2011-07-05

Maximal Unramified Extensions of Cyclic Cubic Fields

Ka Lun Wong
Brigham Young University - Provo

Maximal Unramified Extensions of Cyclic Cubic Fields

Ka Lun Wong

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Darrin Doud, Chair
David Cardon
Pace Nielsen

Department of Mathematics

Brigham Young University

August 2011

Abstract

Maximal Unramified Extensions of Cyclic Cubic Fields

Ka Lun Wong

Department of Mathematics

Master of Science

Maximal unramified extensions of quadratic number fields have been well studied. This thesis focuses on maximal unramified extensions of cyclic cubic fields. We use the unconditional discriminant bounds of Moreno to determine cyclic cubic fields having no non-solvable unramified extensions. We also use a theorem of Roquette, developed from the method of Golod-Shafarevich, and some results by Cohen to construct cyclic cubic fields in which the unramified extension is of infinite degree.

Acknowledgments

First, I want to thank my advisor Darrin Doud who introduced this project to me. He has been kind and enthusiastic to help me. I am grateful for his patience with my lack of knowledge. His wide knowledge has been of great value to me. He has made available his support in a number of ways. I have enjoyed the time and study with him. Besides Professor Doud, I would also like to thank my research committee, including Professor David Cardon and Professor Pace Nielsen, for their time and comments on my thesis.

I also want to thank my wife and my family for their sacrifice and support. Without their support, it would have been impossible to complete this project.

Contents

1 Introduction **1**

1.1 Preliminaries I 2

1.2 Preliminaries II - Class Field Theory 6

2 Cyclic Cubic Fields **9**

2.1 General Parametric Description of Cyclic Cubic Fields 9

2.2 Specific Parametric Description of Cyclic Cubic Fields 17

3 Discriminant Bounds **29**

4 Maximal Unramified Extensions of Cyclic Cubic Fields **32**

4.1 Maximal Unramified Solvable Extensions 32

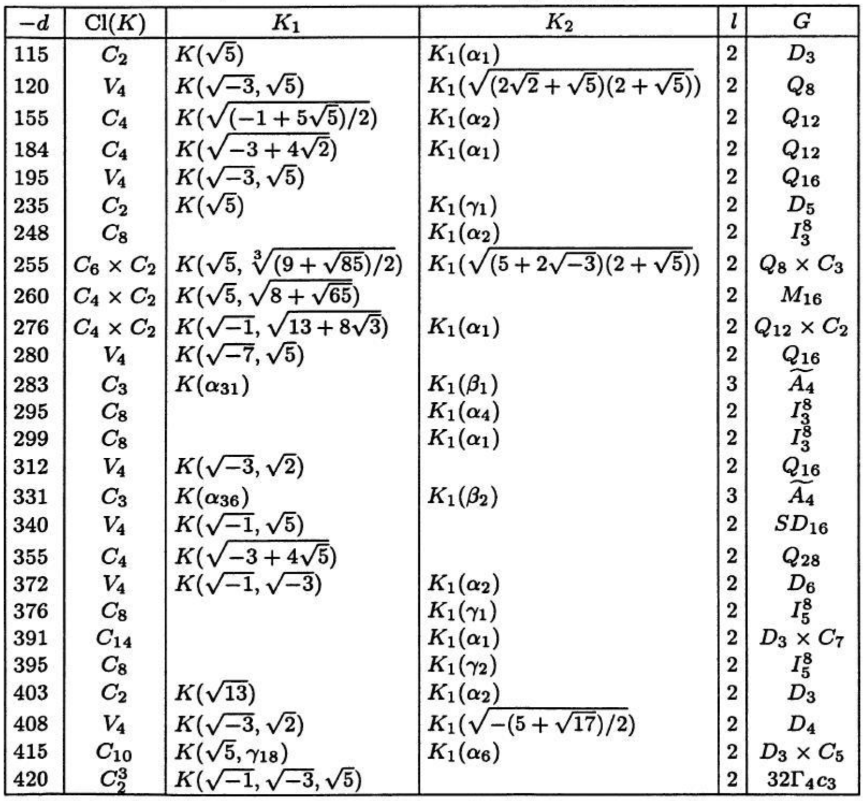
4.2 Unramified Non-Solvable Extensions 45

4.3 Unramified Extensions of Infinite Order 49

Chapter 1. Introduction

Maximal unramified extensions of quadratic number fields have been well studied. Yamamura [11] studied maximal unramified extensions of imaginary quadratic number fields of small conductors $\leqslant 420$ (and $\leqslant 1000$ under the Generalized Riemann Hypothesis (GRH)) and determined the structures of the Galois groups $\mathrm{Gal}(K_{ur}/K)$ of the maximal unramified extensions K_{ur} of these imaginary quadratic number fields K. The main idea in Yamamura's paper is to use the discriminant bounds to show that certain fields with discriminant less than the bounds have no non-solvable unramified extension. Then, the maximal unramified extension will coincide with the top of the class field tower of K which is also the maximal unramified solvable extension. In his paper, he gives the explicit structure of K_{ur} and $\mathrm{Gal}(K_{ur}/K)$ in the following table.

Table of imaginary quadratic number fields $K = \mathbf{Q}(\sqrt{d})$, $|d| \leqq 420$ with $K_{ur} \neq K_1$



$-d$	$\mathrm{Cl}(K)$	K_1	K_2	l	G
115	C_2	$K(\sqrt{5})$	$K_1(\alpha_1)$	2	D_3
120	V_4	$K(\sqrt{-3}, \sqrt{5})$	$K_1(\sqrt{(2\sqrt{2}+\sqrt{5})(2+\sqrt{5})})$	2	Q_8
155	C_4	$K(\sqrt{(-1+5\sqrt{5})/2})$	$K_1(\alpha_2)$	2	Q_{12}
184	C_4	$K(\sqrt{-3+4\sqrt{2}})$	$K_1(\alpha_1)$	2	Q_{12}
195	V_4	$K(\sqrt{-3}, \sqrt{5})$		2	Q_{16}
235	C_2	$K(\sqrt{5})$	$K_1(\gamma_1)$	2	D_5
248	C_8		$K_1(\alpha_2)$	2	I_3^8
255	$C_6 \times C_2$	$K(\sqrt{5}, \sqrt[3]{(9+\sqrt{85})/2})$	$K_1(\sqrt{(5+2\sqrt{-3})(2+\sqrt{5})})$	2	$Q_8 \times C_3$
260	$C_4 \times C_2$	$K(\sqrt{5}, \sqrt{8+\sqrt{65}})$		2	M_{16}
276	$C_4 \times C_2$	$K(\sqrt{-1}, \sqrt{13+8\sqrt{3}})$	$K_1(\alpha_1)$	2	$Q_{12} \times C_2$
280	V_4	$K(\sqrt{-7}, \sqrt{5})$		2	Q_{16}
283	C_3	$K(\alpha_{31})$	$K_1(\beta_1)$	3	$\widetilde{A_4}$
295	C_8		$K_1(\alpha_4)$	2	I_3^8
299	C_8		$K_1(\alpha_1)$	2	I_3^8
312	V_4	$K(\sqrt{-3}, \sqrt{2})$		2	Q_{16}
331	C_3	$K(\alpha_{36})$	$K_1(\beta_2)$	3	$\widetilde{A_4}$
340	V_4	$K(\sqrt{-1}, \sqrt{5})$		2	SD_{16}
355	C_4	$K(\sqrt{-3+4\sqrt{5}})$		2	Q_{28}
372	V_4	$K(\sqrt{-1}, \sqrt{-3})$	$K_1(\alpha_2)$	2	D_6
376	C_8		$K_1(\gamma_1)$	2	I_5^8
391	C_{14}		$K_1(\alpha_1)$	2	$D_3 \times C_7$
395	C_8		$K_1(\gamma_2)$	2	I_5^8
403	C_2	$K(\sqrt{13})$	$K_1(\alpha_2)$	2	D_3
408	V_4	$K(\sqrt{-3}, \sqrt{2})$	$K_1(\sqrt{-(5+\sqrt{17})/2})$	2	D_4
415	C_{10}	$K(\sqrt{5}, \gamma_{18})$	$K_1(\alpha_6)$	2	$D_3 \times C_5$
420	C_2^3	$K(\sqrt{-1}, \sqrt{-3}, \sqrt{5})$		2	$32\Gamma_4 c_3$

In the above table, K_1 is the (first) Hilbert class field of K and K_2 is the second Hilbert class field (Hilbert class field of K_1) of K. The constant l is the length of the class field tower, i.e., the smallest number l such that $K_l = K_{l+1}$, provided that such l exists.

He also gives examples of unramified non-solvable extensions of K. The following is the first example.

Proposition 1.1. *The field $\mathbb{Q}(\sqrt{-1507})$ is the first imaginary quadratic number field having an unramified A_5-extension which is normal over $\mathbb{Q}$ in the sense that none of $\mathbb{Q}(\sqrt{d})$ of discriminant d with $0 > d > -1507$ has such an extension. Moreover, such an extension of $K = \mathbb{Q}(\sqrt{-1507})$ is given by the composite field of K with the splitting field of the quintic polynomial $x^5 - 5x^3 + 5x^2 + 24x + 4$, which is an A_5-extension of $\mathbb{Q}$.*

Our research focuses on maximal unramified extensions of cyclic cubic fields. We follow his ideas but use the unconditional discriminant bounds of Moreno [8] to determine cyclic cubic fields having no non-solvable unramified extensions. That will imply the maximal unramified solvable extensions, which are also the top of the class field tower, are the maximal unramified extensions. We give several examples of cyclic cubic fields with non-solvable unramified extensions as well. We also use a theorem of Roquette (see [5]), developed from the method of Golod-Shafarevich, to construct cyclic cubic fields in which the unramified extension is of infinite degree. Some results by Cohen [2] on cyclic cubic fields are also very useful and important to our construction of certain examples.

1.1 Preliminaries I

All of the results in this section can be found in most introductory books on algebraic number theory, such as Marcus [6].

Let K be a number field over $\mathbb{Q}$ and let $\mathcal{O}_K$ be the ring of integers in K. Let L be a number field containing K and let $\mathcal{O}_L$ be the ring of integers in L. Let P be a prime in $\mathcal{O}_K$. Then the ideal $P\mathcal{O}_L$ in $\mathcal{O}_L$ factors uniquely into prime ideals in $\mathcal{O}_L$, i.e. $P\mathcal{O}_L = {Q_1}^{e_1}{Q_2}^{e_2}...{Q_g}^{e_g}$. The exponent e_i of Q_i is called the *ramification index* of Q_i over P, denoted by $e(Q_i|P)$.

Definition 1.2. A prime P is *ramified* if $e_i > 1$ for some i. The prime P *splits* if $g > 1$. The prime P is *inert* (remains prime) if $g = 1$ and $e_1 = 1$.

Here we also give some definitions from Cox [3] about infinite primes.

Definition 1.3. Prime ideals of $\mathcal{O}_K$ are often called *finite primes* to distinguish them from the *infinite primes*, which are determined by the embeddings of K into $\mathbb{C}$. A *real infinite prime* is an embedding $\sigma : K \to \mathbb{R}$, while a *complex infinite prime* is a pair of complex conjugate embeddings $\sigma, \overline{\sigma} : K \to \mathbb{C}$, $\sigma \neq \overline{\sigma}$. Given an extension L/K, an infinite prime σ of K *ramifies* in L provided that σ is real but it has an extension to L which is complex.

For example, the infinite prime of $\mathbb{Q}$ is unramified in $\mathbb{Q}(\sqrt{2})$ but ramified in $\mathbb{Q}(\sqrt{-2})$. We say L is an *unramified extension* of K if L is unramified at all primes, finite or infinite.

Definition 1.4. Let P be a prime of $\mathcal{O}_K$ and Q be a prime of $\mathcal{O}_L$. The fields $\mathcal{O}_K/P$ and $\mathcal{O}_L/Q$ are called the *residue fields* associated with P and Q, respectively. The degree f of $\mathcal{O}_L/Q$ over $\mathcal{O}_K/P$ is called the inertial degree of Q over P, denoted by $f(Q|P)$.

Proposition 1.5. *If $U \subset P \subset Q$ are primes in three number rings $\mathcal{O}_F \subset \mathcal{O}_K \subset \mathcal{O}_L$, then $e(Q|U) = e(Q|P)e(P|U)$ and $f(Q|U) = f(Q|P)f(P|U)$.*

Proof. Let the factorization of U in $\mathcal{O}_K$ be $P^{e(P|U)}P_2^{e_{P_2}}...P_n^{e_{P_n}}$ and the factorization of P in $\mathcal{O}_L$ be $Q^{e(Q|P)}Q_2^{e_{Q_2}}...Q_r^{e_{Q_r}}$. Since every prime of $\mathcal{O}_L$ lies over a unique prime of $\mathcal{O}_K$ and every prime of $\mathcal{O}_K$ lies over a unique prime of $\mathcal{O}_F$, the factorization of U in $\mathcal{O}_L$ looks like $[Q^{e(Q|P)}Q_2^{e_{Q_2}}...Q_r^{e_{Q_r}}]^{e(P|U)}[...]^{e_{P_2}}...[...]^{e_{P_n}}$. Thus, $e(Q|U) = e(Q|P)e(P|U)$.
And $f(Q|U) = [\mathcal{O}_L/Q : \mathcal{O}_F/U] = [\mathcal{O}_L/Q : \mathcal{O}_K/P][\mathcal{O}_K/P : \mathcal{O}_F/U] = f(Q|P)f(P|U)$. □

The following proposition can be found in Marcus [6]. It relates an important relation between the degree of L over K and the ramification indices and inertial degrees.

Proposition 1.6. *Let n be the degree of L over K and let $Q_1, ..., Q_g$ be the primes of $\mathcal{O}_L$ over a prime P of $\mathcal{O}_K$. Denote by $e_1, ..., e_g$ and $f_1, ..., f_g$ the corresponding ramification indices and inertial degrees. Then $\sum_{i=1}^{g} e_i f_i = n$.*

Proposition 1.7. *If L is normal over K and Q and Q' are two primes lying over P, then $e(Q|P) = e(Q'|P) = e$ and $f(Q|P) = f(Q'|P) = f$. Moreover, $efg = n$.*

Proof. Let $P = Q^{e(Q|P)}Q'^{e(Q'|P)}Q_3^{e_{P_3}}...Q_n^{e_{P_n}}$. Let $G = \text{Gal}(\mathcal{O}_L/\mathcal{O}_K)$. We know that G permutes the primes lying over P and $\sigma(Q) = Q'$ for some $\sigma \in G$. Thus, $P = \sigma(P) = Q'^{e(Q|P)}\sigma(Q')^{e(Q'|P)}\sigma(Q_3)^{e_{P_3}}...\sigma(Q_n)^{e_{P_n}}$ and $e(Q|P) = e(Q'|P)$.

We define $\overline{\sigma} : \mathcal{O}_L/Q \to \mathcal{O}_L/Q'$ by $\overline{\sigma}(x + Q) = \sigma(x) + Q'$ where σ is the specific element in G such that $\sigma(Q) = Q'$ as above. This function is a well-defined function. To show it is one-to-one, we suppose $\overline{\sigma}(x_1 + Q) = \overline{\sigma}(x_2 + Q)$. Then $\sigma(x_1) + Q' = \sigma(x_2) + Q'$ and $\sigma(x_1) - \sigma(x_2) = \sigma(x_1 - x_2) \in Q'$. Thus, $x_1 - x_2 \in Q$ and so $x_1 + Q = x_2 + Q$. This shows $\overline{\sigma}$ is one-to-one. Also, for any $y + Q' \in \mathcal{O}_L/Q'$, $\exists \sigma^{-1}(y) + Q \in \mathcal{O}_L/Q$ where $\sigma^{-1} \in G$ such that $\overline{\sigma}(\sigma^{-1}(y) + Q) = \sigma(\sigma^{-1}(y)) + Q' = y + Q'$. This shows $\overline{\sigma}$ is onto. It is clearly a field homomorphism as it preserves addition and multiplication. Therefore, $\mathcal{O}_L/Q \cong \mathcal{O}_L/Q'$ and $f(Q|P) = f(Q'|P) = f$. □

So if we have a cyclic cubic field K over $\mathbb{Q}$ and if $p \in \mathbb{Z}$ is ramified in K, then $p = P^3$ for some prime P in K and $e(P|p) = 3$. Moreover, if L is an unramified extension over K and Q is a prime in L over P, $e(Q|P) = 1$ and $e(Q|p) = e(P|p) = 3$.

Definition 1.8. Let K be a number field. Let $\alpha_1, ..., \alpha_n$ be an integral basis for K and let $\sigma_1, ..., \sigma_n$ be the n embeddings of K in $\mathbb{C}$. The *discriminant* of K is defined to be

$$\text{disc}(K) = \text{disc}(\alpha_1, ..., \alpha_n) = |\sigma_i(\alpha_j)|^2$$

which is an invariant of K.

Definition 1.9. The *root discriminant* of K is defined to be

$$rd_K = |disc(K)|^{1/[K:\mathbb{Q}]}.$$

The following proposition can be found in Marcus [6]. From it, we know what primes in $\mathbb{Z}$ are ramified in K if we know the discriminant of K.

Proposition 1.10. *Let p be a prime in $\mathbb{Z}$. Then p is ramified in $\mathcal{O}_K$ if and only if $p \mid \mathrm{disc}(K)$.*

Here we quote a proposition from Neukirch [9] which we will use.

Proposition 1.11. *Let $F \subset K \subset L$. Let $\triangle$ denote the relative discriminant and $\mathcal{N}$ denote the relative norm. We have $\triangle_{L/F} = \mathcal{N}_{K/F}(\triangle_{L/K})\triangle_{K/F}^{[L:K]}$.*

Corollary 1.12. *If L is an unramified extension of K, then $\triangle_{L/\mathbb{Q}} = \triangle_{K/\mathbb{Q}}^{[L:K]}$ and the root discriminant rd_L of L is the same as the root discriminant rd_K of K.*

Proof. Let $m = [K : \mathbb{Q}]$ and $n = [L : K]$. By Proposition 1.11, $\triangle_{L/\mathbb{Q}} = \mathcal{N}_{K/\mathbb{Q}}(\triangle_{L/K})\triangle_{K/\mathbb{Q}}^{[L:K]}$. Since L over K is unramified, no prime in K divides $\triangle_{L/K}$ and $\triangle_{L/K}$ is the unit ideal. Then $\mathcal{N}_{K/\mathbb{Q}}(\triangle_{L/K}) = 1$. Thus, $rd_L = \triangle_{L/\mathbb{Q}}^{\frac{1}{mn}} = (\triangle_{K/\mathbb{Q}}^{n})^{\frac{1}{mn}} = \triangle_{K/\mathbb{Q}}^{\frac{1}{m}} = rd_K$. □

Thus, we see that if L is an unramified extension over K, then $p \in \mathbb{Z}$ divides $\mathrm{disc}(L)$ if and only if p divides $\mathrm{disc}(K)$.

Now, we will look at a proposition of Marcus [6] which tells us necessary and sufficient conditions for when a prime splits completely in a subfield of cyclotomic field. Let $\mathbb{Q}(\zeta)$ be a cyclotomic field with $\zeta = e^{2\pi i/p}$. We know that the Galois group G of $\mathbb{Q}(\zeta)$ is cyclic of order $p-1$, hence there is a unique subfield $F_d \subset \mathbb{Q}(\zeta)$ having degree d over $\mathbb{Q}$, for each divisor d of $p-1$.

Proposition 1.13. *Let p be an odd prime, and let q be any prime $\neq p$. Fix a divisor d of $p-1$. Then q is a d-th power $\bmod p$ if and only if q splits completely in F_d.*

1.2 Preliminaries II - Class Field Theory

We now give some definitions and theorems from class field theory, which can be found in Cox [3].

Definition 1.14. A *fractional ideal* $\mathfrak{a}$ of K is a nonzero finitely generated $\mathcal{O}_K$-submodule of K.

We list some properties of fractional ideals found in Cox [3].

(1) Any fractional ideal can be written in the form αI where $\alpha \in K$ and I is an ideal of $\mathcal{O}_K$.

(2) Any fractional ideal $\mathfrak{a}$ is invertible, i.e., there is a fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}_K$.

(3) Any fractional ideal $\mathfrak{a}$ can be written uniquely as a product $\mathfrak{a} = \displaystyle\prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$, where the $\mathfrak{p}_i$'s are distinct prime ideals of $\mathcal{O}_K$, and the a_i are integers.

(4) Let I_K denote the set of all fractional ideals of K. The set I_K is closed under multiplication and I_K is an Abelian group under this operation. The subset P_K (i.e., those of all principal fractional ideals of the form $\alpha\mathcal{O}_K$ for some $\alpha \in K^*$) forms a subgroup. The quotient I_K/P_K is the *ideal class group* and is denoted by $\mathcal{C}_K$. The order of the ideal class group is called the *class number* and is denoted by h_K (or $h(K)$).

We will now introduce the Hilbert class field of K and the relation between the Hilbert class field and the ideal class group. The following propositions are found in Cox [3].

Proposition 1.15. *Given a number field K, there is a finite Galois extension L of K such that:*

(i) The field L is an unramified Abelian extension of K.

(ii) Any unramified Abelian extension of K lies in L.

The field L of Proposition 1.15 is called the *Hilbert class field* of K. It is the maximal unramified Abelian extension of K and is unique. To see the relation between the Hilbert class field and the ideal class group, we introduce a map, called the Artin map. We first define the Artin symbol.

Lemma 1.16. *Let L/K be a Galois extension, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ which is unramified in L. If $\mathfrak{P}$ is a prime of $\mathcal{O}_L$ containing $\mathfrak{p}$, then there is a unique element $\sigma \in \mathrm{Gal}(L/K)$ such that for all α in $\mathcal{O}_L$,*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}},$$

where $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ is the norm of $\mathfrak{p}$.

The unique element σ of Lemma 1.16 is called the *Artin symbol* and is denoted $((L/K)/\mathfrak{P})$ since it depends on the prime $\mathfrak{P}$ of L. When L is an Abelian extension of K, the Artin symbol $((L/K)/\mathfrak{P})$ depends only on the underlying prime $\mathfrak{p}$ because of the following property:

If $\sigma \in \mathrm{Gal}(L/K)$, then

$$\left(\frac{(L/K)}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{(L/K)}{\mathfrak{P}}\right) \sigma^{-1}.$$

So the Artin symbol can be written as $((L/K)/\mathfrak{p})$.

Now we can extend the definition of Artin symbol. When L is an unramified Abelian extension, $((L/K)/\mathfrak{p})$ is defined for all primes $\mathfrak{p}$ of $\mathcal{O}_K$. If I_K is the set of all fractional ideals, then for any $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i} \in I_K$ we can define the Artin symbol $((L/K)/\mathfrak{a})$ to be the product

$$\left(\frac{(L/K)}{\mathfrak{a}}\right) = \prod_{i=1}^{r} \left(\frac{(L/K)}{\mathfrak{p}_i}\right)^{a_i}.$$

The Artin symbol thus defines a homomorphism, called the *Artin map* ,

$$\left(\frac{(L/K)}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K).$$

The *Artin reciprocity theorem* for the Hilbert class field relates the Hilbert class field to the ideal class group $\mathcal{C}_K$ as follows:

Theorem 1.17. *If L is the Hilbert class field of a number field K, then the Artin map*

$$\left(\frac{(L/K)}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K)$$

is surjective, and its kernel is exactly the subgroup P_K of principal fractional ideals. Thus the Artin map induces an isomorphism

$$\mathcal{C}_K \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

If we apply Galois theory to Proposition 1.15 and Theorem 1.17, we get the following classification of unramified Abelian extensions of K.

Corollary 1.18. *Given a number field K, there is a one-to-one correspondence between unramified Abelian extensions M of K and subgroups H of the ideal class group $\mathcal{C}_K$. Furthermore, if the extension M corresponds to the subgroup H, then the Artin map induces an isomorphism*

$$\mathcal{C}_K/H \xrightarrow{\sim} \mathrm{Gal}(M/K).$$

All these results are the special case and consequences of the Existence Theorem and Isomorphy Theorem from class field theory which will not be stated here.

Chapter 2. Cyclic Cubic Fields

This whole chapter is mostly a reproduction of results from Cohen [2] with many of the details reproduced here for completeness. Let K be a number field of degree 3 over $\mathbb{Q}$, i.e. a cubic field. If K is Galois over $\mathbb{Q}$, its Galois group must be isomorphic to the cyclic group $\mathbb{Z}/3\mathbb{Z}$. Hence, we say that K is a cyclic cubic field. The Galois group has an identity element and two other elements which are inverses of each other. We denote them by σ and $\sigma^{-1} = \sigma^2$.

Proposition 2.1. *Let $K = \mathbb{Q}(\theta)$ be a cubic field, where θ is an algebraic integer whose minimal polynomial will be denoted $P(X)$. Then K is a cyclic cubic field if and only if the discriminant of P is a square.*

Proof. Since $\mathrm{Gal}(K/\mathbb{Q})$ is a subgroup of S_3, $\mathrm{Gal}(K/\mathbb{Q}) \cong A_3 (= \mathbb{Z}_3)$ or S_3. By a proposition of Cohen [2], we know that $\mathrm{Gal}(P) \subset A_n$ if and only if $\mathrm{disc}(P)$ is a square, where P is the minimal polynomial of θ for $K = \mathbb{Q}(\theta)$. Thus, K is a cyclic cubic field if and only if the discriminant of P is a square. □

Let K be a cyclic cubic field. Let θ be an algebraic integer such that $K = \mathbb{Q}(\theta)$, and let $P(X) = X^3 - SX^2 + TX - N$ be the minimal polynomial of θ, with integer coefficients S, T and N. Since any cubic field has at least one real embedding and since K is Galois, all the roots of P must be in K. Hence, they must all be real, so a cyclic cubic field must be totally real.

2.1 General Parametric Description of Cyclic Cubic Fields

From Cohen [2], we know we can describe cyclic cubic fields parametrically. First, we set $\zeta = e^{2\pi i/3}$, i.e. a primitive cube root of unity. Since K is totally real, $\zeta \notin K$, hence the extension field $K(\zeta)$ is a degree six field over $\mathbb{Q}$. The field $K(\zeta)$ is still Galois over $\mathbb{Q}$

because it is the composite of two Galois extensions over $\mathbb{Q}$. The Galois group is generated by commuting elements σ and τ, where σ acts on K by permuting the roots of $P(X)$ transitively and trivially on ζ, and τ denotes complex conjugation. Then, the first result we need is as follows.

Lemma 2.2. *Set $\gamma = \theta + \zeta^2\sigma(\theta) + \zeta\sigma^2(\theta) \in K(\zeta)$, and $\beta = \gamma^2/\tau(\gamma)$. Then $\beta \in \mathbb{Q}(\zeta)$ and we have*

$$P(X) = X^3 - SX^2 + \frac{S^2 - e}{3}X - \frac{S^3 - 3Se + eu}{27},$$

where $e = \beta\tau(\beta)$ and $u = \beta + \tau(\beta)$ (i.e. e and u are the norm and trace of β considered as an element of $\mathbb{Q}(\zeta)$).

Proof. We have $\tau(\gamma) = \tau(\theta) + \tau(\zeta^2)\tau(\sigma(\theta)) + \tau(\zeta)\tau(\sigma^2(\theta)) = \theta + \zeta\sigma(\theta) + \zeta^2\sigma^2(\theta)$. One sees immediately that $\sigma(\gamma) = \sigma(\theta) + \sigma(\zeta^2)\sigma(\sigma(\theta)) + \sigma(\zeta)\sigma(\sigma^2(\theta)) = \sigma(\theta) + \zeta^2\sigma^2(\theta) + \zeta\theta = \zeta(\theta + \zeta^2\sigma(\theta) + \zeta\sigma^2(\theta)) = \zeta\gamma$. Hence, $\sigma(\beta) = \dfrac{\sigma(\gamma^2)}{\sigma(\tau(\gamma))} = \dfrac{\zeta^2\gamma^2}{\zeta^2\tau(\gamma)} = \dfrac{\gamma^2}{\tau(\gamma)} = \beta$.

Thus, β is invariant under the action of σ, so by Galois theory β must belong to the quadratic subfield $\mathbb{Q}(\zeta)$ of $K(\zeta)$. In particular, e and u as defined above are in $\mathbb{Q}$. Also, $e = \beta\tau(\beta) = \dfrac{\gamma^2}{\tau(\gamma)} \cdot \dfrac{[\tau(\gamma)]^2}{\tau^2(\gamma)} = \gamma\tau(\gamma)$, and $eu = \gamma\tau(\gamma)\left(\dfrac{\gamma^2}{\tau(\gamma)} + \dfrac{[\tau(\gamma)]^2}{\gamma}\right) = \gamma^3 + [\tau(\gamma)]^3$.

Now we have the matrix equations:

$$\begin{pmatrix} S \\ \gamma \\ \tau(\gamma) \end{pmatrix} = \begin{pmatrix} \theta + \sigma(\theta) + \sigma^2(\theta) \\ \theta + \zeta^2\sigma(\theta) + \zeta\sigma^2(\theta) \\ \theta + \zeta\sigma(\theta) + \zeta^2\sigma^2(\theta) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta^2 & \zeta \\ 1 & \zeta & \zeta^2 \end{pmatrix} \begin{pmatrix} \theta \\ \sigma(\theta) \\ \sigma^2(\theta) \end{pmatrix}.$$

Hence,

$$\begin{pmatrix} \theta \\ \sigma(\theta) \\ \sigma^2(\theta) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta^2 & \zeta \\ 1 & \zeta & \zeta^2 \end{pmatrix}^{-1} \begin{pmatrix} S \\ \gamma \\ \tau(\gamma) \end{pmatrix} = \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 \\ 1 & \zeta^2 & \zeta \end{pmatrix} \begin{pmatrix} S \\ \gamma \\ \tau(\gamma) \end{pmatrix}.$$

Thus,

$$\begin{aligned}\theta &= \frac{1}{3}(S+\gamma+\tau(\gamma)),\\ \sigma(\theta) &= \frac{1}{3}(S+\zeta\gamma+\zeta^2\tau(\gamma)), \text{and}\\ \sigma^2(\theta) &= \frac{1}{3}(S+\zeta^2\gamma+\zeta\tau(\gamma)).\end{aligned}$$

We compute that

$$\begin{aligned}T =&\theta\sigma(\theta)+\theta\sigma^2(\theta)+\sigma(\theta)\sigma^2(\theta)\\ =&\frac{1}{9}[(S+\gamma+\tau(\gamma))(S+\zeta\gamma+\zeta^2\tau(\gamma))+(S+\gamma+\tau(\gamma))(S+\zeta^2\gamma+\zeta\tau(\gamma))\\ &+(S+\zeta\gamma+\zeta^2\tau(\gamma))(S+\zeta^2\gamma+\zeta\tau(\gamma))]\\ =&\frac{1}{9}[S^2+\zeta S\gamma+\zeta^2 S\tau(\gamma)+S\gamma+\zeta\gamma^2+\zeta^2\gamma\tau(\gamma)+S\tau(\gamma)+\zeta\gamma\tau(\gamma)+\zeta^2[\tau(\gamma)]^2\\ &+S^2+\zeta^2 S\gamma+\zeta S\tau(\gamma)+S\gamma+\zeta^2\gamma^2+\zeta\gamma\tau(\gamma)+S\tau(\gamma)+\zeta^2\gamma\tau(\gamma)+\zeta[\tau(\gamma)]^2\\ &+S^2+\zeta^2 S\gamma+\zeta S\tau(\gamma)+\zeta S\gamma+\gamma^2+\zeta^2\gamma\tau(\gamma)+\zeta^2 S\tau(\gamma)+\zeta\gamma\tau(\gamma)+[\tau(\gamma)]^2\\ =&\frac{1}{9}[3S^2+2S\gamma(1+\zeta+\zeta^2)+2S\tau(\gamma)(1+\zeta+\zeta^2)+\gamma^2(1+\zeta+\zeta^2)+[\tau(\gamma)]^2(1+\zeta+\zeta^2)\\ &+3\gamma\tau(\gamma)(\zeta+\zeta^2)]\\ =&\frac{1}{9}(3S^2-3e)\\ =&\frac{S^2-e}{3}.\end{aligned}$$

Next we compute

$$\begin{aligned}N &= \theta\sigma(\theta)\sigma^2(\theta)\\ &= \frac{1}{27}(S+\gamma+\tau(\gamma))(S+\zeta\gamma+\zeta^2\tau(\gamma))(S+\zeta^2\gamma+\zeta\tau(\gamma))\\ &= \frac{1}{27}[(S^2+\zeta S\gamma+\zeta^2 S\tau(\gamma)+S\gamma+\zeta\gamma^2+\zeta^2\gamma\tau(\gamma)+S\tau(\gamma)+\zeta\gamma\tau(\gamma)+\zeta^2[\tau(\gamma)]^2)(S+\zeta^2\gamma\\ &\quad+\zeta\tau(\gamma))]\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{27}[S^3 + \zeta S^2\gamma + \zeta^2 S^2\tau(\gamma) + S^2\gamma + \zeta S\gamma^2 + \zeta^2 S\gamma\tau(\gamma) + S^2\tau(\gamma) + \zeta S\gamma\tau(\gamma) + \zeta^2 S[\tau(\gamma)]^2 \\
&\quad + \zeta^2 S^2\gamma + S\gamma^2 + \zeta S\gamma\tau(\gamma) + \zeta^2 S\gamma^2 + \gamma^3 + \zeta\gamma^2\tau(\gamma) + \zeta^2 S\gamma\tau(\gamma) + \gamma^2\tau(\gamma) + \zeta\gamma[\tau(\gamma)]^2 \\
&\quad + \zeta S^2\tau(\gamma) + \zeta^2 S\gamma\tau(\gamma) + S[\tau(\gamma)]^2 + \zeta S\gamma\tau(\gamma) + \zeta^2\gamma^2\tau(\gamma) + \gamma[\tau(\gamma)]^2 + \zeta S[\tau(\gamma)]^2 \\
&\quad + \zeta^2\gamma[\tau(\gamma)]^2 + [\tau(\gamma)]^3] \\
&= \frac{1}{27}[S^3 + (S^2\gamma + S\gamma^2 + S^2\tau(\gamma) + S[\tau(\gamma)]^2 + \gamma^2\tau(\gamma) + \gamma[\tau(\gamma)]^2)(1 + \zeta + \zeta^2) \\
&\quad + 3S\gamma\tau(\gamma)(\zeta + \zeta^2) + \gamma^3 + [\tau(\gamma)]^3] \\
&= \frac{S^3 - 3Se + eu}{27}.
\end{aligned}$$

This completes the proof. □

We will modify θ (hence its minimal polynomial $P(X)$) so as to obtain a unique defining polynomial for each cyclic cubic field. But before that, we need to prove a lemma.

Lemma 2.3. *If $\mathbb{Q}(\theta)$ is a cyclic cubic field, then $\mathbb{Q}(\theta) = \mathbb{Q}(b\theta + c\sigma(\theta))$ for any b, $c \in \mathbb{Q}$, where b and c are not both zero.*

Proof. First we note that 1 and θ are linearly independent over $\mathbb{Q}$, otherwise $\theta \in \mathbb{Q}$. Now suppose 1, θ, $\sigma(\theta)$ are linearly dependent over $\mathbb{Q}$. Then $A + B\theta + C\sigma(\theta) = 0$ for some A, B, $C \in \mathbb{Q}$, but not all zero. If $C = 0$, then $A + B\theta = 0$ and $A = B = 0$. Thus $C \neq 0$. Then,

$$\begin{aligned}
B\theta + C\sigma(\theta) &= -A \\
\frac{B}{C}\theta + \sigma(\theta) &= -\frac{A}{C} \\
\sigma(\theta) &= -\frac{A}{C} + \frac{B}{C}\theta.
\end{aligned}$$

Let $x = -\dfrac{A}{C}$ and $y = \dfrac{B}{C}$. We compute

$$\sigma(\theta) = x + y\theta, \sigma^2(\theta) = x + y(x + y\theta) = (x + xy) + y^2\theta,$$

$$\theta = \sigma^3(\theta) = x + xy + y^2(x + y\theta) = x(1 + y + y^2) + y^3\theta.$$

Thus, $y = 1$, $x = 0$ because 1 and θ are linearly independent over $\mathbb{Q}$. However, $\sigma(\theta) = \theta$ is a contradiction. Thus, 1, θ, $\sigma(\theta)$ are linearly independent over $\mathbb{Q}$. Then $b\theta + c\sigma(\theta) \notin \mathbb{Q}$ if b, $c \in \mathbb{Q}$ and b, c are not both zero. Thus, $\mathbb{Q} \subset \mathbb{Q}(b\theta + c\sigma(\theta)) \subseteq \mathbb{Q}(\theta)$ and so $\mathbb{Q}(\theta) = \mathbb{Q}(b\theta + c\sigma(\theta))$. □

Now, we modify θ. First note that replacing γ by $(b + c\zeta)\gamma$ is equivalent to changing θ into $b\theta + c\sigma(\theta)$, and β is changed into $\beta\dfrac{(b+c\zeta)^2}{b+c\zeta}$.

To see this, set $\gamma' = (b + c\zeta)\gamma$. Then we compute

$$\begin{aligned}\gamma' &= (b + c\zeta)(\theta + \zeta^2\sigma(\theta) + \zeta\sigma^2(\theta))\\ &= b\theta + c\zeta\theta + b\zeta^2\sigma(\theta) + c\sigma(\theta) + b\zeta\sigma^2(\theta) + c\zeta^2\sigma^2(\theta)\\ &= b\theta + c\sigma(\theta) + \zeta^2[b\sigma(\theta) + c\sigma^2(\theta)] + \zeta[c\theta + b\sigma^2(\theta)]\\ &= b\theta + c\sigma(\theta) + \zeta^2\sigma(b\theta + c\sigma(\theta)) + \zeta(b\theta + c\sigma(\theta)).\end{aligned}$$

Let $\theta' = b\theta + c\sigma(\theta)$. Then $\gamma' = \theta' + \zeta^2\sigma(\theta') + \zeta\sigma^2(\theta')$. Also,

$$\beta' = \frac{\gamma'^2}{\tau(\gamma')} = \frac{(b+c\zeta)^2\gamma^2}{\tau((b+c\zeta)\gamma)} = \frac{(b+c\zeta)^2\gamma^2}{\tau(\gamma)(b+c\zeta^2)} = \beta\frac{(b+c\zeta)^2}{(b+c\zeta^2)}.$$

Now, let $\{p_k\}$ be the set of primes which split in $\mathbb{Q}(\zeta)$ (they are the primes whose factorization looks like $p_k = \pi_k\overline{\pi_k}$). By Proposition 1.13, if we choose $p = 3$, $q = p_k$ and $d = 2$, then p_k splits completely in $F_2 = \mathbb{Q}(\zeta)$ if and only if p_k is a square mod 3, i.e. $p_k \equiv 1 \pmod 3$. Let $\{q_k\}$ be the set of inert primes, i.e. primes such that $q_k \equiv 2 \pmod 3$. Note that 3 is the only prime ramified in $\mathbb{Q}(\zeta)$ because the discriminant of $\mathbb{Q}(\zeta)$ is -3. Let $\rho = 1 + 2\zeta = \sqrt{-3}$

denote the prime above 3. Then, we can write

$$b + c\zeta = (-\zeta)^g \rho^f \prod {\pi_k}^{e_k} \prod \overline{\pi_k}^{f_k} \prod {q_k}^{g_k}.$$

Hence, since $b + c\zeta^2 = \overline{b + c\zeta}$, we have

$$\begin{aligned}\frac{(b+c\zeta)^2}{b+c\zeta^2} &= \frac{(-\zeta)^{2g}\rho^{2f}\prod {\pi_k}^{2e_k}\prod \overline{\pi_k}^{2f_k}\prod {q_k}^{2g_k}}{(-\zeta^2)^g(-\rho)^f\prod \overline{\pi_k}^{e_k}\prod {\pi_k}^{f_k}\prod {q_k}^{g_k}} \\ &= (-1)^{g+f}\rho^f \prod {\pi_k}^{2e_k - f_k} \prod \overline{\pi_k}^{2f_k - e_k} \prod {q_k}^{g_k}.\end{aligned}$$

If the decomposition of β is

$$(-\zeta)^n \rho^m \prod {\pi_k}^{l_k} \prod \overline{\pi_k}^{m_k} \prod {q_k}^{n_k},$$

then choose $g_k = -n_k$ and $f = -m$. Thus,

$$\beta \frac{(b+c\zeta)^2}{(b+c\zeta^2)} = (-1)^{g+f+n}\zeta^n \prod {\pi_k}^{l_k + 2e_k - f_k} \prod \overline{\pi_k}^{m_k + 2f_k - e_k}.$$

Furthermore, for each k consider the quantity $m_k + 2l_k$.

Case(1): If $m_k + 2l_k \equiv 0$ or $1 \pmod 3$, choose $e_k = \left\lfloor \frac{-m_k - 2l_k + 1}{3} \right\rfloor$ and $f_k = l_k + 2e_k$. Then,

$$\pi_k^{l_k+2e_k-f_k}\overline{\pi_k}^{m_k+2f_k-e_k} = \overline{\pi_k}^{m_k+2l_k+3e_k} = \overline{\pi_k}^{m_k+2l_k+3\left\lfloor \frac{-m_k-2l_k+1}{3}\right\rfloor}.$$

Let $m_k + 2l_k = 3M$ or $3M+1$. Then $-m_k - 2l_k + 1 = -3M+1$ or $-3M$. So, $3\left\lfloor \frac{-m_k - 2l_k + 1}{3} \right\rfloor = 3\left\lfloor -M + \frac{1}{3} \right\rfloor = -3M$ or $3\lfloor -M \rfloor = -3M$. Then, $m_k + 2l_k + 3\left\lfloor \frac{-m_k - 2l_k + 1}{3} \right\rfloor = 0$ or 1. Thus,

$$\pi_k^{l_k+2e_k-f_k}\overline{\pi_k}^{m_k+2f_k-e_k} = 1 \text{ or } \overline{\pi_k}.$$

Case(2): If $m_k + 2l_k \equiv 2 \pmod 3$, then $l_k + 2m_k \equiv 1 \pmod 3$, and we choose $f_k =$

$\left\lfloor\dfrac{-l_k-2m_k+1}{3}\right\rfloor$ and $e_k = m_k + 2f_k$. Then,

$$\pi_k^{l_k+2e_k-f_k}\overline{\pi_k}^{m_k+2f_k-e_k} = \pi_k^{l_k+2m_k+3f_k} = \pi_k^{l_k+2m_k+3\left\lfloor\frac{-l_k-2m_k+1}{3}\right\rfloor}.$$

Letting $l_k + 2m_k = 3M + 1$, then $-l_k - 2m_k = -3M - 1$, $-l_k - 2m_k + 1 = -3M$. So $3\left\lfloor\dfrac{-l_k-2m_k+1}{3}\right\rfloor = -3M$. Hence, $l_k + 2m_k + 3\left\lfloor\dfrac{-l_k-2m_k+1}{3}\right\rfloor = 3M + 1 - 3M = 1$. Thus,

$$\pi_k^{l_k+2e_k-f_k}\overline{\pi_k}^{m_k+2f_k-e_k} = \pi_k.$$

With this choice of exponents, $\beta' \in \mathbb{Z}[\zeta]$ because π_k and $\overline{\pi_k}$ are in $\mathbb{Z}[\zeta]$. Also, β' is not divisible by any inert or ramified prime, and is divisible by split primes only to the first power. Also, at most one of π_k or $\overline{\pi_k}$ divides β'. In other words, if $e' = \beta'\tau(\beta')$ is the new value of the norm of β', then e' is equal to a product of distinct primes congruent to 1 modulo 3.

Now, $K = \mathbb{Q}(\theta) = \mathbb{Q}(\theta')$ and θ' is a root of the polynomial $F(X) = X^3 - S'X^2 + T'X - N'$ and by Lemma 2.2, $F(X) = X^3 - S'X^2 + \dfrac{S'^2 - e'}{3}X - \dfrac{S'^3 - 3S'e' + e'u'}{27}$.

Consider $Q(X) = F\left(X + \dfrac{S'}{3}\right)$

$$= \left(X + \frac{S'}{3}\right)^3 - S'\left(X + \frac{S'}{3}\right)^2 + \frac{S'^2 - e'}{3}\left(X + \frac{S'}{3}\right) - \frac{S'^3 - 3S'e' + e'u'}{27}$$

$$= X^3 + S'X^2 + \frac{S'^2}{3}X + \frac{S'^3}{27} - S'X^2 - \frac{2S'^2}{3}X - \frac{S'^3}{9} + \frac{S'^2}{3}X - \frac{e'}{3}X + \frac{S'^3}{9} - \frac{S'e'}{9} - \frac{S'^3}{27} + \frac{S'e'}{9} - \frac{e'u'}{27}$$

$= X^3 - \dfrac{e'}{3}X - \dfrac{e'u'}{27}$ and let $\theta'' = \theta' - \dfrac{S'}{3}$ be a root of $Q(X)$.

Consider $T(X) = 27Q\left(\dfrac{X}{3}\right) = 27\left(\dfrac{X^3}{27} - \dfrac{e'}{9}X - \dfrac{e'u'}{27}\right) = X^3 - 3e'X - e'u'$. Since $\beta' = \dfrac{u' + v'\sqrt{-3}}{2}$ and β' is not divisible by the ramified prime ρ, u' cannot be divisible by 3. Otherwise, ρ divides u' and $v'\sqrt{-3}$ and thus divides β'. Then, by suitably choosing the exponent g above (which amounts to changing β' into $-\beta'$), we may assume $u' \equiv 2 \pmod 3$.

In our process, because we want e' to be equal to a product of primes congruent to 1 modulo 3, b and c are chosen uniquely and thus β' is unique, hence so are e' and u'. We restate this in the following proposition.

Proposition 2.4. *For any cyclic cubic field K, there exists a unique pair of integers e and u such that e is equal to a product of distinct primes congruent to* 1 *modulo* 3*,* $u \equiv 2 \pmod 3$ *and such that $K = \mathbb{Q}(\theta')$ where θ' is a root of the polynomial $Q(X) = X^3 - \frac{e}{3}X - \frac{eu}{27}$, or equivalently $K = \mathbb{Q}(\theta)$ where θ is a root of $P(X) = 27Q(X/3) = X^3 - 3eX - eu$.*

Example 2.5. Consider the cyclic cubic field represented by

$$P(x) = x^3 + 273x^2 - 1911x - 206297.$$

By Lemma 2.2, we find that $\beta = -\frac{1140}{7}\zeta - \frac{2118}{7}$, $e = 68796$ and $u = -\frac{3096}{7}$. When we factor β, we get $\beta = (\sqrt{-3})^3(3+2\zeta)^{-1}(1-2\zeta)^3(3-\zeta)(2)$. The first factor is the prime above 3, the second and third factors are primes above 7. The fourth factor is a prime above 13. The last factor is an inert prime. So we have $n = 4$, $m = 3$, $n_1 = 1$, $l_1 = -1$, $m_1 = 3$, $l_2 = 1$, $m_2 = 0$. So we choose $g_1 = -1$, $f = -3$, $e_1 = 0$, $f_1 = -1$, $e_2 = 0$, $f_2 = 0$. Then we have $b + c\zeta = (-\zeta)^g(\sqrt{-3})^{-3}(1-2\zeta)^{-1}$ and $\beta' = \beta\frac{(c+b\zeta)^2}{(b+c\zeta^2)} = (-1)^{g+1}(-\zeta)^4(1-2\zeta)(3-\zeta) = (-1)^{g+1}\left(\frac{8+10i\sqrt{3}}{2}\right)$. We then choose $g = 1$. We get $\beta' = \frac{8+10i\sqrt{3}}{2}$. So $e' = 91 = (7)(13)$ and $u' = 8$. The canonical defining polynomial is then $P(X) = X^3 - 3(91)X - (91)(8) = X^3 - 273X - 728$.

Example 2.6. Consider the cyclic cubic field represented by

$$P(x) = x^3 + 551x^2 - 2677272958x - 53771714527237.$$

By Lemma 2.2, we find that $\beta = -\frac{45205665}{10921}\zeta + \frac{955376950}{10921}$, $e = 8032122475$ and $u = \frac{1955959565}{10921}$. When we factor β, we get $\beta = (-\zeta)^4(4+\zeta)(1+6\zeta)(7+9\zeta)^{-1}(2+9\zeta)^2(1+9\zeta)(-3-14\zeta)^{-1}(-11-14\zeta)^2(5)$. The first factor is a unit. The second factor is a prime above 13. The third factor is a prime above 31. The fourth and fifth factors are primes above 67. The sixth factor is a prime above 73. The seventh and eighth factors are primes above 163. The last factor is an inert prime. So we have $n = 4$, $m = 0$, $n_1 = 1$, $l_1 = 1$, $m_1 = 0$, $l_2 = 1$, $m_2 = 0$, $l_3 = -1$, $m_3 = 2$, $l_4 = 1$, $m_4 = 0$, $l_5 = -1$, $m_5 = 2$. So we choose $g_1 = -1$, $f = 0$, $e_1 = 0$, $f_1 = 0$, $e_2 = 0$, $f_2 = 0$, $e_3 = 0$, $f_3 = -1$, $e_4 = 0$, $f_4 = 0$, $e_5 = 0$, $f_5 = -1$. Then we have $b + c\zeta = (-\zeta)^g(2+9\zeta)^{-1}(-11-14\zeta)^{-1}(5)^{-1}$ and $\beta' = \beta\dfrac{(c+b\zeta)^2}{(b+c\zeta^2)} = (-1)^g\zeta^4(4+\zeta)(1+6\zeta)(1+9\zeta) = (-1)^g\left(\dfrac{343-3i\sqrt{3}}{2}\right)$. We then choose $g = 1$. We get $\beta' = \dfrac{-343+3i\sqrt{3}}{2}$. So $e' = (13)(31)(73)$ and $u' = -343$. The canonical defining polynomial is then $P(X) = X^3 - 3(13)(31)(73)X - (13)(31)(73)(-343) = X^3 - 88257X + 10090717$.

In the next section, we will prove the converse of this proposition and show examples of how to find cyclic cubic fields with a given discriminant.

2.2 Specific Parametric Description of Cyclic Cubic Fields

From the work of Cohen [2], we know that depending on whether 3 is ramified or not in K, the canonical minimal representing polynomial has different forms. We can see the following theorem due to Cohen.

Theorem 2.7. *All cyclic cubic fields K are given exactly once (up to isomorphism) in the following way:*

(1) If the prime 3 is ramified in K, then $K = \mathbb{Q}(\theta)$ where θ is a root of the equation $P(X) = X^3 - \frac{e}{3}X - \frac{eu}{27} \in \mathbb{Z}[X]$, where $e = \dfrac{u^2+27v^2}{4}$, $u \equiv 6 \pmod 9$, $3 \nmid v$, $u \equiv v \pmod 2$, $v > 0$ and $\dfrac{e}{9}$ is equal to the product of distinct primes congruent to 1 modulo 3.

(2) If the prime 3 is unramified in K, then $K = \mathbb{Q}(\theta)$ where θ is a root of the equation $P(X) = X^3 - X^2 + \dfrac{1-e}{3}X - \dfrac{1-3e+eu}{27} \in \mathbb{Z}[X]$, where $e = \dfrac{u^2+27v^2}{4}$, $u \equiv 2 \pmod 3$, $u \equiv v \pmod 2$, $v > 0$ and e is equal to the product of distinct primes congruent to 1 modulo 3.

In both cases, the discriminant of P is equal to e^2v^2 and the discriminant of the number field K is equal to e^2.

(3) Conversely, if e is equal to 9 times the product of $t-1$ distinct primes congruent to 1 modulo 3, (respectively is equal to the product of t distinct primes congruent to 1 modulo 3), then there exist up to isomorphism exactly 2^{t-1} cyclic cubic fields of discriminant e^2 defined by the polynomials $P(X)$ given in (1) (respectively (2)).

To prove this theorem, we will need in particular to compute explicit integral bases and discriminants of cyclic cubic fields. So, let K be a cyclic cubic field. By Proposition 2.4, we have $K = \mathbb{Q}(\theta)$ where θ is a root of the equation $P(X) = X^3 - 3eX - eu$, where $e = \dfrac{u^2+3v^2}{4}$, $u \equiv 2 \pmod 3$ and e is equal to a product of distinct primes congruent to 1 modulo 3.

We first quote some definitions, a proposition and a few lemmas from Cohen [2].

Definition 2.8. An order R in field K is a subring of K which as a $\mathbb{Z}$-module is finitely generated and of maximal rank $n = deg(K)$.

Definition 2.9. Let $\mathcal{O}$ be an order in a number field K and let p be a prime number. We say $\mathcal{O}$ is p-maximal if $[\mathcal{O}_K : \mathcal{O}]$ is not divisible by p.

The following proposition, called *Dedekind's criterion*, gives the conditions for $\mathbb{Z}[\theta]$ to be p-maximal. We only quote the second part that we will use.

Proposition 2.10. *Let $K = \mathbb{Q}(\theta)$ be a number field, let $T \in \mathbb{Z}[X]$ be the minimal polynomial of θ and let p be a prime number. Denote by $^-$ reduction modulo p (in $\mathbb{Z}$, $\mathbb{Z}[X]$ or $Z[\theta]$). Let $\overline{T}(X) = \prod_{i=1}^{k} \overline{t_i}(X)^{e_i}$ be the factorization of $T(X)$ modulo p in $\mathbb{F}_p[X]$, and set $g(X) = \prod_{i=1}^{k} t_i(X)$ where the $t_i \in \mathbb{Z}[X]$ are arbitrary monic lifts of $\overline{t_i}$.*

(2) Let $h(X) \in \mathbb{Z}[X]$ be a monic lift of $\overline{T}(X)/\overline{g}(X)$ and set $f(X) = (g(X)h(X) - T(X))/p \in \mathbb{Z}[X]$. Then $\mathbb{Z}[\theta]$ is p-maximal if and only if $(\overline{f}, \overline{g}, \overline{h}) = 1$ in $\mathbb{F}_p[X]$.

Lemma 2.11. *Let $p \mid e$. Then the order $\mathbb{Z}[\theta]$, where θ is a root of $X^3 - 3eX + eu$ (as in Proposition 2.4), is p-maximal.*

Proof. We apply Dedekind's criterion. Since $p \mid e$, $\overline{P}(X) = X^3$, therefore, $t_1(X) = X$, $g(X) = X$, $h(X) = X^2$ and $f(X) = \dfrac{g(X)h(X) - P(X)}{p} = \dfrac{3e}{p}X + \dfrac{eu}{p}$. Since $p \mid e$, we cannot have $p \mid u$, otherwise $p \mid v$, hence $p^2 \mid e$ which was assumed not to be true. Therefore, $p \nmid \dfrac{eu}{p}$ so $(\overline{f}, \overline{g}, \overline{h}) = 1$, showing that $\mathbb{Z}[\theta]$ is p-maximal. □

Corollary 2.12. *The discriminant of $P(X)$ is equal to $81e^2v^2$. The discriminant of the number field K is divisible by e^2.*

Proof. The discriminant of $X^3 + aX + b$ is equal to $-4a^3 - 27b^2$, hence the discriminant of P is equal to $-4(-3e)^3 - 27(eu)^2 = 27e^2(4e - u^2) = 27e^2(3v^2) = 81e^2v^2$, thus proving the first statement. For the second statement, we know that the discriminant of the field K is a square divisor of $81e^2v^2$. We also know $\operatorname{disc}(P) = \operatorname{disc}(K)f^2$ where $f = [\mathcal{O}_K : \mathbb{Z}[\theta]]$. By the preceding lemma, $\mathbb{Z}[\theta]$ is p-maximal for all primes dividing e, and e is coprime to $81v^2$. That means if $p \mid e$, $p \nmid f$ and thus $p \mid \operatorname{disc}(K)$ and $e^2 \mid \operatorname{disc}(K)$. □

Since, as we will see, the prime divisors of v other than 3 are irrelevant, what remains is to look at behavior of the prime 3.

Lemma 2.13. *Assume that $3 \nmid v$. Then $\mathbb{Z}[\theta]$ is 3-maximal.*

Proof. Again we use Dedekind's criterion. Since $eu \equiv 2 \pmod 3$, we have $\overline{P} = X^3 - eu = X^3 + 1 = (X+1)^3$ in $\mathbb{F}_3[X]$, hence $t_1 = X + 1$, $g(X) = X + 1$, $h(X) = (X+1)^2$ and $f(X) = \dfrac{(X+1)^3 - (X^3 - 3eX - eu)}{3} = X^2 + (e+1)X + \dfrac{1 + eu}{3} = (X+1)(X+e) + \dfrac{eu + 1 - 3e}{3}$. Hence $(\overline{f}, \overline{g}, \overline{h}) = (X+1, \overline{f}) = \left(X + 1, \overline{\dfrac{eu+1-3e}{3}}\right)$. Now we check that $r = \dfrac{eu + 1 - 3e}{3} = \dfrac{(u^2 + 3v^2)(u-3) + 4}{12} = \dfrac{u^2(u-3) + 3v^2(u-3) + 4}{12} = \dfrac{(u^3 - 3u^2 + 4) + 3v^2(u-3)}{12} = \dfrac{(u-2)^2(u+1) + 3v^2(u-3)}{12}$. Since $u \equiv 2 \pmod 3$, $4r \equiv v^2(u-3) \pmod 9$ and since $3 \nmid v$, $r \equiv 2 \pmod 3$ so $(\overline{f}, \overline{g}, \overline{h}) = 1$, which proves the lemma. □

Lemma 2.14. *With the above notation, let θ be a root of $P(X) = X^3 - 3eX - eu$, where $e = \dfrac{u^2 + 3v^2}{4}$ and $u \equiv 2 \pmod 3$. The conjugates of θ are given by the formulas $\sigma(\theta) = \dfrac{-2e}{v} - \dfrac{u+v}{2v}\theta + \dfrac{1}{v}\theta^2$, $\sigma^2(\theta) = \dfrac{2e}{v} + \dfrac{u-v}{2v}\theta - \dfrac{1}{v}\theta^2$.*

Proof. Let $\theta_2 = \sigma(\theta)$ and $\theta_3 = \sigma^2(\theta)$. The discriminant of $P(X) = f^2$ where $f = (\theta - \theta_2)(\theta_2 - \theta_3)(\theta_3 - \theta)$ and $f = \pm 9ev$ by Corollary 2.12. If necessary, by exchanging θ_2 and θ_3, we may assume that $\theta_2 - \theta_3 = \dfrac{9ev}{(\theta - \theta_2)(\theta - \theta_3)} = \dfrac{9ev}{P'(\theta)} = \dfrac{9ev}{(3\theta^2 - 3e)}$. Using the extended Euclidean algorithm with $A(X) = X^3 - 3eX - eu$ and $B(X) = X^2 - e$, we find the inverse of B modulo A. Thus,

$$\begin{aligned}
A(X) &= [B(X)]X - 2eX - eu \\
-\frac{1}{2e}A(X) &= -\frac{X}{2e}B(X) + X + \frac{u}{2} \\
X + \frac{u}{2} &= -\frac{1}{2e}A(X) + \frac{X}{2e}B(X).
\end{aligned}$$

And,

$$\begin{aligned}
B(X) &= \left(X + \frac{u}{2}\right)\left(X - \frac{u}{2}\right) + \frac{u^2 - 4e}{4} \\
\frac{u^2 - 4e}{4} &= B(X) - \left(-\frac{1}{2e}A(X) + \frac{X}{2e}B(X)\right)\left(X - \frac{u}{2}\right) \\
\frac{u^2 - 4e}{4} &= \frac{1}{2e}\left(X - \frac{u}{2}\right)A(X) + \left[1 - \frac{X}{2e}\left(X - \frac{u}{2}\right)\right]B(X) \\
1 &= \frac{4}{2e(u^2 - 4e)}\left(X - \frac{u}{2}\right)A(X) + \left(\frac{4}{u^2 - 4e}\right)\left[1 - \frac{X}{2e}\left(X - \frac{u}{2}\right)\right]B(X).
\end{aligned}$$

So,

$$A(X)r(X) + B(X)s(X) = 1,$$

$$\begin{aligned}
\text{where } r(X) = \frac{4}{2e(u^2 - 4e)}\left(X - \frac{u}{2}\right) \text{ and } s(X) &= \left(\frac{4}{u^2 - 4e}\right)\left[1 - \frac{X}{2e}\left(X - \frac{u}{2}\right)\right] \\
&= \frac{4}{4e - u^2}\left[\frac{X}{2e}\left(X - \frac{u}{2}\right) - 1\right] \\
&= \frac{1}{4e - u^2}\left[\frac{X}{e}(2X - u) - 4\right] \\
&= \frac{1}{3v^2e}[X(2X - u) - 4e] \\
&= \frac{2X^2 - uX - 4e}{3v^2e}.
\end{aligned}$$

Hence, $B(X)s(X) \equiv 1 \pmod{A(X)}$ and $s(X)$ is the inverse of $B(X)$ modulo $A(X)$. Also, $s(\theta) = \dfrac{1}{B(\theta)}$. Thus, $\theta_2 - \theta_3 = \dfrac{9ev}{(3\theta^2 - 3e)} = \dfrac{9ev}{3B(\theta)} = \dfrac{9ev}{3}s(\theta) = \left(\dfrac{9ev}{3}\right)\left(\dfrac{2\theta^2 - u\theta - 4e}{3v^2e}\right) = \dfrac{1}{v}(2\theta^2 - u\theta - 4e)$. Then, since $\theta + \theta_2 + \theta_3 = 0$, $\theta_2 - \theta_3 - \theta = 2\theta_2$. Hence, $\theta_2 = \dfrac{1}{2}\left(\dfrac{1}{v}(2\theta^2 - u\theta - 4e) - \theta\right) = -\dfrac{2e}{v} - \dfrac{u+v}{2v}\theta + \dfrac{1}{v}\theta^2$. And we obtain $\theta_3 = -\theta_2 - \theta = \dfrac{2e}{v} + \dfrac{u-v}{2v}\theta - \dfrac{1}{v}\theta^2$. □

Now we will prove a theorem that implies the first two statements of Theorem 2.7.

Theorem 2.15. *Let $K = \mathbb{Q}(\theta)$ be a cyclic cubic field where θ is a root of $X^3 - 3eX - eu$ and where, as above, $e = \dfrac{u^2+3v^2}{4}$ is equal to a product of distinct primes congruent to* 1 *modulo* 3.

(1) Assume that $3 \nmid v$. Then $(1, \theta, \sigma(\theta))$ (where $\sigma(\theta)$ is given by the above formula) is an integral basis of K and the discriminant of K is equal to $(9e)^2$.

(2) Assume that $3 \mid v$. Then if $\theta' = \dfrac{\theta+1}{3}$, $(1, \theta', \sigma(\theta'))$ is an integral basis of K and the discriminant of K is equal to e^2.

Proof. (1) Since $\theta^2 = v\sigma(\theta) + \dfrac{u+v}{2}\theta + 2e$, the $\mathbb{Z}$-module $\mathcal{O}$ generated by $(1, \theta, \sigma(\theta))$ contains $\mathbb{Z}[\theta]$. We also see $\mathbb{Z}[\theta] = \langle 1, \theta, v\sigma(\theta)\rangle$. Thus $[\mathcal{O} : \mathbb{Z}[\theta]] = v$. That means $81e^2v^2 = \operatorname{disc}(\mathcal{O})[\mathcal{O} : \mathbb{Z}[\theta]]^2$ and hence $\operatorname{disc}(\mathcal{O})$ is equal to $81e^2$. We know that $\mathbb{Z}[\theta]$ is 3-maximal and p-maximal for every prime dividing e. Hence, $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ is not divisible by 3 or p. Therefore, 3 and p do not divide $[\mathcal{O}_K : \mathcal{O}]$, so $\mathcal{O}$ is 3-maximal and p-maximal for every prime p dividing e. Thus, $[\mathcal{O}_K : \mathcal{O}] = 1$ and $\operatorname{disc}(K) = 81e^2$ and it follows that $\mathcal{O}$ is the maximal order and $(1, \theta, \sigma(\theta))$ is an integral basis of K.

(2) We now consider the case where $3 \mid v$. The field K can then be defined by the polynomial $Q(X) = P(3X-1)/27 = X^3 - X^2 + \dfrac{1-e}{3} - \dfrac{1-3e+eu}{27}$. Since $e \equiv 1 \pmod 3$, $u \equiv 2 \pmod 3$ and $3 \mid v$, we know $\dfrac{1-e}{3} \in \mathbb{Z}$ and $\dfrac{1-3e+eu}{27} \in \mathbb{Z}$. To see the second one, we let $u = 3n+2$ and $v = 3m$ for some n, $m \in \mathbb{Z}$. Then, $e = \dfrac{u^2+3v^2}{4} = \dfrac{(3n+2)^2+3(3m)^2}{4}$

for some n, $m \in \mathbb{Z}$. Also, $27 \mid (1-3e+eu) \iff 27 \mid (4-12e+4eu)$ and

$$\begin{aligned}4-12e+4eu =& 4-3[(3n+2)^2+3(3m)^2]+[(3n+2)^2+3(3m)^2](3n+2)\\ =&4-3(9n^2+12n+4+27m^2)+[9n^2+12n+4+27m^2](3n+2)\\ =&4-27n^2-36n-12-81m^2+27n^3+36n^2+12n+81m^2n+18n^2+24n\\ &+8+54m^2\\ =&27n^2-27m^2+27n^3+81m^2n.\end{aligned}$$

Thus, $27 \mid (4-12e+4eu)$ and $27 \mid (1-3e+eu)$ and $\dfrac{1-3e+eu}{27} \in \mathbb{Z}$. So $Q(X) \in \mathbb{Z}[X]$.

Furthermore, the discriminant of $Q(X)$ is $\displaystyle\prod_{1 \leqslant i<j \leqslant 3}^{3} \left(\frac{\theta_i+1}{3}-\frac{\theta_j+1}{3}\right)^2 = \prod_{1 \leqslant i<j \leqslant 3}^{3} \left(\frac{\theta_i}{3}-\frac{\theta_j}{3}\right)^2 = \frac{1}{3^6}\prod_{1 \leqslant i<j \leqslant 3}^{3}(\theta_i-\theta_j)^2 = \frac{1}{3^6}\operatorname{disc}(P(X)) = \frac{e^2v^2}{3^2}$. Set $\theta' = \dfrac{\theta+1}{3}$, which is a root of $Q(X)$, and let $\mathcal{O}$ be the $\mathbb{Z}$-module generated by $(1, \theta', \sigma(\theta'))$. So $\sigma(\theta') = \sigma\left(\dfrac{\theta+1}{3}\right) = \dfrac{\frac{-2e}{v}-\frac{u+v}{2v}\theta+\frac{1}{v}\theta^2+1}{3} = \dfrac{v-2e}{3v}-\dfrac{u+v}{6v}\theta+\dfrac{1}{3v}\theta^2$. Since $\theta = 3\theta'-1$,

$$\begin{aligned}\sigma(\theta') =&\frac{v-2e}{3v}-\frac{u+v}{6v}(3\theta'-1)+\frac{1}{3v}(3\theta'-1)^2\\ =&\frac{v-2e}{3v}-\frac{u+v}{2v}\theta'+\frac{u+v}{6v}+\frac{1}{3v}(9\theta'^2-6\theta'+1)\\ =&\frac{v-2e}{3v}-\frac{u+v}{2v}\theta'+\frac{u+v}{6v}+\frac{1}{3v}(9\theta'^2-6\theta'+1)\\ =&\frac{2+u+3v-4e}{6v}-\frac{4+u+v}{2v}\theta'+\frac{3}{v}\theta'^2.\end{aligned}$$

Thus, $\theta'^2 = -\dfrac{2+u+3v-4e}{18}+\dfrac{4+u+v}{6}\theta'+\dfrac{v}{3}\sigma(\theta')$. Since $4e = u^2+3v^2$, $u^2 \equiv v^2 \pmod 2$ and thus $u \equiv v \pmod 2$. And since we let $u = 3n+2$ and $v = 3m$, we see that $n \equiv m \pmod 2$. So we have,

$$\begin{aligned}2+u+3v-4e &= 2+3n+2+3(3m)-(3n+2)^2-3(3m)^2\\ &= 4+3n+9m-9n^2-12n-4-27m^2\\ &= 9m-9n-9n^2-27m^2\\ &= 9(m-n)-9(n^2-m^2)-18m^2.\end{aligned}$$

Hence, $18 \mid (2+u+3v-4e)$. Also, $4+u+v = 4+3n+2+3m = 6+3(n+m)$, so $6 \mid (4+u+v)$.

Thus, $\mathcal{O} \supset \mathbb{Z}[\theta']$ and since $\mathbb{Z}[\theta'] = \left\langle 1, \theta', \frac{v}{3}\sigma(\theta')\right\rangle$, $[\mathcal{O} : \mathbb{Z}[\theta']] = \frac{v}{3}$. Therefore, the discriminant of $\mathcal{O}$ is equal to e^2. By Corollary 2.12, $\mathrm{disc}(K)$ must be divisible by e^2 and so $\mathrm{disc}(K) = e^2$ and $(1, \theta', \sigma(\theta'))$ is an integral basis of K. □

Now we will prove Theorem 2.7.

Proof. First, we note that the polynomials given in Theorem 2.7 are irreducible in $\mathbb{Q}[X]$. We use Eisenstein's Criterion for $\mathbb{Z}[X]$ for the first polynomial and the second one is obtained from the first one by changing X to $3X-1$ and dividing by 27. Thus, the irreducibility follows.

(1) From Theorem 2.15, one sees immediately that 3 is ramified in K if and only if $3 \nmid v$. Hence Proposition 2.4 tells us that K is given by an equation $P(X) = X^3 - 3eX - eu$. If we set $u' = 3u$, $v' = v$ and $e' = 9e$, we have $e' = \dfrac{u'^2 + 27v'^2}{4}$, $u' \equiv 6 \pmod 9$, $3 \nmid v'$, and $P(X) = X^3 - \dfrac{e'}{3}X - \dfrac{e'u'}{27}$.

(2) Assume now that 3 is not ramified, i.e. that $3 \mid v$. From the proof of the second part of Theorem 2.15, we know that K can be defined by the polynomial $X^3 - X^2 + \dfrac{1-e}{3}X - \dfrac{1-3e+eu}{27} \in \mathbb{Z}[X]$ and this time we set $e' = e$, $v' = \dfrac{v}{3}$ and $u' = u$, it is clear that the second statement of Theorem 2.7 follows.

Now we prove that any two fields defined by different polynomials $P(X)$ given in (1) or any two fields defined by different polynomials $P(X)$ given in (2) are not isomorphic, i.e. the pair (e, u) determines the isomorphism class. This follows immediately from the uniqueness statement of Proposition 2.4. (Note that the e and u in Proposition 2.4 are either equal to the e and u of the theorem (in case(2)), or to $e/9$ and $u/3$ (in case (1)).)

Let us prove (3). Assume that e is equal to a product of t distinct primes congruent to 1 modulo 3. Let $A = \mathbb{Z}[(1+\sqrt{-3})/2]$ be the ring of algebraic integers of $\mathbb{Q}(\sqrt{-3})$. If $\alpha \in A$ with $3 \nmid \mathcal{N}(\alpha)$, there exists a unique α' associate to α (i.e. generating the same principal ideal) such that $\alpha' = (u + 3v\sqrt{-3})/2$, $u \equiv 2 \pmod 3$.

To see this, we look at the following: Let $\alpha = \dfrac{a + b\sqrt{-3}}{2}$ where $a \equiv b \pmod 2$. Suppose $3 \nmid \mathcal{N}(\alpha) = \dfrac{a^2+3b^2}{4}$. Then, $3 \nmid \mathcal{N}(\alpha) \iff 3 \nmid (a^2+3b^2) \iff 3 \nmid a^2 \iff 3 \nmid a$.

Let $\zeta = \dfrac{1+\sqrt{-3}}{2}$, $\zeta^2 = \dfrac{-1+\sqrt{-3}}{2}$, $\zeta^3 = -1$, $\zeta^4 = \dfrac{-1-\sqrt{-3}}{2}$, $\zeta^5 = \dfrac{1-\sqrt{-3}}{2}$. Then,

$$\begin{aligned}
\alpha &= \frac{a + b\sqrt{-3}}{2} \\
\alpha\zeta^3 &= -\alpha = \frac{-a - b\sqrt{-3}}{2} \\
\alpha\zeta &= \frac{a - 3b + (a+b)\sqrt{-3}}{4} = \frac{\frac{a-3b}{2} + \frac{a+b}{2}\sqrt{-3}}{2} \\
\alpha\zeta^4 &= -\alpha\zeta = \frac{\frac{-a+3b}{2} + \frac{-a-b}{2}\sqrt{-3}}{2} \\
\alpha\zeta^2 &= \frac{-a - 3b + (a-b)\sqrt{-3}}{4} = \frac{\frac{-a-3b}{2} + \frac{a-b}{2}\sqrt{-3}}{2} \\
\alpha\zeta^5 &= -\alpha\zeta^2 = \frac{\frac{a+3b}{2} + \frac{-a+b}{2}\sqrt{-3}}{2}
\end{aligned}$$

Consider the following cases:

(i) If $3 \mid b$ and $a \equiv 2 \pmod 3$, then take $\alpha' = \alpha$.

(ii) If $3 \mid b$ and $a \equiv 1 \pmod 3$, then take $\alpha' = -\alpha$.

(iii) If $b \equiv 1 \pmod 3$ and $a \equiv 1 \pmod 3$, then let $b = 3t + 1$ and $a = 3k + 1$. We know that $t \equiv k \pmod 2$. Then $\dfrac{a+b}{2} = \dfrac{3t+3k+2}{2} = 3\left(\dfrac{t+k}{2}\right) + 1$, so $3 \nmid \left(\dfrac{a+b}{2}\right)$. $\dfrac{a-b}{2} = 3t - 3k$, so $3 \mid \left(\dfrac{a-b}{2}\right)$. We would take $\alpha' = \alpha\zeta^2$ or $\alpha\zeta^5$. Now look at $\dfrac{-a-3b}{2} = \dfrac{-3k-1-9t-3}{2} = -3\left(\dfrac{k+t}{2}\right) - 3t - 2 \equiv 1 \pmod 3$. Thus we take $\alpha' = \alpha\zeta^5$.

(iv) If $b \equiv 1 \pmod 3$ and $a \equiv 2 \pmod 3$, then let $b = 3t + 1$ and $a = 3k + 2$. We know that $t + 1 \equiv k \pmod 2$. Then $\dfrac{a+b}{2} = \dfrac{3t+3k+3}{2} = 3\left(\dfrac{t+k+1}{2}\right)$, so $3 \mid \left(\dfrac{a+b}{2}\right)$. $\dfrac{a-b}{2} = 3t - 3k + 1$, so $3 \nmid \left(\dfrac{a-b}{2}\right)$. We would take $\alpha' = \alpha\zeta$ or $\alpha\zeta^4$. Now look at $\dfrac{-a+3b}{2} = \dfrac{-3k-2+9t+3}{2} = \dfrac{9t+3k+1}{2} = \dfrac{3(3t-k+1)}{2} \equiv 2 \pmod 3$. Thus, we will take $\alpha' = \alpha\zeta^4$.

(v) If $b \equiv 2 \pmod 3$ and $a \equiv 1 \pmod 3$, we will take $\alpha' = \alpha\zeta$.

(vi) If $b \equiv 2 \pmod 3$ and $a \equiv 2 \pmod 3$, we will take $\alpha' = \alpha\zeta^2$.

Again, by Proposition 1.13, if p_i is a prime congruent to 1 modulo 3, then p_i splits in A and $p_i = \alpha_i\overline{\alpha_i}$ for a unique $\alpha_i = (u_i + 3v_i\sqrt{-3})/2$ with $u_i \equiv 2 \pmod 3$ and $v_i > 0$ because $3 \nmid \mathcal{N}(\alpha_i) = p_i$.

Hence, if $e = \prod_{1 \leqslant i \leqslant t} p_i$, then $e = \prod_{1 \leqslant i \leqslant t} p_i = \prod_{1 \leqslant i \leqslant t} \alpha_i\overline{\alpha_i} = \dfrac{u^2+27v^2}{4} = \mathcal{N}\left(\dfrac{u+3v\sqrt{-3}}{2}\right)$ $= \left(\dfrac{u+3v\sqrt{-3}}{2}\right)\left(\dfrac{u-3v\sqrt{-3}}{2}\right)$ if and only if $\dfrac{u+3v\sqrt{-3}}{2} = \prod_{1 \leqslant i \leqslant t} \beta_i$ where $\beta_i = \alpha_i$ or $\beta_i = \overline{\alpha_i}$ and this gives 2^t solutions to the equation $e = \dfrac{u^2+27v^2}{4}$. (We choose this specific associate in order to get $u \equiv 2 \pmod 3$ and $3v$.)

But, we have seen above that the isomorphism class of a cyclic cubic field is determined uniquely by the pair (e, u) satisfying appropriate conditions. Since $e = \dfrac{u^2+27(-v)^2}{4}$ gives the same field as $e = \dfrac{u^2+27v^2}{4}$, this shows, as claimed, that there exactly 2^{t-1} distinct value of u, hence 2^{t-1} non-isomorphic fields of discriminant e^2. This finishes the proof of one case.

Assume e is equal to 9 times the product of $t-1$ distinct primes congruent to 1 modulo 3. If $\alpha \in A$ with $3 \nmid \mathcal{N}(\alpha)$, there exist 2 unique α' associates to α (i.e. generating the same principal ideal) such that $\alpha' = (a+b\sqrt{-3})/2$, $a \equiv 2 \pmod 3$ and $3 \nmid b$. Hence, if $e = 9 \prod_{1\leqslant i\leqslant t-1} p_i$, then $e = 9 \prod_{1\leqslant i\leqslant t-1} p_i = 9 \prod_{1\leqslant i\leqslant t-1} \alpha_i'\overline{\alpha_i'} = \dfrac{u^2+27v^2}{4} = \mathcal{N}\left(\dfrac{u+3v\sqrt{-3}}{2}\right)$ $= \left(\dfrac{u+3v\sqrt{-3}}{2}\right)\left(\dfrac{u-3v\sqrt{-3}}{2}\right)$ if and only if $\dfrac{u+3v\sqrt{-3}}{2} = 3 \prod_{1\leqslant i\leqslant t-1} \beta_i$ where $\beta_i = \alpha_i'$ or $\beta_i = \overline{\alpha_i'}$. Now, we want to count how many unique solutions we can get from this equation. First, we note that any $p_i = \alpha_i\overline{\alpha_i}$, where we can set α_i to be the unique form in the previous part and $\alpha_i\zeta^2$ and $\alpha_i\zeta^4$ to be the 2 unique associates that we want. Then $\dfrac{u+3v\sqrt{-3}}{2}$ always has the form $3\alpha_1 \prod_{2\leqslant i\leqslant t-1} \beta_i\zeta^k$ where $\beta_i = \alpha_i$ or $\beta_i = \overline{\alpha_i}$ and $k = 0$, $k = 2$ or $k = 4$ (The case with $3\overline{\alpha_1} \prod_{2\leqslant i\leqslant t-1} \beta_i\zeta^k$ just give the same u and $-v$) . All possible solutions will be generated and we just need to count the wanted unique solutions. (The case where $k = 0$ does not give any solutions.) We see that the number of unique solutions is $2\sum_{i=0}^{t-2}\binom{t-2}{i} = 2(1+1)^{t-2} = 2^{t-1}$. We have seen above that the isomorphism class of a cyclic cubic field is determined uniquely by the pair (e,u) satisfying appropriate conditions. Hence there are 2^{t-1} non-isomorphic fields of discriminant e^2. This finishes the proof of the second case. □

Example 2.16. We can continue Example 2.5. We have the cyclic cubic field $K = \mathbb{Q}(\theta)$ where θ is a root of $x^3 - 273x - 728$ with $e = 7\cdot 13$, $u = 8$ and $v = 10$ under the notation of Proposition 2.4. By Theorem 2.15, $\operatorname{disc}(K) = (9e)^2$. Using notation of Theorem 2.7(1), we get new values of e and u, namely $e = 9\cdot 7\cdot 13$ and $u = 3\cdot 8$ (with $v = 10$). We nevertheless obtain the same defining polynomial $P(x) = x^3 - \dfrac{e}{3}x - \dfrac{eu}{27} = x^3 - 273x - 728$. In addition, we are now able to find all cyclic cubic fields ramified at 3, 7 and 13. According to Theorem

2.7(3), there exist up to isomorphism exactly 4 cyclic cubic fields of discriminant e^2. To find them, we see that $7 = \left(\frac{-1+3i\sqrt{3}}{2}\right)\left(\frac{-1-3i\sqrt{3}}{2}\right)$ and $13 = \left(\frac{5-3i\sqrt{3}}{2}\right)\left(\frac{5+3i\sqrt{3}}{2}\right)$. Then,

$$\begin{aligned}
\frac{u+3vi\sqrt{3}}{2} &= 3\left(\frac{-1+3i\sqrt{3}}{2}\right)\left(\frac{5-3i\sqrt{3}}{2}\right)\left(\frac{1+i\sqrt{3}}{2}\right)^2 = \frac{-57+3i\sqrt{3}}{2}, \\
\text{or } &= 3\left(\frac{-1+3i\sqrt{3}}{2}\right)\left(\frac{5-3i\sqrt{3}}{2}\right)\left(\frac{1+i\sqrt{3}}{2}\right)^4 = \frac{24-30i\sqrt{3}}{2}, \\
\text{or } &= 3\left(\frac{-1+3i\sqrt{3}}{2}\right)\left(\frac{5+3i\sqrt{3}}{2}\right)\left(\frac{1+i\sqrt{3}}{2}\right)^2 = \frac{-3-33i\sqrt{3}}{2}, \\
\text{or } &= 3\left(\frac{-1+3i\sqrt{3}}{2}\right)\left(\frac{5+3i\sqrt{3}}{2}\right)\left(\frac{1+i\sqrt{3}}{2}\right)^4 = \frac{51+15i\sqrt{3}}{2}.
\end{aligned}$$

Thus, the 4 cyclic cubic fields are determined uniquely by the pairs $(e,-57)$, $(e,24)$, $(e,-3)$ and $(e,51)$, with $e = 3\cdot 7\cdot 13$.

Example 2.17. We can continue Example 2.6. We have the cyclic cubic field $K = \mathbb{Q}(\theta)$ where θ is a root of $x^3 - 88257x + 10090717$ with $e = 13\cdot 31\cdot 73$, $u = -343$ and $v = 3$ under the notation of Proposition 2.4. By Theorem 2.15, $\operatorname{disc}(K) = e^2$. Using notation of Theorem 2.7(2), we have the same e and u, but with a new v, namely $v = 1$. Thus, we have the defining polynomial $P(x) = x^3 - x^2 + \frac{1-e}{3}x - \frac{1-3e+eu}{27} = x^3 - x^2 - 9806x + 376999$. Also, as in the previous example, we can find all cyclic cubic fields of discriminant e^2. According to Theorem 2.7(3), there exist up to isomorphism exactly 4 cyclic cubic fields of discriminant e^2. To find them, we see that $13 = \left(\frac{5-3i\sqrt{3}}{2}\right)\left(\frac{5+3i\sqrt{3}}{2}\right)$, $31 = \left(\frac{-4+6i\sqrt{3}}{2}\right)\left(\frac{-4-6i\sqrt{3}}{2}\right)$ and $73 = \left(\frac{-7+9i\sqrt{3}}{2}\right)\left(\frac{-7-9i\sqrt{3}}{2}\right)$. Then,

$$\begin{aligned}\frac{u+3vi\sqrt{3}}{2} &= \left(\frac{5-3i\sqrt{3}}{2}\right)\left(\frac{-4+6i\sqrt{3}}{2}\right)\left(\frac{-7+9i\sqrt{3}}{2}\right) = \frac{-343+3i\sqrt{3}}{2},\\ \text{or } &= \left(\frac{5-3i\sqrt{3}}{2}\right)\left(\frac{-4-6i\sqrt{3}}{2}\right)\left(\frac{-7+9i\sqrt{3}}{2}\right) = \frac{251-135i\sqrt{3}}{2},\\ \text{or } &= \left(\frac{5-3i\sqrt{3}}{2}\right)\left(\frac{-4+6i\sqrt{3}}{2}\right)\left(\frac{-7-9i\sqrt{3}}{2}\right) = \frac{224-150i\sqrt{3}}{2},\\ \text{or } &= \left(\frac{5-3i\sqrt{3}}{2}\right)\left(\frac{-4-6i\sqrt{3}}{2}\right)\left(\frac{-7-9i\sqrt{3}}{2}\right) = \frac{8+198i\sqrt{3}}{2}.\end{aligned}$$

Thus, the 4 cyclic cubic fields are determined uniquely by the pairs $(e, -343)$, $(e, 251)$, $(e, 224)$ and $(e, 8)$, with $e = 13 \cdot 31 \cdot 73$.

Example 2.18. In this example, we want to find all cyclic cubic fields that ramify at 7, 13, and 19. According to Theorem 2.7(3), there exist up to isomorphism exactly 4 cyclic cubic fields of discriminant e^2 where $e = 7 \cdot 13 \cdot 19$. We have $7 = \left(\frac{-1+3i\sqrt{3}}{2}\right)\left(\frac{-1-3i\sqrt{3}}{2}\right)$, $13 = \left(\frac{5-3i\sqrt{3}}{2}\right)\left(\frac{5+3i\sqrt{3}}{2}\right)$ and $19 = \left(\frac{-7-3i\sqrt{3}}{2}\right)\left(\frac{-7+3i\sqrt{3}}{2}\right)$. Then,

$$\begin{aligned}\frac{u+3vi\sqrt{3}}{2} &= \left(\frac{-1+3i\sqrt{3}}{2}\right)\left(\frac{5-3i\sqrt{3}}{2}\right)\left(\frac{-7-3i\sqrt{3}}{2}\right) = \frac{2-48i\sqrt{3}}{2},\\ \text{or } &= \left(\frac{-1+3i\sqrt{3}}{2}\right)\left(\frac{5-3i\sqrt{3}}{2}\right)\left(\frac{-7+3i\sqrt{3}}{2}\right) = \frac{-79-15i\sqrt{3}}{2},\\ \text{or } &= \left(\frac{-1+3i\sqrt{3}}{2}\right)\left(\frac{5+3i\sqrt{3}}{2}\right)\left(\frac{-7-3i\sqrt{3}}{2}\right) = \frac{83+3i\sqrt{3}}{2},\\ \text{or } &= \left(\frac{-1+3i\sqrt{3}}{2}\right)\left(\frac{5+3i\sqrt{3}}{2}\right)\left(\frac{-7+3i\sqrt{3}}{2}\right) \frac{29-45i\sqrt{3}}{2}.\end{aligned}$$

Thus, the 4 cyclic cubic fields are determined uniquely by the pairs $(e, 2)$, $(e, -79)$, $(e, 83)$ and $(e, 29)$, with $e = 7 \cdot 13 \cdot 19$.

Chapter 3. Discriminant Bounds

Discriminant bounds have been a popular topic in number theory. Minkowski gave the first proof that $|d_K| > 1$ for any number field K using the geometry of numbers, based on the lower bound $|d_K| \geqslant \left(\frac{\pi}{4}\right)^{2r_2} \left(\frac{n^n}{n!}\right)^2$ (see [6]). Discriminant bounds have been improved over the years. Odlyzko [10] utilized the zeros of the Dedekind zeta function to get better lower bounds. Also, if Generalized Riemann Hypothesis (GRH) is assumed, much better bounds can be obtained. Serre suggested using explicit formulae to achieve greater flexibility in the choice of parameters. The unconditional bound that we use from C.J. Moreno [8] is also derived by using Weil's explicit formulas and the bound is given by:

$$rd_K \geqslant (60.8)^{\frac{r_1}{n}} (22.3)^{\frac{2r_2}{n}} e^{-\frac{8.6}{n^{2/3}}}. \tag{3.1}$$

If K is a totally real field, the inequality becomes:

$$rd_K \geqslant (60.8) e^{-\frac{8.6}{n^{2/3}}} \tag{3.2}$$

Now we look at the following proposition from Yamamura [11] and see how we use the lower bound to determine that a field has no non-solvable unramified extension.

Proposition 3.1. *Let $B(n_K, r_1, r_2)$ be the lower bound for the root discriminant of K of degree n_K with signature (r_1, r_2). Suppose that K has an unramified normal extension L of degree m. If $h(L) = 1$ and $rd_K < B(60mn_K, 60mr_1, 60mr_2)$, then $K_{ur} = L$.*

Proof. Suppose that L/K is normal, that $h(L) = 1$ and that $rd_K < B(60mn_k, 60mr_1, 60mr_2)$. Given any normal unramified extension F of K, we see that LF is a normal unramified extension of L. Set $h = [LF : L]$ and set $G = \mathrm{Gal}(LF/L)$. Clearly, G must be non-solvable, since otherwise it would have an Abelian quotient (i.e. G/G_1 is Abelian where G_1 is a normal subgroup of G) which would yield an Abelian unramified extension of L. Such an extension can not exist, because L has class number 1.

$$\begin{tikzcd}
& LF \arrow[dl, dash, "h\geqslant 60"'] \arrow[dr, dash] & \\
L \arrow[dr, dash, "m"'] & & F \arrow[dl, dash] \\
& K \arrow[d, dash, "n_K"'] & \\
& \mathbb{Q} &
\end{tikzcd}$$

Since G is non-solvable, we have $h \geqslant 60$ where 60 is the order of A_5, the smallest non-solvable group. In addition, since LF/K is unramified, we have $rd_{LF} = rd_K < B(60mn_k, 60mr_1, 60mr_2) \leqslant B(hmn_k, hmr_1, hmr_2)$. This is a contradiction, since the degree of LF is hmn_k, and it has hmr_1 real places and hmr_2 pairs of complex places (no real places turns to complex places as LF is unramified over L). Thus, all unramified extensions of K are contained in L and $K_{ur} = L$. □

Let K be a cyclic cubic field and L is the top of the class field tower of K. We will make a table of unconditional lower bounds for totally real fields F with degree n over $\mathbb{Q}$ using inequality (3.2).

$[L : K]$	n	lower bounds for rd_F
1	180	46.42
3	540	53.40
4	720	54.62
7	1260	56.47
8	1440	56.83

Table 3.1

The conditional (under GRH) lower bounds for totally real fields F are found in the unpublished tables due to A.M. Odlyzko, which are copied in Martinet's expository paper [7]. We only list part of the tables here.

n	lower bounds for rd_F
180	72.553
360	87.642
480	93.555
720	101.488
1000	107.548
1200	110.728

Table 3.2

Chapter 4. Maximal Unramified Extensions of Cyclic Cubic Fields

With the information above, we proceed to look at cyclic cubic fields and their maximal unramified extensions.

4.1 Maximal Unramified Solvable Extensions

Since we know the canonical representing polynomial of cyclic cubic fields, we can generate a full list of cyclic cubic fields of root discriminant less than a certain number. We first look at the cyclic cubic fields of root discriminant less than 72.553 (the lower bound for totally real fields of degree 180 under GRH in Table 3.2), ramified at only one prime and having $h(K) = 1$. The first column gives the canonical representing polynomials.

$P(x)$	disc(K)	rd_K	$h(K)$
$x^3 - x^2 - 2x + 1$	7^2	3.66	1
$x^3 - 3x - 1$	3^4	4.33	1
$x^3 - x^2 - 4x - 1$	13^2	5.53	1
$x^3 - x^2 - 6x + 7$	19^2	7.12	1
$x^3 - x^2 - 10x + 8$	31^2	9.87	1
$x^3 - x^2 - 12x - 11$	37^2	11.1	1
$x^3 - x^2 - 14x - 8$	43^2	12.27	1
$x^3 - x^2 - 20x + 9$	61^2	15.5	1
$x^3 - x^2 - 22x - 5$	67^2	16.5	1
$x^3 - x^2 - 24x + 27$	73^2	17.47	1
$x^3 - x^2 - 26x - 41$	79^2	18.41	1
$x^3 - x^2 - 32x + 79$	97^2	21.11	1
$x^3 - x^2 - 34x + 61$	103^2	21.97	1
$x^3 - x^2 - 36x + 4$	109^2	22.82	1
$x^3 - x^2 - 42x - 80$	127^2	25.27	1
$x^3 - x^2 - 46x - 103$	139^2	26.83	1
$x^3 - x^2 - 50x + 123$	151^2	28.36	1
$x^3 - x^2 - 52x - 64$	157^2	29.1	1
$x^3 - x^2 - 60x + 67$	181^2	32	1
$x^3 - x^2 - 64x - 143$	193^2	33.4	1
$x^3 - x^2 - 66x - 59$	199^2	34.09	1
$x^3 - x^2 - 70x + 125$	211^2	35.44	1
$x^3 - x^2 - 74x + 256$	223^2	36.77	1
$x^3 - x^2 - 76x + 212$	229^2	37.43	1
$x^3 - x^2 - 80x - 125$	241^2	38.73	1
$x^3 - x^2 - 90x - 261$	271^2	41.88	1
$x^3 - x^2 - 94x - 304$	283^2	43.1	1
$x^3 - x^2 - 102x + 216$	307^2	45.51	1

(Continued)

$P(x)$	disc(K)	rd_K	$h(K)$
$x^3 - x^2 - 110x + 49$	331^2	47.85	1
$x^3 - x^2 - 112x - 25$	337^2	48.43	1
$x^3 - x^2 - 122x - 435$	367^2	51.26	1
$x^3 - x^2 - 124x + 221$	373^2	51.82	1
$x^3 - x^2 - 126x - 365$	379^2	52.37	1
$x^3 - x^2 - 136x + 515$	409^2	55.1	1
$x^3 - x^2 - 140x + 343$	421^2	56.17	1
$x^3 - x^2 - 144x + 16$	433^2	57.23	1
$x^3 - x^2 - 146x + 504$	439^2	57.76	1
$x^3 - x^2 - 152x + 220$	457^2	59.33	1
$x^3 - x^2 - 154x - 343$	463^2	59.85	1
$x^3 - x^2 - 162x + 505$	487^2	61.9	1
$x^3 - x^2 - 166x - 536$	499^2	62.91	1
$x^3 - x^2 - 174x + 891$	523^2	64.91	1
$x^3 - x^2 - 180x - 521$	541^2	66.39	1
$x^3 - x^2 - 190x + 719$	571^2	68.83	1
$x^3 - x^2 - 192x - 171$	577^2	69.31	1
$x^3 - x^2 - 200x - 512$	601^2	71.22	1
$x^3 - x^2 - 204x - 999$	613^2	72.16	1

Table 4.1

The following table shows cyclic cubic fields of root discriminant less than 72.553, ramified at only one prime but having $h(K) \neq 1$. We will explain the first three lines in this table in Example 4.2, 4.3, 4.4. The others are proven similarly.

$P(x)$	disc(K)	rd_K	$h(K)$	$h(K_1)$	$h(K_2)$
$x^3 - x^2 - 54x + 169$	163^2	29.84	4	1	1
$x^3 - x^2 - 92x - 236$	277^2	42.49	4	2	1
$x^3 - x^2 - 104x - 371$	313^2	46.1	7	1	1
$x^3 - x^2 - 116x + 517$	349^2	49.57	4	1	1
$x^3 - x^2 - 132x + 544$	397^2	54.02	4	1	1
$x^3 - x^2 - 182x + 81$	547^2	66.88	4	1	1
$x^3 - x^2 - 202x + 1169$	607^2	71.69	4	2	1

Table 4.2

The following table shows cyclic cubic fields of root discriminant less than 72.553, ramified at two primes. The first pair of cyclic cubic fields in the first two lines of this table will be explained in Example 4.5. The others are proven similarly.

$P(x)$	$\mathrm{disc}(K)$	rd_K	$h(K)$	$h(K_1)$
$x^3-21x-35$	$3^4\cdot 7^2$	15.83	3	1
$x^3-21x-28$	$3^4\cdot 7^2$	15.83	3	1
$x^3-x^2-30x-27$	$7^2\cdot 13^2$	20.23	3	1
$x^3-x^2-30x+64$	$7^2\cdot 13^2$	20.23	3	1
$x^3-39x-26$	$3^4\cdot 13^2$	23.92	3	1
$x^3-39x-91$	$3^4\cdot 13^2$	23.92	3	1
$x^3-x^2-44x+64$	$7^2\cdot 19^2$	26.06	3	1
$x^3-x^2-44x-69$	$7^2\cdot 19^2$	26.06	3	1
$x^3-57x-152$	$3^4\cdot 19^2$	30.81	3	1
$x^3-57x-19$	$3^4\cdot 19^2$	30.81	3	1
$x^3-x^2-72x-209$	$7^2\cdot 31^2$	36.11	3	1
$x^3-x^2-72x+225$	$7^2\cdot 31^2$	36.11	3	1
$x^3-x^2-82x+64$	$13^2\cdot 19^2$	39.37	3	1
$x^3-x^2-82x+311$	$13^2\cdot 19^2$	39.37	3	1
$x^3-x^2-86x-48$	$7^2\cdot 37^2$	40.63	3	1
$x^3-x^2-86x+211$	$7^2\cdot 37^2$	40.63	3	1
$x^3-93x-341$	$3^4\cdot 31^2$	42.7	3	1
$x^3-93x-217$	$3^4\cdot 31^2$	42.7	3	1
$x^3-x^2-100x+379$	$7^2\cdot 43^2$	44.91	3	1
$x^3-x^2-100x-223$	$7^2\cdot 43^2$	44.91	3	1
$x^3-111x-370$	$3^4\cdot 37^2$	48.04	3	1
$x^3-111x-37$	$3^4\cdot 37^2$	48.04	3	1

(Continued)

$P(x)$	$\mathrm{disc}(K)$	rd_K	$h(K)$	$h(K_1)$
$x^3 - 129x - 215$	$3^4 \cdot 43^2$	53.11	3	1
$x^3 - 129x - 559$	$3^4 \cdot 43^2$	53.11	3	1
$x^3 - x^2 - 134x - 209$	$13^2 \cdot 31^2$	54.56	3	1
$x^3 - x^2 - 134x + 597$	$13^2 \cdot 31^2$	54.56	3	1
$x^3 - x^2 - 142x - 601$	$7^2 \cdot 61^2$	56.7	3	1
$x^3 - x^2 - 142x + 680$	$7^2 \cdot 61^2$	56.7	3	1
$x^3 - x^2 - 156x + 799$	$7^2 \cdot 67^2$	60.36	3	1
$x^3 - x^2 - 156x - 608$	$7^2 \cdot 67^2$	60.36	3	1
$x^3 - x^2 - 160x - 677$	$13^2 \cdot 37^2$	61.39	3	1
$x^3 - x^2 - 160x - 196$	$13^2 \cdot 37^2$	61.39	3	1
$x^3 - x^2 - 170x - 776$	$7^2 \cdot 73^2$	63.92	3	1
$x^3 - x^2 - 170x + 757$	$7^2 \cdot 73^2$	63.92	3	1
$x^3 - 183x - 854$	$3^4 \cdot 61^2$	67.05	3	1
$x^3 - 183x - 793$	$3^4 \cdot 61^2$	67.05	3	1
$x^3 - x^2 - 184x - 41$	$7^2 \cdot 79^2$	67.37	3	1
$x^3 - x^2 - 184x + 512$	$7^2 \cdot 79^2$	67.37	3	1
$x^3 - x^2 - 186x - 911$	$13^2 \cdot 43^2$	67.86	3	1
$x^3 - x^2 - 186 + 207$	$13^2 \cdot 43^2$	67.86	3	1
$x^3 - x^2 - 196x - 829$	$19^2 \cdot 31^2$	70.27	3	1
$x^3 - x^2 - 196x + 349$	$19^2 \cdot 31^2$	70.27	3	1
$x^3 - 201x - 737$	$3^4 \cdot 67^2$	71.37	3	1
$x^3 - 201x - 1072$	$3^4 \cdot 67^2$	71.37	3	1

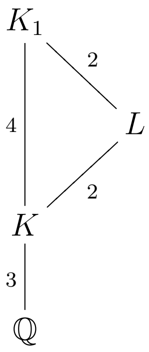
Table 4.3

According to Table 4.1, the first 28 cyclic cubic fields with class number 1 have root discriminant less than 46.42 which is the unconditional lower bound for totally real fields of degree 180 (from Table 3.1), and the first 47 cyclic cubic fields with class number 1 have root discriminant less than 72.553 which is the conditional lower bound for totally real fields of degree 180 (from Table 3.2). Therefore, they do not have non-solvable unramified extension. Applying Proposition 3.1, we can conclude as follows:

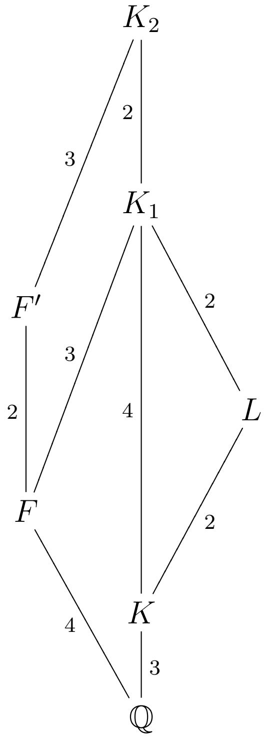
Theorem 4.1. *The first* 28 *(*47 *under* GRH*) cyclic cubic fields with class number* 1 *have trivial maximal unramified extension.*

Now we examine each of the cyclic cubic fields with $h(K) \neq 1$ in the tables above and demonstrate how we determine the maximal unramified extensions.

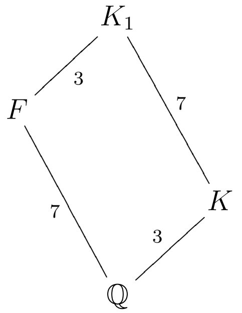
Example 4.2. Let K be the cyclic cubic field defined by $x^3 - x^2 - 54x + 169$ with $d_K = 163^2$ and $rd_K = 29.84$. It is the first cyclic cubic field with $h(K) = 4$ (from Table 4.2). The class field K_1 of K is the splitting field L' (A_4-extension over $\mathbb{Q}$) of the sextic field L represented by $x^6 - 3x^5 - 11x^4 + 27x^3 - 3x^2 - 11x + 1$ with field discriminant 163^4, found from John Jones' website *Number Fields.* To confirm L' is K_1, we see that L' has degree 12 and the prime 163 is unramified in L'/K. Also, we know that $\mathrm{Gal}(L'/K)$ is Abelian ($\mathbb{Z}_2 \times \mathbb{Z}_2$, normal subgroup of A_4). We then use PARI to compute the class number of K_1. Since $h(K_1) = 1$ and $rd_K = 29.84 < 54.62$ which is the lower bound for totally real fields of degree 720, we have $K_{ur} = K_1$ by Proposition 3.1. In this case, we have $\mathrm{Gal}(K_{ur}/K) = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathrm{Gal}(K_{ur}/\mathbb{Q}) = A_4$.



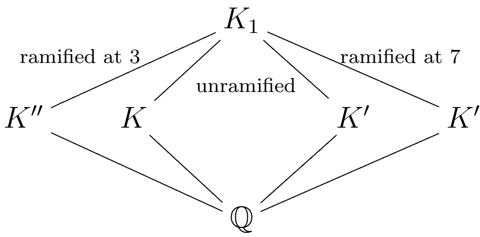
Example 4.3. Let K be the cyclic cubic field defined by $x^3 - x^2 - 92x - 236$ with $d_K = 277^2$ and $rd_K = 42.49$. It is the second cyclic cubic field with $h(K) = 4$ (from Table 4.2). The class field K_1 of K is the splitting field of the sextic field L represented by $x^6 - 3x^5 - 19x^4 + 43x^3 + 47x^2 - 69x + 16$ with field discriminant 277^4. This sextic field is obtained from John Jones' website *Number Fields*. We use PARI to find that $h(K_1) = 2$. And K_2 turns out to be the splitting field of the octic field F' represented by $x^8 - x^7 - 11x^6 + 13x^5 + 32x^4 - 41x^3 - 23x^2 + 32x - 1$ with field discriminant 277^4. We use PARI again to find that $h(K_2) = 1$. Since $rd_K = 42.49 < 56.83$ which is the lower bound for totally real fields of degree 1440, we have $K_{ur} = K_2$ by Proposition 3.1. In this case, we have $\mathrm{Gal}(K_{ur}/K) = Q_8$ and $\mathrm{Gal}(K_{ur}/\mathbb{Q}) = SL(2,3)$.



Example 4.4. Let K be the cyclic cubic field defined by $x^3 - x^2 - 104x - 371$ with $d_K = 313^2$ and $rd_K = 46.10$. It is the first cyclic cubic field with $h(K) = 7$ (from Table 4.2). The class field K_1 of K is the splitting field of the heptic field F represented by $x^7 - x^6 - 15x^5 + 20x^4 + 33x^3 - 22x^2 - 32x - 8$ with field discriminant 313^4. This heptic field is obtained from John Jones' website *Number Fields*. Since $h(K_1) = 1$ and $rd_K = 46.10 < 56.47$ which is the lower bound for totally real fields of degree 1260, we have $K_{ur} = K_1$ by Proposition 3.1. In this case, we have $\mathrm{Gal}(K_{ur}/K) = \mathbb{Z}_7$ and $\mathrm{Gal}(K_{ur}/\mathbb{Q}) = F_{21}$.



Example 4.5. Let K be the cyclic cubic field defined by $x^3 - 21x - 35$ and K' be the cyclic cubic field defined by $x^3 - 21x - 28$. They are the first two cyclic cubic fields with class number not equal to 1 ($h(K) = h(K') = 3$) and with $d_K = d_{K'} = 3^4 \cdot 7^2$ and $rd_K = rd_{K'} = 15.83$ (from Table 4.3). We take the composite field L of K(or K') and the cubic subfield of the cyclotomic field $\mathbb{Q}(\zeta_9)$ ramified only at 3. To confirm the composite field L is the class field of K (or K'), we again check the degree of L, the ramification indices of 3 and 7 in L and the Galois group of L/K. We then use PARI to compute the class number of K_1. Since $h(K_1) = 1$ and $rd_K = 15.83 < 53.40$ which is the lower bound for totally real fields of degree 540, we have $K_{ur} = K_1$ by Proposition 3.1. In this case, we have $\mathrm{Gal}(K_{ur}/K) = \mathrm{Gal}(K_{ur}/K') = \mathbb{Z}_3$ and $\mathrm{Gal}(K_{ur}/\mathbb{Q}) = \mathbb{Z}_3 \times \mathbb{Z}_3$.



There are some cyclic cubic fields that have different and bigger class numbers and if we assume GRH, we can still show that they have no non-solvable unramified extension and find their maximal unramified extensions. We give several examples.

Example 4.6. Examine the following two cyclic cubic fields.

$P(x)$	$\text{disc}(K)$	rd_K	$h(K)$	$h(K_1)$
$x^3 - 219x - 1241$	$3^4 \cdot 73^2$	75.57	9	1
$x^3 - 219x - 730$	$3^4 \cdot 73^2$	75.57	9	1

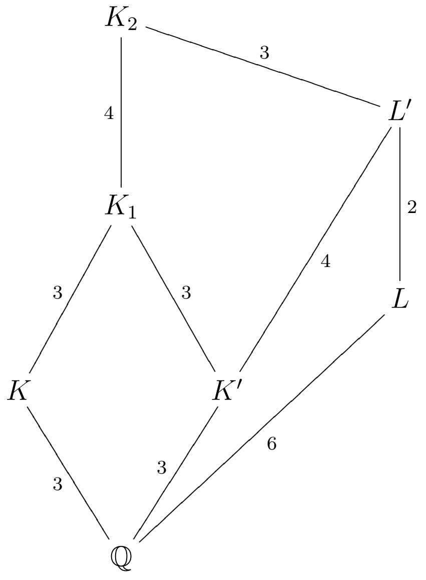
Let K be the first cyclic cubic field in the above table and K' be the second one. On John Jones' website *Number Fields*, we find that there are two nonic fields ramified at 3 and 73. Let L be the nonic field represented by $x^9 - 3x^8 - 54x^7 + 95x^6 + 843x^5 - 417x^4 - 3347x^3 + 1278x^2 + 3204x - 1457$ and L' be the nonic field represented by $x^9 - 3x^8 - 54x^7 + 137x^6 + 759x^5 - 1971x^4 - 2178x^3 + 5625x^2 + 1608x - 3284$. Using PARI, we confirm that $K \subset L$ and $K' \subset L'$. Also, we check that L and L' are unramified extensions of K and K' respectively by checking the ramification indices of 3 and 73 in L and L'. Using PARI, we find that the splitting field S of L and L' is the same field. Since S has degree 9 over K (K'), the primes 3 and 73 are unramified in S/K (S/K') and S is Abelian over K (K'), we know that $K_1 = K_1' = S$. If K_1 has a non-solvable unramified extension, the degree would be at least 1620. Since $h(K_1) = 1$ and $rd_K = 75.57 < 110.728$ which is the lower bound for totally real fields of degree 1200 under GRH (the lower bound for totally real fields of degree 1620 under GRH would be bigger than 110.728) from Table 3.2, we have $K_{ur} = K_1$ by Proposition 3.1. In this case, we have $\text{Gal}(K_{ur}/K) = \text{Gal}(K_{ur}/K') = \mathbb{Z}_3 \times \mathbb{Z}_3$ and $\text{Gal}(K_{ur}/\mathbb{Q}) = (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_3$.

$$\begin{tikzcd}
 & K_1 \arrow[dl, dash, "3"'] \arrow[dr, dash, "3"] & \\
L \arrow[d, dash, "3"'] & & L' \arrow[d, dash, "3"] \\
K \arrow[dr, dash, "3"'] & & K' \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Example 4.7. Examine the following two cyclic cubic fields.

$P(x)$	$\mathrm{disc}(K)$	rd_K	$h(K)$	$h(K_1)$	$h(K_2)$
$x^3 - x^2 - 226x - 503$	$7^2 \cdot 97^2$	77.25	3	4	1
$x^3 - x^2 - 226x + 176$	$7^2 \cdot 97^2$	77.25	12	1	1

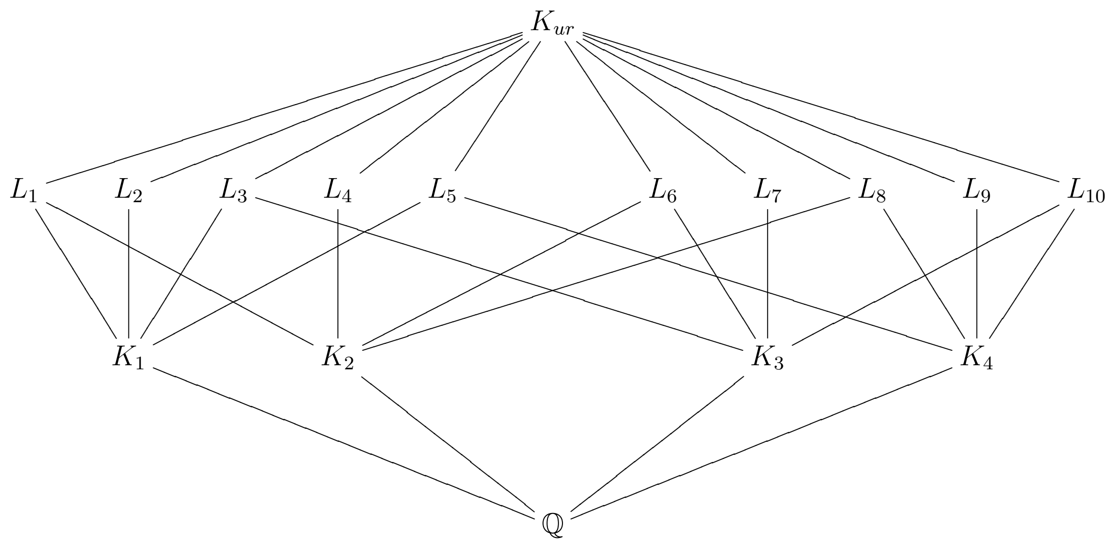
Let K be the first cyclic cubic field in the above table and K' be the second one. We take the composite field of K and K' and get a field of degree 9 over $\mathbb{Q}$. After checking the ramification indices of 7 an 97 in the composite field, we confirm that is the class field of K. Then, on John Jones' website *Number Fields*, we find a sextic field L ramified at 7 and 97. It is represented by $x^6 - 3x^5 - 45x^4 + 95x^3 + 41x^2 - 89x - 22$. Its splitting field L' is an A_4-extension of $\mathbb{Q}$. We use PARI to find that L' is an unramified $\mathbb{Z}_2 \times \mathbb{Z}_2$-extension of K'. Now, we take the composite field of K_1 and L', we get a field of degree 36 over $\mathbb{Q}$. Using PARI, we check that 7 and 97 are unramified in K_1L'/K_1. Thus, the composite field is K_2. Since K_2 is unramified over K' and $\mathrm{Gal}(K_2/K') = \mathbb{Z}_6 \times \mathbb{Z}_2$, K_2 is the class field of K'. Since $h(K_2) = 1$ and $rd_K = 77.25 < 110.728$ which is the lower bound for totally real fields of degree 1200 under GRH (the lower bound for totally real fields of degree 2160 under GRH would be bigger than 110.728) from Table 3.2, we have $K_{ur} = K_2$ by Proposition 3.1. In this case, we have $\mathrm{Gal}(K_{ur}/K) = A_4$, $\mathrm{Gal}(K_{ur}/K') = \mathbb{Z}_6 \times \mathbb{Z}_2$ and $\mathrm{Gal}(K_{ur}/\mathbb{Q}) = A_4 \times \mathbb{Z}_3$.



Example 4.8. Examine the following four cyclic cubic fields. They are the first four cyclic cubic fields ramified at 3 primes.

$P(x)$	$\text{disc}(K)$	rd_K	$h(K)$	$h(K_1)$
$x^3 - 273x - 728$	$3^4 \cdot 7^2 \cdot 13^2$	87.54	9	1
$x^3 - 273x - 91$	$3^4 \cdot 7^2 \cdot 13^2$	87.54	9	1
$x^3 - 273x - 1729$	$3^4 \cdot 7^2 \cdot 13^2$	87.54	9	1
$x^3 - 273x - 1547$	$3^4 \cdot 7^2 \cdot 13^2$	87.54	9	1

Let K_1, K_2, K_3, K_4 be the first, second, third and fourth cyclic cubic field in the above table. Then, on John Jones' website *Number Fields*, we find 10 nonic fields ramified at 3, 7 and 13. We label them L_1 to L_{10}. Using PARI, we check that each of the cyclic cubic fields is contained in four different nonic fields. If we take the composite field of L_i and K_j where $L_i \not\supset K_j$, we can get the same field of degree 27 over $\mathbb{Q}$. After checking the ramification indices of 3, 7, and 13 using PARI, we confirm that the composite field is the class field H of K_i. Since $h(H) = 1$ and $rd_K = 87.54 < 110.728$ which is the lower bound for totally real fields of degree 1200 under GRH (the lower bound for totally real fields of degree 1620 under GRH would be bigger than 110.728) from Table 3.2, we have $K_{ur} = H$ by Proposition 3.1. In this case, we have $\text{Gal}(K_{ur}/K_i) = \mathbb{Z}_3 \times \mathbb{Z}_3$ and $\text{Gal}(K_{ur}/\mathbb{Q}) = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.



Now, we can organize our results in the following tables. The first table shows the complete list of cyclic cubic fields with $rd_K \leqslant 54.02$ having non-trivial maximal unramified extensions. The second table shows the complete list of cyclic cubic fields with rd_K between 54.02 and 71.96 having non-trivial maximal unramified extensions under GRH. The final table gives additional examples, assuming GRH, in which the cyclic cubic fields have $rd_K > 72$ and non-trivial maximal unramified extensions. In these three tables, $h(K_2) = 1$ for all K_2.

Cubic Polynomial f	$D(K)$	rd_K	$h(K)$	$h(K_1)$	Gal(K_{ur}/K)	Gal$(K_{ur}/\mathbb{Q})$
$x^3 - 21x - 35$	$3^4 \cdot 7^2$	15.83	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - 21x - 28$	$3^4 \cdot 7^2$	15.83	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 30x - 27$	$7^2 \cdot 13^2$	20.23	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 30x + 64$	$7^2 \cdot 13^2$	20.23	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - 39x - 26$	$3^4 \cdot 13^2$	23.92	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - 39x - 91$	$3^4 \cdot 13^2$	23.92	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 44x + 64$	$7^2 \cdot 19^2$	26.06	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 44x - 69$	$7^2 \cdot 19^2$	26.06	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 54x + 169$	169^2	29.84	4	1	$\mathbb{Z}_2 \times \mathbb{Z}_2$	A_4
$x^3 - 57x - 152$	$3^4 \cdot 19^2$	30.81	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - 57x - 19$	$3^4 \cdot 19^2$	30.81	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 72x - 209$	$7^2 \cdot 31^2$	36.11	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 72x + 229$	$7^2 \cdot 31^2$	36.11	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 82x + 64$	$13^2 \cdot 19^2$	39.37	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 82x + 311$	$13^2 \cdot 19^2$	39.37	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 86x - 48$	$7^2 \cdot 37^2$	40.63	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 86x + 211$	$7^2 \cdot 37^2$	40.63	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 92x - 236$	277^2	42.49	4	2	Q_8	$SL(2,3)$
$x^3 - 93x - 341$	$3^4 \cdot 31^2$	42.70	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - 93x - 271$	$3^4 \cdot 31^2$	42.70	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 100x + 379$	$7^2 \cdot 43^2$	44.91	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 100x - 223$	$7^2 \cdot 43^2$	44.91	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 104x - 371$	313^2	46.10	7	1	$\mathbb{Z}_7$	F_{21}
$x^3 - 111x - 370$	$3^4 \cdot 37^2$	48.04	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - 111x - 37$	$3^4 \cdot 37^2$	48.04	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 116x + 517$	349^2	49.57	4	1	$\mathbb{Z}_2 \times \mathbb{Z}_2$	A_4
$x^3 - 129x - 215$	$3^4 \cdot 43^2$	53.11	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - 129x - 559$	$3^4 \cdot 43^2$	53.11	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - x^2 - 132x + 544$	397^2	54.02	4	1	$\mathbb{Z}_2 \times \mathbb{Z}_2$	A_4

Under GRH

Cubic Polynomial f	$D(K)$	rd_K	$h(K)$	$h(K_1)$	$\mathrm{Gal}(K_{ur}/K)$	$\mathrm{Gal}(K_{ur}/\mathbb{Q})$
$x^3-x^2-134x-209$	$13^2\cdot 31^2$	54.56	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-134x+597$	$13^2\cdot 31^2$	54.56	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-142x-601$	$7^2\cdot 61^2$	56.70	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-142x+680$	$7^2\cdot 61^2$	56.70	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-156x+799$	$7^2\cdot 67^2$	60.36	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-156x-608$	$7^2\cdot 67^2$	60.36	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-160x-677$	$13^2\cdot 37^2$	61.39	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-160x-196$	$13^2\cdot 37^2$	61.39	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-170x-776$	$7^2\cdot 73^2$	63.92	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-170x+757$	$7^2\cdot 73^2$	63.92	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-182x+81$	547^2	66.88	4	1	$\mathbb{Z}_2\times\mathbb{Z}_2$	A_4
$x^3-183x-854$	$3^4\cdot 61^2$	67.05	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-183x-793$	$3^4\cdot 61^2$	67.05	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-184x-41$	$7^2\cdot 79^2$	67.37	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-184x+512$	$7^2\cdot 79^2$	67.37	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-186x-911$	$13^2\cdot 43^2$	67.86	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-186x+207$	$13^2\cdot 43^2$	67.86	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-196x-829$	$19^2\cdot 31^2$	70.27	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-196x+349$	$19^2\cdot 31^2$	70.27	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-201x-737$	$3^4\cdot 67^2$	71.37	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-201x-737$	$3^4\cdot 67^2$	71.37	3	1	$\mathbb{Z}_3$	$\mathbb{Z}_3\times\mathbb{Z}_3$
$x^3-x^2-202x+1169$	607^2	71.96	4	2	Q_8	$SL(2,3)$

Other examples under GRH (with $rd_K > 72$)

Cubic Polynomial f	$D(K)$	rd_K	$h(K)$	$h(K_1)$	$\mathrm{Gal}(K_{ur}/K)$	$\mathrm{Gal}(K_{ur}/\mathbb{Q})$
$x^3 - 219x - 1241$	$3^4 \cdot 73^2$	75.57	9	1	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_3$
$x^3 - 219x - 730$	$3^4 \cdot 73^2$	75.57	9	1	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_3$
$x^3 - x^2 - 226x - 503$	$7^2 \cdot 97^2$	77.25	3	4	A_4	$A_4 \times \mathbb{Z}_3$
$x^3 - x^2 - 226x + 176$	$7^2 \cdot 97^2$	77.25	12	1	$Z_6 \times \mathbb{Z}_2$	$A_4 \times \mathbb{Z}_3$
$x^3 - 273x - 728$	$3^4 \cdot 7^2 \cdot 13^2$	87.54	9	1	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - 273x - 91$	$3^4 \cdot 7^2 \cdot 13^2$	87.54	9	1	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - 273x - 1729$	$3^4 \cdot 7^2 \cdot 13^2$	87.54	9	1	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
$x^3 - 273x - 1547$	$3^4 \cdot 7^2 \cdot 13^2$	87.54	9	1	$\mathbb{Z}_3 \times \mathbb{Z}_3$	$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

4.2 Unramified Non-Solvable Extensions

Theorem 4.9. *The cyclic cubic field K defined by $x^3-x^2-3422x+1521$, ramified at* 10267, *has an unramified A_5-extension. Moreover, such an extension of K is given by the composite field of K with the splitting field of the quintic polynomial $x^5-25x^3-7x^2+116x-45$, which is an A_5-extension of $\mathbb{Q}$.*

Before we prove this, we first explain how we find this cyclic cubic field. We want a cyclic cubic field to have an unramified non-solvable extension, so we try to get an A_5-extension of a cyclic cubic field ramified at only one prime. We search on John Jones' website *Number Fields* for totally real quintic fields ramified at only one prime, and with splitting field an A_5-extension of $\mathbb{Q}$. Here we let L denote a totally real quintic field and let S denote the splitting field of L. If we take the composite field of a cyclic cubic field K with S, we get an A_5-extension of K because any A_5-extension does not contain a cyclic cubic extension and $K \cap S = \mathbb{Q}$.

Here we list the first two (in terms of field discriminants) totally real quintic fields ramified at only one prime (3 or prime congruent to 1 modulo 3), and with splitting field an A_5-extension of $\mathbb{Q}$ because only 3 or primes congruent to 1 modulo 3 can be ramified in a cyclic cubic field.

d_L	Polynomial
8311^2	$x^5-x^4-16x^3+7x^2+57x+35$
10267^2	$x^5-25x^3-7x^2+116x-45$

Now we will construct the two cyclic cubic fields ramified at 8311 and 10267 respectively. We factor them in the ring of algebraic integers of $\mathbb{Q}(\sqrt{-3})$ into the unique associates as in the proof of Theorem 2.7. $8311 = \left(\dfrac{-13+105i\sqrt{3}}{2}\right)\left(\dfrac{-13-105i\sqrt{3}}{2}\right)$ and $10267 = \left(\dfrac{-1-117i\sqrt{3}}{2}\right)\left(\dfrac{-1+117i\sqrt{3}}{2}\right)$. Thus, $e = 8311$ and $u = -13$ for the first cyclic cubic field and $e = 10267$ and $u = -1$ for the second one. The representing polynomials are $x^3 - x^2 - 2770x + 4925$ and $x^3 - x^2 - 3422x + 1521$.

Now, we can look at the ramification indices of primes lying over 8311 and 10267 in the A_5-extensions over K. Let K be the cyclic cubic field defined by $x^3 - x^2 - 2770x + 4925$ with $d_K = 8311^2$. There is only one prime in $\mathcal{O}_K$ lying over 8311 and $e = 3$. Let L be the totally real quintic field, with an A_5-extension as the splitting field, defined by $x^5 - x^4 - 16x^3 + 7x^2 + 57x + 35$ and $d_L = 8311^2$. There are 2 primes lying over 8311 in $\mathcal{O}_L$ with ramification indices $e_1 = 1$, and $e_2 = 2$ respectively. This implies if we take the composite field of K and the splitting field S of L, the ramification index of primes lying over 8311 in $\mathcal{O}_{KS}$ is divisible by 2 and thus at least 6. Thus, 8311 is ramified more in KS and it is not an unramified extension of K.

We will now prove our theorem.

Proof. Let K be the cyclic cubic field defined by $x^3 - x^2 - 3422x + 1521$ with $d_K = 10267^2$. There is only one prime in $\mathcal{O}_K$ lying over 10267 and $e = 3$. Let L be the totally real quintic field, with an A_5-extension as the splitting field, defined by $x^5 - 25x^3 - 7x^2 + 116x - 45$ and $d_L = 10267^2$. There are 3 primes lying over 10267 in $\mathcal{O}_L$ with ramification indices $e_1 = 1$, $e_2 = 1$, and $e_3 = 3$ respectively. Let S be the splitting field of L. So we know that $3 \mid e_S$. Since the characteristic of the residue field of 10267 in $\mathbb{Q}$ is 10267 and it is relatively prime to e_S, primes lying above 10267 are tamely ramified. Thus the inertia group in S is cyclic which implies $e_S = 1$, 2, 3 or 5 and thus $e_S = 3$. Now we take the composite field of K and the splitting field S. The Galois group $\mathrm{Gal}(KS/Q) = A_5 \times \mathbb{Z}_3$. Again, primes lying above 10267 are tamely ramified in $\mathcal{O}_{KS}$. Thus, $e_{KS} = 1$, 2, 3, 5, 6 or 15 because the inertia group in KS is cyclic and $A_5 \times \mathbb{Z}_3$ only has elements of orders 1, 2, 3, 5, 6 and 15. Also $e_{KS} = e_S e_{KS/S} = 3$ or 9. Thus, $e_{KS} = 3$. Therefore, KS is a non-solvable unramified extension of K.

We confirmed that the cyclic cubic field K defined by $x^3 - x^2 - 3422x + 1521$ and ramified at 10267 has a non-solvable unramified extension. Such extension is given by the

the composite field of K with the splitting field of the totally real quintic field defined by $x^5 - 25x^3 - 7x^2 + 116x - 45$, which is an A_5-extension of $\mathbb{Q}$. □

Theorem 4.10. *The cyclic cubic fields K defined by $x^3 - x^2 - 4020x + 76833$ and $x^3 - x^2 - 4020x - 92021$, both ramified at 7 and 1723, have an unramified A_5-extension. Moreover, such an extension of K is given by the composite field of K with the splitting field of the quintic polynomial $x^5 - 2x^4 - 23x^3 + 22x^2 + 140x + 9$, which is an A_5-extension of $\mathbb{Q}$.*

We follow the same strategy as the previous example and look for totally real quintic fields with splitting field an A_5-extension of $\mathbb{Q}$ but ramified at two primes (3 or primes congruent to 1 modulo 3). Here we list the first (in terms of field discriminants) several totally real quintic fields ramified at two primes that are 3 or primes congruent to 1 modulo 3, and with splitting field an A_5-extension of $\mathbb{Q}$. The list is obtained from John Jones' website *Number Fields.*

d_L	Polynomial
$3^2 \cdot 883^2$	$x^5 - 2x^4 - 12x^3 + 17x^2 + 30x - 31$
$7^2 \cdot 1579^2$	$x^5 - x^4 - 23x^3 + 25x^2 + 22x - 1$
$7^2 \cdot 1723^2$	$x^5 - 2x^4 - 23x^3 + 22x^2 + 140x + 9$

Let K be a cyclic cubic field ramified at 3 and 883. Let L be the totally real quintic field, with an A_5-extension as the splitting field, defined by $x^5 - 2x^4 - 12x^3 + 17x^2 + 30x - 31$ and $d_L = 3^2 \cdot 883^2$. There are 2 primes lying over 3 in $\mathcal{O}_L$ with ramification indices $e_1 = 1$, and $e_2 = 2$ respectively. This implies if we take the composite field of K with the splitting field S of L, the ramification index of primes lying over 3 in $\mathcal{O}_{KS}$ is divisible by 2 and thus at least 6. Thus, 3 is ramified more in KS and it is not an unramified extension of K.

Let K be a cyclic cubic field ramified at 7 and 1579. Let L be the totally real quintic field, with an A_5-extension as the splitting field, defined by $x^5 - x^4 - 23x^3 + 25x^2 + 22x - 1$ and $d_L = 7^2 \cdot 1579^2$. There are 2 primes lying over 7 in $\mathcal{O}_L$ with ramification indices $e_1 = 1$, and $e_2 = 2$ respectively. This implies if we take the composite field of K with the splitting field S of L, the ramification index of primes lying over 7 in $\mathcal{O}_{KS}$ is divisible by 2 and thus at least 6. Thus, 7 is ramified more in KS and it is not an unramified extension of K.

Now we proceed to find the two cyclic cubic fields ramified at 7 and 1723. We factor 7 and 1723 in the ring of algebraic integers of $\mathbb{Q}(\sqrt{-3})$ into the unique associates. $7 = \left(\frac{-1+3i\sqrt{3}}{2}\right)\left(\frac{-1-3i\sqrt{3}}{2}\right)$ and $1723 = \left(\frac{-40+42i\sqrt{3}}{2}\right)\left(\frac{-40-42i\sqrt{3}}{2}\right)$. Then, $\frac{u+3vi\sqrt{3}}{2} = \left(\frac{-1+3i\sqrt{3}}{2}\right)\left(\frac{-40+42i\sqrt{3}}{2}\right)$ or $\left(\frac{-1+3i\sqrt{3}}{2}\right)\left(\frac{-40-42i\sqrt{3}}{2}\right)$ $= \left(\frac{-169-81i\sqrt{3}}{2}\right)$ or $\left(\frac{209-39i\sqrt{3}}{2}\right)$. Thus, $u = -169$ or $u = 209$. The representing polynomials are $x^3 - x^2 - 4020x + 76833$ and $x^3 - x^2 - 4020x - 92021$.

Now we prove our theorem.

Proof. Let K be one of the cyclic cubic fields ramified at 7 and 1723. Let L be the totally real quintic field, with an A_5-extension as the splitting field, defined by $x^5 - 2x^4 - 23x^3 + 22x^2 + 140x + 9$ with $d_L = 7^2 \cdot 1723^2$. There are 3 primes lying over 7 and 1723 respectively in $\mathcal{O}_L$ with ramification indices $e_1 = 1$, $e_2 = 1$, and $e_3 = 3$ respectively for both 7 and 1723. Let S be the splitting field of L. So we know that $3 \mid e_S$. Since the characteristic of the residue field of 7 in $\mathbb{Q}$ is 7 and the characteristic of the residue field of 1723 in $\mathbb{Q}$ is 1723. The two characteristics are relatively prime to e_S, thus primes lying above 7 and 1723 are tamely ramified. Thus the inertia groups in S are cyclic which implies $e_S = 1$, 2, 3 or 5 and thus $e_S = 3$ for both 7 and 1723. Now we take the composite field of K and the splitting field S. The Galois group $\mathrm{Gal}(KS/Q) = A_5 \times \mathbb{Z}_3$. Similar to the previous proof, we have $e_{KS} = 1$, 2, 3, 5, 6 or 15. Also, we have $e_{KS} = e_S e_{KS/S} = 3$ or 9. Thus, we have $e_{KS} = 3$ for both 7 and 1723. Therefore, KS is an unramified extension of K. □

4.3 Unramified Extensions of Infinite Order

In 1964, Golod and Shafarevich [4] found first example of algebraic number field with infinite class field tower. In 1965, Brumer [1] showed that a number field with sufficiently many ramified prime ideals has infinite class field tower. In 1967, Roquette proved a sharper result (see [5]).

Theorem 4.11. *Let K be a normal extension of degree n over $\mathbb{Q}$, let r be the number of infinite places of K, and let p be a prime with exponent $v_p(n) > 0$ in n. Moreover let t_p be the number of primes which are ramified in K with ramification index $e \equiv 0 \pmod{p}$. Then K has infinite class field tower if*

$$t_p \geqslant \frac{r-1}{p-1} + v_p(n)\delta_p + 2 + 2\sqrt{r+\delta_p},$$

where $\delta_p = 1$ if the p-th roots of unity are in K and $\delta_p = 0$ if not.

When K is a cyclic cubic field, $n = 3$, $r = 3$, $p = 3$, $v_3(3) = 1$, $\delta_3 = 0$. Thus, K has infinite class field tower if $t_3 \geqslant \frac{3-1}{3-1} + 0 + 2 + 2\sqrt{3+0} \approx 6.46$. That means K has infinite class field tower if 7 or more primes are ramified in K. My goal is to construct a cubic polynomial which represents a cyclic cubic field with 7 ramified primes.

We applied Theorem 2.7 to construct two examples:

Example 4.12. We want a cyclic cubic field K to have discriminant $e^2 = (3^4)(7^2)(13^2)(19^2)$ $(31^2)(37^2)(43^2)$. Using the algorithm in the proof of Theorem 2.7, we find a solution of u which is 3(73). Thus, K defined by the polynomial $f(x) = x^3 - 255828027x + 6225148657$ has 7 ramified primes. According to Theorem 4.11, K has infinite class field tower and the unramified extension of K is infinite.

Example 4.13. We want a cyclic cubic field K to have discriminant $e^2 = (7^2)(13^2)(19^2)(31^2)$ $(37^2)(43^2)(61^2)$. Using the algorithm in the proof of Theorem 2.7, we find a solution of

u which is 2582. Thus, K defined by the polynomial $f(x) = x^3 - x^2 - 1733945516x - 496871720736$ has 7 ramified primes. According to Theorem 4.11, K has infinite class field tower and the unramified extension of K is infinite.

Bibliography

[1] A. Brumer. Ramification and class towers of number fields. *Michigan Math. J.*, 12:129–131, 1965.

[2] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[3] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[4] E. S. Golod and I. R. Šafarevič. On the class field tower. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28:261–272, 1964.

[5] H. Koch. *Algebraic number theory.* Springer-Verlag, Berlin, russian edition, 1997. Reprint of the 1992 translation.

[6] Daniel A. Marcus. *Number fields.* Springer-Verlag, New York, 1977. Universitext.

[7] Jacques Martinet. Petits discriminants des corps de nombres. In *Number theory days, 1980 (Exeter, 1980)*, volume 56 of *London Math. Soc. Lecture Note Ser.*, pages 151–193. Cambridge Univ. Press, Cambridge, 1982.

[8] Carlos Julio Moreno. *Advanced analytic number theory: L-functions*, volume 115 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, RI, 2005.

[9] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[10] A. M. Odlyzko. Lower bounds for discriminants of number fields. *Acta Arith.*, 29(3):275–297, 1976.

[11] Ken Yamamura. Maximal unramified extensions of imaginary quadratic number fields of small conductors. *J. Théor. Nombres Bordeaux*, 9(2):405–448, 1997.