f(K) = 24,\ d(K) = 576$
$l = 5,\ A \equiv 6 \pmod 8$	$x^4 + 6x^2 - 96x + 289$	$f(K) = 8,\ d(K) = 256$
$l > 5,\ A \equiv 2 \pmod 8$	$x^4 - 342x^2 + 1152x - 423$	$f(K) = 24,\ d(K) = 2304$
$l > 5,\ A \equiv 6 \pmod 8$	$x^4 + 134x^2 + 640x + 809$	$f(K) = 40,\ d(K) = 1600$

6(*ii*)	$x^4 + 86x^2 + 480x + 6169$	$f(K) = 15,\ d(K) = 225$
6(*iii*)	$x^4 + 86x^2 + 416x + 3929$	$f(K) = 52,\ d(K) = 2704$
6(*iv*)	$x^4 + 78x^2 + 672x + 8017$	$f(K) = 28,\ d(K) = 784$
6(*v*)	$x^4 - 274x^2 + 2080x - 4111$	$f(K) = 65,\ d(K) = 4225$
6(*vi*)	$x^4 - 58x^2 + 384x + 4297$	$f(K) = 12,\ d(K) = 144$
6(*vii*)	$x^4 - 19146x^2 - 24960x + 83663449$	$f(K) = 65,\ d(K) = 4225$
6(*viii*)	$x^4 - 34x^2 + 1920x + 17569$	$f(K) = 15,\ d(K) = 225$
6(*ix*)	$x^4 + 94x^2 + 1920x + 15649$	$f(K) = 60,\ d(K) = 3600$

6(*x*)

$A \equiv 2 \pmod 8$	$x^4 - 106x^2 + 272x + 89$	$f(K) = 136,\ d(K) = 18496$
$A \equiv 6 \pmod 8$	$x^4 + 58x^2 - 192x + 457$	$f(K) = 264,\ d(K) = 69696$

6(*xi*)	$x^4 + 282x^2 + 864x + 6057$	$f(K) = 12,\ d(K) = 144$
6(*xii*)	$x^4 - 1854x^2 - 28800x + 2126529$	$f(K) = 12,\ d(K) = 144$
6(*xiii*)	$x^4 + 3074x^2 + 4608x + 3683329$	$f(K) = 12,\ d(K) = 144$
6(*xiv*)	$x^4 + 70x^2 + 2496x + 11833$	$f(K) = 39,\ d(K) = 1521$
6(*xv*)	$x^4 + 50x^2 + 192x + 193$	$f(K) = 12,\ d(K) = 144$
6(*xvi*)	$x^4 + 2x^2 + 184x + 2117$	$f(K) = 92,\ d(K) = 8464$
6(*xvii*)	$x^4 + 74x^2 + 280x + 1229$	$f(K) = 35,\ d(K) = 1225$

6(*xviii*)

$A \equiv 2 \pmod 8$	$x^4 + 2x^2 + 16x + 17$	$f(K) = 8,\ d(K) = 256$
$A \equiv 6 \pmod 8$	$x^4 - 90x^2 + 576x + 9513$	$f(K) = 24,\ d(K) = 576$

6(*xix*)	$x^4 + 2x^2 + 384x + 9217$	$f(K) = 12,\ d(K) = 144$

Case 7 $x^4 - 86x^2 + 120x - 36$ $f(K) = 40,\ d(K) = 1600$

Case 8 $x^4 - 100x^2 + 132x + 223$ $f(K) = 264,\ d(K) = 69696$

Case 9 $x^4 - 148x^2 + 744x - 383$ $f(K) = 744,\ d(K) = 2214144$

Case 10 $x^4 - 52x^2 + 192x - 188$ $f(K) = 24,\ d(K) = 2304$

See Table X BELOW

Case 11 $x^4 - 88x^2 + 116x + 167$ $f(K) = 232,\ d(K) = 53824$

Case 12 $x^4 + 96x^2 + 120x + 601$ $f(K) = 8,\ d(K) = 256$

Case 13 $x^4 + 80x^2 + 288x + 388$ $f(K) = 12,\ d(K) = 144$

TABLE X

l even		
$b,\ l$	β	$f(K)$ $d(K)$
$b = l - 1$	$E \equiv 1 \pmod 4$, $x^4 + 12x^2 + 384x + 1252$	8 256
	$E \equiv 3 \pmod 4$, $x^4 + 140x^2 + 384x + 868$	24 576
$b \geq l$	$E \equiv 1 \pmod 4$, $x^4 + 668x^2 + 3840x + 7300$	24 576
	$E \equiv 3 \pmod 4$, $x^4 + 268x^2 + 768x + 612$	8 256
l odd		
$b = l - 1,\ l = 7$	$AE \equiv 4 \pmod{16}$, $x^4 + 4x^2 + 192x + 484$	24 2304
	$AE \equiv 12 \pmod{16}$, $x^4 - 4x^2 + 320x + 1124$	40 1600
$b = l - 1,\ l > 7$	$AE \equiv 4 \pmod{16}$, $x^4 + 148x^2 + 768x + 1252$	24 576
	$AE \equiv 12 \pmod{16}$, $x^4 + 4x^2 + 768x + 3204$	8 256
$b \geq l,\ l = 7$	$AE \equiv 4 \pmod{16}$, $x^4 + 20x^2 + 896x + 3908$	56 3136
	$AE \equiv 12 \pmod{16}$, $x^4 + 20x^2 + 1408x + 6788$	88 30976
$b \geq l,\ l > 7$	$AE \equiv 4 \pmod{16}$, $x^4 + 396x^2 + 2560x + 6564$	40 6400
	$AE \equiv 12 \pmod{16}$, $x^4 + 340x^2 + 1536x + 8548$	24 576

Main Case 2

$x^4 + 26x^2 + 96x + 169$ $\qquad$ b odd, $f(K) = 12$, $d(K) = 144$

$x^4 + 98x^2 + 960x + 2401$ $\qquad$ b even, $A \equiv 2 \pmod 8$, $f(K) = 120$, $d(K) = 57600$

$x^4 + 14x^2 + 48x + 49$ $\qquad$ b even, $A \equiv 6 \pmod 8$, $f(K) = 24$, $d(K) = 576$

Main Case 3

$x^4 + x^2 + 16$ $\quad A \equiv 1 \pmod 4,\ C$ odd, $f(K) = 28,\ d(K) = 784$

$x^4 + x^2 + 49$ $\quad A \equiv 1 \pmod 4,\ C$ even, $f(K) = 195,\ d(K) = 38025$

$x^4 + 3x^2 + 16$ $\quad A \equiv 3 \pmod 4,\ C$ even, $f(K) = 55,\ d(K) = 3025$

$x^4 + 3x^2 + 1$ $\quad A \equiv 3 \pmod 4,\ C$ odd, $f(K) = 20,\ d(K) = 400$

$x^4 + 4x^2 + 1$ $\quad A \equiv 0 \pmod 4,\ C$ odd, $f(K) = 24,\ d(K) = 2304$

$x^4 + 8x^2 + 4$ $\quad A \equiv 0 \pmod 8,\ C$ even, $f(K) = 12,\ d(K) = 144$

$x^4 + 4x^2 + 36$ $\quad A \equiv 4 \pmod 8,\ C$ even, $f(K) = 8,\ d(K) = 256$

$x^4 + 2x^2 + 4$ $\quad A \equiv 2 \pmod 4,\ C$ even, $f(K) = 24,\ d(K) = 576$

Main Case 3: when $A \equiv 2 \pmod 4$ and at least one of c_+ or c_- is even.

Recall: c_+ and c_- are the square-free parts of $-A + 2\sqrt{C}$ and $-A - 2\sqrt{C}$, respectively.

$x^4 + 2x^2 + 25$ $\quad c_- \equiv 1 \pmod 4,\ f(K) = 24,\ d(K) = 576$

$x^4 + 6x^2 + 1$ $\quad c_+ \equiv 3 \pmod 4,\ f(K) = 8,\ d(K) = 256$

Main Case 3: when $A \equiv 2 \pmod 4$ and both c_+ and c_- are odd.

$x^4 + 2x^2 + 49$	$A \equiv 2 \pmod 8$, $f(K) = 12$, $d(K) = 144$
$x^4 + 22x^2 + 9$	$A \equiv 6 \pmod 8$, $c_+ \equiv 3 \pmod 4$, $f(K) = 28$, $d(K) = 784$
$x^4 + 46x^2 + 1$	$A \equiv 6 \pmod 8$, $c_+ \equiv 1 \pmod 4$, $f(K) = 33$, $d(K) = 1089$

Main Case 4:

$x^4 - 144x + 468$	C even, $f(K) = 12$, $d(K) = 144$
$x^4 + 36x + 63$	$b = 2$ and C odd, $f(K) = 24$, $d(K) = 576$
$x^4 + 24x + 73$	$b \geq 3$ and C odd, $f(K) = 8$, $d(K) = 256$

Main Case 5:

$x^4 + 1$	C odd, $f(K) = 8$, $d(K) = 256$
$x^4 + 36$	C even, $f(K) = 12$, $d(K) = 144$

Bibliography

[1] A. Alaca and S. Alaca, *An integral basis and the discriminant of a quintic feld defned by a trinomial* $x^5 + ax + b$, JP J. Algebra Number Theory Appl. **4** (2004), no. 2, 261-299.

[2] S. Alaca, *p-integral bases of a cubic field*. Proc. Amer. Math. Soc. **126** (1998), no. 7, 1949-1953.

[3] S. Alaca and K. S. Williams, *On Voronoi's method for finding an integral basis of a cubic field*, Util. Math. **65** (2004), 163-166.

[4] S. Alaca and K. S. Williams, *p-integral bases of a quartic field defined by trinomial* $x^4 + ax + b$, Far East Journal of Mathematical Sciences **12** (2004), 137-168.

[5] S. Alaca and K. S. Williams, Introductory Algebraic Number Theory, Cambridge University Press, 2004.

[6] S. Alaca and K. S. Williams, *A simple method for finding an integral basis of a quartic field defined by a trinomial* $x^4 + ax + b$, JP J. Algebra Number Theory Appl. **3** (2003), 477-505.

[7] A. Biróand K. Lapkova, *The class number one problem for the real quadratic fields* $\mathbb{Q}\left(\sqrt{(an)^2 + 4a}\right)$, Acta Arith. **172** (2016), no. 2, 117-131.

[8] A. Borodin, R. Fagin, J. E. Hopcroft and M. Tompa, *Decreasing the Nesting Depth of Expressions Involving Square Roots*, Journal of Symbolic Computation **1** (1985), 169-188.

[9] N. Bourbaki, Elements of the History of Mathematics, Springer-Verlag Berlin Heidelberg., 1994.

[10] E. Brown and C. J. Parry, *The imaginary bicyclic biquadratic fields with class-number* 1, J. Reine Angew. Math. **266** (1974), 118-120.

[11] J. Buchmann, M. Maurer and B. Möller, *Cryptography based on number fields with large regulator*, J. Théor. Nombres Bordeaux **12** (2000), no. 2, 293-307.

[12] J. Buchmann, T. Takagi, and U. Vollmer, *Number field cryptography*, High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Fields Institute Communications, vol. 41, American Mathematical Society, Providence, RI, 2004, pp. 111-121.

[13] D. A. Buell, H. C. Williams and K. S. Williams, *On the Imaginary Bicyclic Biquadratic Fields With Class-Number* 2, Mathematics of computation **31** (1977), no. 140, 1034-1042.

[14] J. M. Calloway, *On The Discriminant of Arbitrary Algebraic Number Fields*, Proceedings of the American Mathematical Society **6** (1955), 482-489.

[15] H. Cohen and H. W. Lenstra, Jr., *Heuristics on Class Groups of Number Fields.* In Number Theory, pp. 33-62, Lecture Notes in Mathematics 1068. Berlin: Springer Verlag, 1984.

[16] H. Cohn and N. Heninger, *Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding*, Adv. Math. Commun. **9** (2015), no. 3, 311-339.

[17] R. Dedekind, *Uber die Theorie der ganzen algebraischen Zahlen*, XI Suupl. to Dirichlet's "Vorlesungen uber Zahlentheorie" 2nd ed. (1871), 3rd ed. (1879), 4th d. (1894). [Gesammelte mathematische Werke, vol. III, 1-314, Vieweg, 1932.]

[18] D. Dummit and R. Foote, Abstract Algebra, Third Edition, John Wiley and Sons, 2004.

[19] D. Eloff, B. K. Spearman and K. S. Williams, *Integral bases for an infinite family of cyclic quintic fields*, Asian J. Math **10** (2006), no. 4, 765-772.

[20] M. Gras and F. Tanoé, *Corps biquadratiques monogènes*, Manuscripta Math. **86** (1995), no. 1, 63-79.

[21] H. Graves, $\mathbb{Q}\left(\sqrt{2}, \sqrt{35}\right)$ *has a non-principal Euclidean ideal*, Int. J. Number Theory **7** (2011), no. 8, 2269-2271.

[22] J. Guàrdia, J. Montes and E. Nart, *Higher Newton polygons and integral bases*, J. Number Theory **147** (2015), 549-589.

[23] J. Guàrdia, J. Montes and E. Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, J. Théor. Nombres Bordeaux **23** (2011), no. 3, 667-696.

[24] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper ("Zahlbericht")*, II, 1930. 3. Auflage, Physica-Verlag, Würzburg, 1970.

[25] David Hilbert, The Theory of Algebraic Number Fields (English translation-Translated by I. Adamson), Springer-Verlag, Berlin, Heidelberg, New York, 1998.

[26] P. Hu, *Bounds of Discriminants of Number Fields*, p-Adic Numbers Ultrametric Anal. Appl. **5** (2013), no. 4, 302-312.

[27] T. W. Hungerford, Algebra, Holt, Rinehart and Winston, Inc., New York, 1974.

[28] I. Kaplansky, Fields and Rings, second edition, University of Chicago Press, Chicago, 1972.

[29] B. Jadrijević, *On elements with index of the form 2a3b in a parametric family of biquadratic fields*, Glas. Mat. Ser. III **50(70)** (2015), no. 1, 43-63.

[30] S. Jeannin, *Nombre de classes et unités des corps de nombres cycliques quintiques d'E. Lehmer*, Journal de Théorie des Nombres de Bordeaux **8** (1996), 75-92.

[31] C. Ji, B. Zhang, *Sums of three integral squares in biquadratic fields*, J. Number Theory **138** (2014), 37-47.

[32] S. Jung and S. Kwon, *Determination of all imaginary bicyclic biquadratic number fields of class number* 3, Bull. Korean Math. Soc. **35**, no. 1, 83-89.

[33] L. -C. Kappe and B. Warren, *An elementary test for the Galois group of a quartic polynomial*, American Mathematical Monthly **96** (1989), 133-137.

[34] S. Katayama, *The abc conjecture and the fundamental system of units of certain real bicyclic biquadratic fields*, Proc. Japan Acad. Ser. A Math. Sci. **75** (1999), no. 10, 198-199.

[35] Y. Kôhno, T. Nakahara and M. Sultan, *Monogenity of biquadratic fields related to Dedekind-Hasse's problem*, Punjab Univ. J. Math. (Lahore) **47** (2015), no. 2, 77-82.

[36] P. Llorente, E. Nart and N. Vila, *Discriminants of number fields defined by trinomials*, Acta Arith. **43** (1984), 367-373.

[37] P. Llorente and E. Nart, *Effective determination of the decomposition of the rational primes in a cubic field*, Proc. Amer. Math. Soc. **87** (1983), 579-585.

[38] R. L. Long, Algebraic Number Theory, Marcel Dekker, Inc., New York and Basel, 1977.

[39] A. Meyer, S. Neis and T. Pfahler, *First implementation of cryptographic protocols based on algebraic number fields*, Information Security and Privacy, ACISP 2001, Sydney (Vijay Varadharajan and Yi Mu, eds.), Lecture Notes in Computer Science, vol. 2119, Springer, 2001, 84-103.

[40] R. A. Mollin, Algebraic Number Theory, Second Edition, Chapman and Hall/CRC, 2001.

[41] T. Nakahara, *On the indices and integral bases of noncyclic but abelian biquadratic fields*, Arch. Math. (Basel) **41** (1983), no. 6, 504-508.

[42] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Third Edition, Springer-Verlag New York, 2004.

[43] G. Nyul, *Power integral bases in mixed biquadratic number fields*, Acta Acad. Paed. Agriensis, Sectio Mathematicae **28** (2001) 79-86.

[44] A.E. Özlük and C. Snyder, *On the distribution of the nontrivial zeros of quadratic L-functions of imaginary quadratic number fields close to the real axis*, Acta Arith. **124** (2006), no. 3, 205-233.

[45] M. Pohst and D. Schielzeth, *On real quadratic number fields suitable for cryptography*, Experiment. Math. **14** (2005), no. 2, 189-197.

[46] H. Riele and H. Williams, *New computations concerning the Cohen-Lenstra heuristics*, Experiment. Math. **12** (2003), no. 1, 99-113.

[47] B. Setzer, *The Determination of all Imaginary, Quartic, Abelian Number Fields With Class Number* 1, Mathematics of Computation **35** (Oct., 1980), no. 152, 1383-1386.

[48] B. K. Spearman and K. S. Williams, *The Simplest D_4-octics*, Int. J. Algebra **2** (2008), no. 1-4, 79-89.

[49] B. K. Spearman and K. S. Williams, *The conductor of a cyclic quartic field*, Publ. Math. Debrecen **48** (1996), 13-43.

[50] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. **14** (1967), 1-27.

[51] K. Uchida, *Imaginary abelian number fields with class-number one*, Tôhoku Math. Journ. **24** (1972), 487-499.

[52] L. Washington, Introduction to Cyclotomic Fields, Second Edition, Springer-Verlag New York, 1982.

[53] K. S. Williams, *Integers of biquadratic fields*, Canadian Mathematical Bulletin **13** (1970), 519-526.

[54] H. Yokoi, *Imaginary bicyclic biquadratic fields with the real quadratic subfield of class-number one*, Nagoya Math J. **102** (1986), 91-100.