Dirichlet Series Associated to Cubic and Quartic Fields with given Resolvent

Karim Belabas, Henri Cohen, and Anna Morra,
Université Bordeaux I,
Institut de Mathématiques, U.M.R. 5251 du C.N.R.S,
351 Cours de la Libération,
33405 TALENCE Cedex, FRANCE

October 17, 2011

In [4] and [1] we were mainly interested in giving asymptotic results for the number of cubic and quartic number fields having given quadratic and cubic resolvent respectively. In the present paper, which is a sequel to these two papers, we want to give explicit formulas for the corresponding Dirichlet series. We will divide the paper in three parts: the first and second will be devoted to the cubic and quartic case respectively, and the third to detailed examples. The main result in the cubic case is Theorem 3.5, in the quartic A_4 case it is Conjecture 5.8, and in the quartic S_4 case it is Conjecture 6.19. Although these are named "conjectures", they should be easy to prove from the results of [1]. All the other conjectures should be either classical or easy exercises in algebraic number theory.

PART I: THE CUBIC CASE

1 Introduction and Notation

This part of the paper is a sequel to [4]. In that paper, we compute the number of isomorphism classes of cubic extensions of a given base number field k having a given quadratic resolvent field K_2. In particular, we give the asymptotic value of this quantity and an exact formula for the corresponding Dirichlet series. Although this latter formula is completely explicit it is quite complicated, and in [4] we show that it has a very simple form when K_2 is an imaginary quadratic field of class number coprime to 3. The purpose of this paper is to generalize this to any quadratic field K_2, and in particular we assume that that the base field k is equal to $\mathbb{Q}$, in other words we enumerate isomorphism classes of cubic number fields having a given K_2.

It is interesting to note that as an aside we prove a generalization of Ohno's conjecture proved by Nakagawa on the enumeration of binary cubic forms which is of interest for its own sake.

In what follows, by abuse of language we use the term "cubic field" to mean "isomorphism class of cubic number fields".

Definition 1.1 *Let L be a cubic field. For a prime number p we set*

$$\omega_L(p) = \begin{cases} 2 & \text{if } p \text{ is totally split in } L\ , \\ -1 & \text{if } p \text{ is inert in } L\ , \\ 0 & \text{otherwise.} \end{cases}$$

Note that we have $\omega_L(p) = 0$ if and only if $\left(\frac{\operatorname{disc}(L)}{p}\right) \neq 1$, and since in all cases that we will use we have $\operatorname{disc}(L) = -D/3$, $-3D$, or $-27D$ for some fundamental discriminant D, for $p \neq 3$ this is true if and only if $\left(\frac{-3D}{p}\right) \neq 1$. Thus, in Euler products involving the quantities $1 + \omega_L(p)/p^s$ we can either include all $p \neq 3$, or restrict to $\left(\frac{-3D}{p}\right) = 1$.

Definition 1.2 *1. Let D be a fundamental discriminant (including 1). We set $D^* = -3D$ if $3 \nmid D$ and $D^* = -D/3$ if $3 \mid D$, and call it the* mirror discriminant *of D.*

2. For any fundamental discriminant D we denote by $\operatorname{rk}_3(D)$ the 3-rank of the class number of the field $\mathbb{Q}(\sqrt{D})$.

3. We let $\mathcal{D}^+$ be the set of all fundamental discriminants $D > 1$ together with $D = -3$, and we let $\mathcal{D}^-$ be the set of all fundamental discriminants $D < -3$ together with $D = 1$.

Remarks 1.3 *1. The set of all fundamental discriminants is thus the disjoint union of $\mathcal{D}^+$ and $\mathcal{D}^-$, and the mirror map exchanges them.*

2. Scholtz's theorem tells us that for $D < 0$ we have $0 \leq \mathrm{rk}_3(D) - \mathrm{rk}_3(D^*) \leq 1$ (or equivalently that for $D > 0$ we have $0 \leq \mathrm{rk}_3(D^*) - \mathrm{rk}_3(D) \leq 1$), and gives also a necessary and sufficient condition for $\mathrm{rk}_3(D) = \mathrm{rk}_3(D^*)$ in terms of the fundamental unit of the real field.

Definition 1.4 *1. For any integer N we let $\mathcal{L}_N$ be the set of cubic fields of discriminant N.*

2. If $K_2 = \mathbb{Q}(\sqrt{D})$ with D fundamental we denote by $\mathcal{F}(K_2)$ the set of cubic fields with resolvent field equal to K_2, or equivalently of discriminant of the form Df^2.

3. With a slight abuse of notation, we let

$$\mathcal{L}_3(K_2) = \mathcal{L}_3(D) = \mathcal{L}_{D^*} \cup \mathcal{L}_{-27D} \ .$$

Remarks 1.5 *1. We will use the notation $\mathcal{L}_N$ only with $N = D^*$ or $N = -27D$, for D a fundamental discriminant.*

2. It is clear that

$$\mathcal{F}(K_2) = \bigsqcup_{f \geq 1} \mathcal{L}_{Df^2} \ .$$

2 Properties of Discriminants of Cubic Fields

Theorem 2.1 *If K is a cubic field then $v_3(\mathrm{disc}(K))$ can only be equal to 0, 1, 3, 4, and 5 in relative proportions $24/35$, $8/35$, $2/35$, $2/105$, and $1/105$.*

Proof. The proof that $v_3(\mathrm{disc}(K))$ can take only the given values is classical, see for instance [5] and Corollary 2.6 below. The given proportions follows from the proof of the Davenport–Heilbronn theorem. ☐

A detailler par K.B., proportions peut etre fausses.

Theorem 2.2 *Let D be a fundamental discriminant, and set $r = \mathrm{rk}_3(D^*)$.*

1. *Assume that $D \in \mathcal{D}^-$. We have*

$$\left(|\mathcal{L}_{D^*}|, |\mathcal{L}_{-27D}|\right) = \begin{cases} ((3^r-1)/2, 3^r) & \text{if } \mathrm{rk}_3(D) = r+1 \ , \\ ((3^r-1)/2, 0) & \text{if } \mathrm{rk}_3(D) = r \ . \end{cases}$$

In particular, $|\mathcal{L}_3(D)| = (3^{\mathrm{rk}_3(D)} - 1)/2$.

2. *Assume that $D \in \mathcal{D}^+$. We have*

$$\left(|\mathcal{L}_{D^*}|, |\mathcal{L}_{-27D}|\right) = \begin{cases} ((3^r-1)/2, 0) & \text{if } \mathrm{rk}_3(D) = r-1 \ , \\ ((3^r-1)/2, 3^r) & \text{if } \mathrm{rk}_3(D) = r \ . \end{cases}$$

In particular, $|\mathcal{L}_3(D)| = (3^{\mathrm{rk}_3(D)+1} - 1)/2$.

Proof. .... ☐

A faire par K.B.

It follows from this theorem that $\mathcal{L}_3(D) = \emptyset$ if and only if $D \in \mathcal{D}^-$ and $\mathrm{rk}_3(D) = 0$, i.e., $3 \nmid h(D)$, which is exactly the case treated in [4].

The following (apart from (1), which is classical) is essentially Nakagawa's theorem:

Corollary 2.3

1. *If $D \in \mathcal{D}^-$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (0,0)$ there do not exist any cubic field of discriminant D^* or $-27D$.*

2. *If $D \in \mathcal{D}^-$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (1,0)$ there exist no cubic field of discriminant D^* and a unique cubic field of discriminant $-27D$.*

3. *If $D \in \mathcal{D}^-$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (1,1)$ there exist a unique cubic field of discriminant D^* and no cubic field of discriminant $-27D$.*

4. *If $D \in \mathcal{D}^+$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (0,0)$ there exist no cubic field of discriminant D^* and a unique cubic field of discriminant $-27D$.*

5. *If $D \in \mathcal{D}^+$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (0,1)$ there exist a unique cubic field of discriminant D^* and no cubic field of discriminant $-27D$.*

Proof. Clear. ☐

Proposition 2.4 *1. If $D \in \mathcal{D}^-$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (2,1)$ or $D \in \mathcal{D}^+$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (1,1)$ there exist a unique cubic field of discriminant D^* and three cubic fields of discriminant $-27D$.*

2. If $D \in \mathcal{D}^-$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (2,2)$ or $D \in \mathcal{D}^+$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (1,2)$ there exist four cubic fields of discriminant D^* and no cubic field of discriminant $-27D$.

In addition, if $3 \nmid D$ then 3 is partially ramified in the four cubic fields, if $D \equiv 3 \pmod 9$ then 3 is partially split in the four cubic fields, and if $D \equiv 6 \pmod 9$ then 3 is totally split in one of the four cubic fields and inert in the three others.

Proof. The first statements are special cases of the theorem, the behavior of 3 when $3 \nmid D$ is classical (see [5] or Proposition 2.5 (3)), and when $D \equiv 3 \pmod 9$ is trivial since $D^* \equiv 2 \pmod 3$. Thus assume that $D \equiv 6 \pmod 9$....

A completer par K.B.

□

Proposition 2.5 *Let L be a cubic field, write $\mathrm{disc}(L) = Df^2$ with D a fundamental discriminant, and let p be a prime.*

1. *If $p \neq 3$ we have $v_p(f) \leq 1$ and $p \nmid \gcd(D, f)$.*
2. *We have $v_3(f) \leq 2$, and if $v_3(f) = 1$ then $3 \mid D$.*
3. *p is totally ramified in L if and only if $p \mid f$.*
4. *p is partially ramified in L if and only if $p \mid D$ and $p \nmid f$.*

Proof. This is classical, and we refer to [2] Section 10.1.5 for a proof, except for (2) which can be easily deduced from loc. cit. Note that the last statement of (2) is true but empty for cyclic cubic fields since we have $v_3(f) = 0$ or 2. □

Donner une preuve de (2) et expliquer pourquoi on ne peut pas avoir $v_3(f) = 1$ si L est cubique cyclique

Corollary 2.6 *1. The prime 3 is totally ramified in a cubic field L if and only if $27 \mid \mathrm{disc}(L)$.*

2. *If L is a cubic field we have $v_3(\mathrm{disc}(L)) = 0$, 1, 3, 4, or 5.*

Proof. If 3 is totally ramified then $3 \mid f$, so either $v_3(f) = 2$, in which case $v_3(\mathrm{disc}(L)) = 4 + v_3(D) = 4$ or 5, or $v_3(f) = 1$, in which case $v_3(D) = 1$ so $v_3(\mathrm{disc}(L)) = 3$. On the other hand, if 3 is not totally ramified then $3 \nmid f$, so $v_3(\mathrm{disc}(L)) = v_3(D) = 0$ or 1. $\square$

3 The Main Theorem

If K is a cubic field with resolvent field $K_2 = \mathbb{Q}(\sqrt{D})$, we have $\mathrm{disc}(K) = Df^2$, and we set $f(K) = f$. In fact, f is the unique positive integer such that $f\mathbb{Z}_{K_2}$ is the conductor of the cubic cyclic extension K^g/K_2, where K^g is the Galois closure of K over $\mathbb{Q}$.

Definition 3.1 *If D is a fundamental discriminant we define*

$$\Phi_D(s) := \frac{1}{2} + \sum_{K \in \mathcal{F}(\mathbb{Q}(\sqrt{D}))} \frac{1}{f(K)^s} .$$

Corollary 3.2 *If $3 \nmid D$ and $\Phi_D(s) = \sum_{f \geq 1} a(f)/f^s$, if $a(f) \neq 0$ we have either $v_3(f) = 0$ or $v_3(f) \geq 2$, in other words $v_3(f) \neq 1$.*

Proof. Indeed, if $v_3(f) = 1$ we would have $v_3(Df^2) = 2$, which is impossible if Df^2 is the discriminant of a cubic field. $\square$

We define Euler factors at 3 as follows:

Definition 3.3 1. *We define*

$$M_{3,1}(s) = \begin{cases} 1 + 2/3^{2s} & \text{if } 3 \nmid D , \\ 1 + 2/3^s & \text{if } D \equiv 3 \pmod 9 , \\ 1 + 2/3^s + 6/3^{2s} & \text{if } D \equiv 6 \pmod 9 . \end{cases}$$

2. *Let $L \in \mathcal{L}_{-27D}$. We define*

$$M_{3,2,L}(s) = \begin{cases} 1 - 1/3^{2s} & \text{if } 3 \nmid D , \\ 1 - 1/3^s & \text{if } 3 \mid D . \end{cases}$$

3. Let $L \in \mathcal{L}_{D^*}$. We define

$$M_{3,2,L}(s) = \begin{cases} 1 + 2/3^{2s} & \text{if } 3 \nmid D\ , \\ 1 + 2/3^s & \text{if } D \equiv 3 \pmod{9}\ , \\ 1 + 2/3^s + 3\omega_L(3)/3^{2s} & \text{if } D \equiv 6 \pmod{9}\ . \end{cases}$$

Remarks 3.4 *1. When $D \equiv 3 \pmod{9}$ we have $D^* \equiv 2 \pmod{3}$, so 3 is partially split in any cubic field of discriminant D^*. It follows that when $L \in \mathcal{L}_{D^*}$ we have $M_{3,2,L}(s) = 1 + 2/3^s + 3\omega_L(3)/3^{2s}$ for all D such that $3 \mid D$.*

2. When $3 \nmid D$ there are no terms in $1/3^s$, in accordance with Corollary 3.2.

Theorem 3.5 (Main Theorem for Cubic Fields) *Let D be a fundamental discriminant. We have*

$$c_D\Phi_D(s) = \frac{1}{2}M_{3,1}(s) \prod_{\left(\frac{-3D}{p}\right)=1} \left(1 + \frac{2}{p^s}\right) + \sum_{L \in \mathcal{L}_3(D)} M_{3,2,L}(s) \prod_{\left(\frac{-3D}{p}\right)=1} \left(1 + \frac{\omega_L(p)}{p^s}\right)\ ,$$

where $c_D = 1$ if $D \in \mathcal{D}^-$ and $c_D = 3$ if $D \in \mathcal{D}^+$.

Remark 3.6 *As mentioned above, if desired, in the terms involving $L \in \mathcal{L}_{D^*}$ the condition $\left(\frac{-3D}{p}\right) = 1$ can be replaced by $p \neq 3$ and even omitted altogether if $3 \nmid D$, and in the terms involving $L \in \mathcal{L}_{-27D}$ it can be omitted.*

Proof. ... □

A faire par A.M.

See Section 7 below for examples in each possible case.

PART II: THE QUARTIC CASE

4 The Quartic Case: Introduction and Notation

We now come to the similar but *theoretically simpler* case of counting quartic extensions having given cubic resolvent. The reason that this case is simpler is the following: in the cubic case, it is necessary to count cyclic cubic extensions of a quadratic field, and for this (because of Kummer theory, or equivalently, of class field theory) we must adjoin cube roots of unity, which complicates matters. On the other hand, in the quartic case, we must count V_4 extensions of a cubic field having certain properties, and here it is *not* necessary to adjoin any root of unity since the square roots of unity are already in the base field.

Even though the theory is simpler, the formulas are longer simply because the number of splitting types in a quartic field is much larger than in a cubic field.

If $K/\mathbb{Q}$ is an A_4 or S_4-extension and if we denote by k its resolvent cubic field (cyclic for A_4 extensions, noncyclic otherwise), then $\operatorname{disc}(K) = \operatorname{disc}(k)\mathcal{N}(\mathfrak{d}(K_6/k))$ for a quadratic extension $K_6 = k(\sqrt{\alpha})$ of k *of square norm*, meaning that $\mathcal{N}(\alpha)$ is a square in $\mathbb{Q}^*$. More precisely, we have the following relation between zeta functions, coming from simple character relations, which implies the discriminant equality:

Proposition 4.1 *We have*

$$\zeta_L(s) = \frac{\zeta(s)\zeta_{K_6}(s)}{\zeta_k(s)} \ .$$

For future reference, note the following:

Corollary 4.2

1. *A prime p is totally ramified in L if and only if all the prime ideals above p in k are ramified in the quadratic extension K_6/k.*
2. *If $p \neq 2$, then p can be totally ramified in L only if p is partially ramified in k ($p\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$).*

Proof. (1). The prime p is totally ramified in L if and only if the Euler factor at p of $\zeta_L(s)$ is equal to $(1 - 1/p^s)^{-1}$, equal to that of $\zeta(s)$, so by the proposition, if and only if the Euler factors at p of $\zeta_{K_6}(s)$ and $\zeta_k(s)$ are the same, which is the condition given in (1).

(2). It is easy to see that for $\mathfrak{p}$ a prime ideal of k such that $\mathfrak{p} \nmid 2\mathbb{Z}_k$ then $v_{\mathfrak{p}}(\mathfrak{d}(K_6/k)) \leq 1$ (in fact if $\alpha\mathbb{Z}_k = \mathfrak{a}\mathfrak{q}^2$ with $\mathfrak{a}$ squarefree we have $\mathfrak{d}(K_6/k) = 4\mathfrak{a}/\mathfrak{c}^2$ for some $\mathfrak{c} \mid 2\mathbb{Z}_k$). Since $\mathcal{N}(\mathfrak{d}(K_6/k))$ is a square, we have $v_p(\mathcal{N}(\mathfrak{d}(K_6/k))) \equiv 0 \pmod{2}$, or equivalently

$$\sum_{\substack{\mathfrak{p}|p\mathbb{Z}_k \\ \mathfrak{p}|\mathfrak{d}(K_6/k)}} f(\mathfrak{p}/p) \equiv 0 \pmod{2} .$$

By (1), if p is totally ramified in L we have $\mathfrak{p} \mid p\mathbb{Z}_k$ implies $p \mid \mathfrak{d}(K_6/k)$, so $\sum_{\mathfrak{p}|p\mathbb{Z}_k} f(\mathfrak{p}/p) \equiv 0 \pmod{2}$. When p is unramified this sum is equal to 3, and when p is totally ramified it is equal to 1, so the only remaining possibility is when p is partially ramified, in which case the sum is equal to 2. $\square$

Since there exists a positive integer f such that $\mathcal{N}(\mathfrak{d}(K_6/k)) = f^2$, we will write $f = f(K)$. Thus, if we denote by $\mathcal{F}(k)$ the set of isomorphism classes of quartic extensions whose cubic resolvent is isomorphic to k we have

$$\sum_{K \in \mathcal{F}(k)} \frac{1}{|\operatorname{disc}(K)|^s} = \frac{1}{\operatorname{disc}(k)^s} \sum_{K \in \mathcal{F}(k)} \frac{1}{f(K)^{2s}} .$$

It is thus natural to set the following definition:

Definition 4.3 *For a cubic field k, we set*

$$\Phi_k(s) = \frac{1}{a(k)} + \sum_{K \in \mathcal{F}(k)} \frac{1}{f(K)^s} ,$$

where $a(k) = 3$ if k is cyclic and $a(k) = 1$ otherwise.

Note. This differs slightly from the definition given in [1]. Note also that there is a misprint in the definition of square norm, where "$\mathcal{N}_{K_6/k}(\alpha)$ square in k" should be replaced by what we have written, i.e., "$\mathcal{N}(\alpha)$ square in $\mathbb{Q}$".

For ease of reference, note the following results.

Proposition 4.4 *1. The equation of the cubic resolvent of a quartic polynomial $x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ is*

$$x^3 - a_2x^2 + (a_1a_3 - 4a_0)x + 4a_0a_2 - a_1^2 - a_0a_3^2 ,$$

whose (polynomial) discriminant is the same as the (polynomial) discriminant of the quartic.

2. *If $K_6 = k(\sqrt{\alpha})$ with α of square norm with characteristic polynomial $x^3 + a_2x^2 + a_1x + a_0$, the corresponding quartic field is given by the equation*
$$x^4 + 2a_2x^2 - 8\sqrt{-a_0}x + a_2^2 - 4a_1 ,$$
whose (polynomial) discriminant is 2^{12} times the (polynomial) discriminant of the cubic.

Since in the quartic case there are so many decomposition types, we introduce the following abbreviations, given in the following table, where p is a prime, k is always a cubic field, and L a quartic field:

Field	Splitting	Degrees	Abbreviation
k	$p\mathbb{Z}_k = \mathfrak{p}_1$	(3)	IN
k	$p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2$	$(2,1)$	PS
k	$p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$(1,1,1)$	TS
k	$p\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$	$(1,1)$	PR
k	$p\mathbb{Z}_k = \mathfrak{p}_1^3$	(1)	TR
L	$p\mathbb{Z}_L = \mathfrak{p}_1$	(4)	IN
L	$p\mathbb{Z}_L = \mathfrak{p}_1\mathfrak{p}_2$	$(3,1)$	$\mathrm{PS}_{3,1}$
L	$p\mathbb{Z}_L = \mathfrak{p}_1\mathfrak{p}_2$	$(2,2)$	$\mathrm{PS}_{2,2}$
L	$p\mathbb{Z}_L = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$(2,1,1)$	$\mathrm{PS}_{2,1,1}$
L	$p\mathbb{Z}_L = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$(1,1,1,1)$	TS
L	$p\mathbb{Z}_L = \mathfrak{p}_1^2\mathfrak{p}_2$	$(1,2)$	$\mathrm{PR}_{2,1}$
L	$p\mathbb{Z}_L = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$	$(1,1,1)$	$\mathrm{PR}_{2,1,1}$
L	$p\mathbb{Z}_L = \mathfrak{p}_1^2\mathfrak{p}_2^2$	$(1,1)$	$\mathrm{PR}_{2,2}$
L	$p\mathbb{Z}_L = \mathfrak{p}_1^2$	(2)	PR_2
L	$p\mathbb{Z}_L = \mathfrak{p}_1^3\mathfrak{p}_2$	$(1,1)$	$\mathrm{PR}_{3,1}$
L	$p\mathbb{Z}_L = \mathfrak{p}_1^4$	(1)	TR

The reasons for the symbols are as follows: IN, PS, TS, PR, and TR are for inert, partially split, totally split, partially ramified, and totally ramified respectively, the indices for PS are the residual indexes, while the indices for PR are the ramification degrees.

Definition 4.5 *For an ideal $\mathfrak{c} \mid 2\mathbb{Z}_k$ we define*

$$C(\mathfrak{c}^2) = \frac{\{\mathfrak{a}/\ (\mathfrak{a},\mathfrak{c}) = 1,\ \mathcal{N}(\mathfrak{a})\ \textit{square}\}}{\{\mathfrak{q}^2\beta/\ (\mathfrak{q}^2\beta,\mathfrak{c}) = 1,\ \beta \equiv 1 \pmod{{}^*\mathfrak{c}^2},\ \mathcal{N}(\beta)\ \textit{square}\}}$$

(which is a finite group), and we define $X(\mathfrak{c}^2)$ to be the group of characters of $C(\mathfrak{c}^2)$.

(Note that there is a misprint in Definition 2.2 of [1], the condition $\beta \equiv 1 \pmod{{}^*\mathfrak{c}^2}$ having been omitted from the denominator.)

Since trivially $C(\mathfrak{c}^2)$ has exponent dividing 2, all the elements of $X(\mathfrak{c}^2)$ are quadratic characters, which can be applied only on ideals of square norm. With this definition, the main result of [1] is the following:

Theorem 4.6

$$\Phi_k(s) = \frac{1}{a(k)2^{r_2(k)}2^{3s-2}} \sum_{\mathfrak{c}|2\mathbb{Z}_k} \mathcal{N}(\mathfrak{c})^{s-1} z_k(\mathfrak{c}) \prod_{\mathfrak{p}|\mathfrak{c}} \left(1 - \frac{1}{\mathcal{N}(\mathfrak{p})^s}\right) \sum_{\chi \in X_{\mathfrak{c}^2}} F_k(\chi, s) \ ,$$

where $r_2(k)$ is half the number of complex places of k,

$$F_k(\chi, s) = \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2} \left(1 + \frac{\chi(\mathfrak{p}_2)}{p^s}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2} \left(1 + \frac{\chi(\mathfrak{p}_1\mathfrak{p}_2)}{p^s}\right)$$
$$\prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{\chi(\mathfrak{p}_1\mathfrak{p}_2) + \chi(\mathfrak{p}_1\mathfrak{p}_3) + \chi(\mathfrak{p}_2\mathfrak{p}_3)}{p^s}\right) \ ,$$

where in the product over $p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2$ it is understood that $\mathfrak{p}_1$ has degree 1 and $\mathfrak{p}_2$ has degree 2, $z_k(s) = 1$ or 2, with $z_k(s) = 2$ if and only if either $c = 2\mathbb{Z}_k$, or $2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$ and $\mathfrak{c} = \mathfrak{p}_1\mathfrak{p}_2$, or $2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$, $\operatorname{disc}(k) \equiv 4 \pmod 8$, and $\mathfrak{c} = \mathfrak{p}_2$, or $2\mathbb{Z}_k = \mathfrak{p}_1^3$ and $\mathfrak{c} = \mathfrak{p}_1^2$.

It follows in particular from this theorem that for $p \neq 2$ the quantities occurring in the products over $p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2$ or $p\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$ are of the form $1 \pm 1/p^s$, and those in the products over $p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ are either of the form $1 + 3/p^s$ (if all the χ values are equal to 1), or $1 - 1/p^s$ (if one of the χ value is 1 and the other two -1; note that since $(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^2 = p^2$, the product of the χ values is equal to 1). For $p = 2$, some of the χ values may vanish, so we may also have factors equal to 1, or when 2 is totally split and $\mathfrak{c} = \mathfrak{p}_i$ for some i, factors $1 + 1/p^s$.

Because of this theorem, we introduce a notation specific to the PR case:

Definition 4.7 *Let k be a cubic field and assume that 2 is* PR*, in other words that $2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$. We will write that 2 is* PR_0 *(resp.,* PR_4*) in k if 2 is* PR *and* $\operatorname{disc}(k) \equiv 0 \pmod 8$ *(resp.,* $\operatorname{disc}(k) \equiv 4 \pmod 8$*).*

We will also sometimes write that 2 is TR_4 with a similar definition, but this is in fact redundant since if 2 is TR in a cubic field k we have $\mathrm{disc}(k) \equiv 4 \pmod 8$.

Proposition 4.8 *Let k be a cubic field.*

1. *If k is complex the group $X(4\mathbb{Z}_k)$ is never trivial.*
2. *If k is totally real and $2 \nmid h^+(k)$, the narrow class number of k, then for all $\mathfrak{c} \mid 2\mathbb{Z}_k$ the group $X(\mathfrak{c}^2)$ is trivial, in other words no nontrivial characters occur in Theorem 4.6.*
3. *Conversely, if $X(4\mathbb{Z}_k)$ is trivial then $X(\mathfrak{c}^2)$ is trivial for all $\mathfrak{c} \mid 2\mathbb{Z}_k$, and k is totally real with $2 \nmid h^+(k)$.*

Proof. (1). By Corollary 3.3 of [1], we have

$$|C(4\mathbb{Z}_k)| = |Z_2[N]/Z_2^2||S_4[N]|/2^r ,$$

where r is the unit rank of k. Furthermore, by Proposition 3.4 and Corollary 3.6 we have $|Z_2[N]/Z_2^2| = 4$, so that independently of the signature of k we have $|C(4\mathbb{Z}_k)| = 2^{2-r}|S_4[N]|$. (1) follows immediately since $r = 1$.

(2). Since trivially $X(4\mathbb{Z}_k)$ surjects on $X(\mathfrak{c}^2)$ for all $\mathfrak{c} \mid 2\mathbb{Z}_k$, it is sufficient to show that $C(4\mathbb{Z}_k)$ is trivial, and since $r = 2$ in the totally real case, by the above formula we must show that $S_4[N]$ is trivial. By definition, it is clear that this is equivalent to the following statement: if ε is a unit of positive norm such that $x^2 \equiv \varepsilon \pmod{4\mathbb{Z}_k}$ has a solution, then ε is a square in k. Indeed, consider the field $K_6 = k(\sqrt{\varepsilon})$. By [2], we have $\mathfrak{d}(K_6/k) = 4\mathbb{Z}_k/4 = \mathbb{Z}_k$, so K_6/k is unramified outside infinity. By class field theory, if K_6 was a quadratic extension this would mean that $2 \mid h^+(k)$, in contradiction with our assumption. Thus $K_6 = k$, in other words ε is a square, proving (2).

(3). Since there is a natural surjection from $X(4\mathbb{Z}_k)$ to $X(\mathfrak{c}^2)$ for all $\mathfrak{c} \mid 2\mathbb{Z}_k$, the first statement is clear. The second will follow from Proposition 6.2 (2) below. ◻

In view of the above remarks, analogously to the cubic case it is natural to set the following definition:

Definition 4.9 *Let L be a quartic A_4 or S_4 field. For a prime number p we set*

$$\omega_L(p) = \begin{cases} 3 & \text{if } p \text{ is } \mathrm{TS} \text{ in } L\ , \\ 1 & \text{if } p \text{ is } \mathrm{PS}_{2,1,1} \text{ or } \mathrm{PR}_{2,1,1} \text{ in } L\ , \\ -1 & \text{if } p \text{ is } \mathrm{IN},\ \mathrm{PS}_{2,2}, \text{ or } \mathrm{PR}_{2,1} \text{ in } L\ , \\ 0 & \text{if } p \text{ is } \mathrm{PS}_{3,1},\ \mathrm{PR}_2,\ \mathrm{PR}_{2,2},\ \mathrm{PR}_{3,1}, \text{ or } \mathrm{TR} \text{ in } L\ . \end{cases}$$

Proposition 4.10 *Let L be a quartic A_4 or S_4-field, and let k be its cubic resolvent.*

1. *Let $p \geq 3$ be a prime number.*
   (a) *If p is* IN *in k then p is* $\mathrm{PS}_{3,1}$ *in L, so that $\omega_L(p) = 0$.*
   (b) *If p is* TS *in k then either p is* TS *in L (so that $\omega_L(p) = 3$), or p is* $\mathrm{PS}_{2,2}$ *in L (so that $\omega_L(p) = -1$), or p is* PR_2 *or* $\mathrm{PR}_{2,2}$ *(so that $\omega_L(p) = 0$).*
   (c) *If p is* PS *in k then either p is* IN *in L (so that $\omega_L(p) = -1$), or p is* $\mathrm{PS}_{2,1,1}$ *in L (so that $\omega_L(p) = 1$), or p is* PR_2 *or* $\mathrm{PR}_{2,2}$ *in L (so that $\omega_L(p) = 0$).*
   (d) *If p is* PR *in k then either p is* $\mathrm{PR}_{2,1}$ *in L (so that $\omega_L(p) = -1$) or p is* $\mathrm{PR}_{2,1,1}$ *in L (so that $\omega_L(p) = 1$), or p is* TR *in L (so that $\omega_L(p) = 0$).*
   (e) *If p is* TR *in k then p is* $\mathrm{PR}_{3,1}$ *in L (so that $\omega_L(p) = 0$).*
2. *Assume now that $p = 2$. In addition to the above decomposition types, in all cases 2 can also be* TR *in L, and if 2 is* PR *in k then 2 can also be* PR_2 *or* $\mathrm{PR}_{2,2}$ *in L.*

Proof. This follows from a tedious case by case study from Proposition 4.1, Stickelberger's theorem stating that if p is unramified in some number field K and has g prime ideal factors then $\left(\frac{\mathrm{disc}(K)}{p}\right) = (-1)^{n-g}$, and Corollary 4.2, and is left to the reader. ☐

Evidently (c) and (d) can occur only for S_4 fields.

Statements (1) of this proposition can be summarized in the following table, where the notation for splitting types is self-explanatory (recall that we assume that $p \neq 2$):

Code in k	Splitting in k	Splitting in L	Code in L	$\omega_L(p)$
IN	3^1	$1^1 \cdot 3^1$	$\mathrm{PS}_{3,1}$	0
TS	$1^1 \cdot 1^1 \cdot 1^1$	$1^1 \cdot 1^1 \cdot 1^1 \cdot 1^1$	TS	3
TS	$1^1 \cdot 1^1 \cdot 1^1$	$2^1 \cdot 2^1$	$\mathrm{PS}_{2,2}$	-1
TS	$1^1 \cdot 1^1 \cdot 1^1$	2^2	PR_2	0
TS	$1^1 \cdot 1^1 \cdot 1^1$	$1^2 \cdot 1^2$	$\mathrm{PR}_{2,2}$	0
PS	$1^1 \cdot 2^1$	4^1	IN	-1
PS	$1^1 \cdot 2^1$	$1^1 \cdot 1^1 \cdot 2^1$	$\mathrm{PS}_{2,1,1}$	1
PS	$1^1 \cdot 2^1$	2^2	PR_2	0
PS	$1^1 \cdot 2^1$	$1^2 \cdot 1^2$	$\mathrm{PR}_{2,2}$	0
PR	$1^2 \cdot 1^1$	1^4	TR	0
PR	$1^2 \cdot 1^1$	$1^2 \cdot 2^1$	$\mathrm{PR}_{2,1}$	-1
PR	$1^2 \cdot 1^1$	$1^2 \cdot 1^1 \cdot 1^1$	$\mathrm{PR}_{2,1,1}$	1
TR	1^3	$1^3 \cdot 1^1$	$\mathrm{PR}_{3,1}$	0

Splitting Types for $p \neq 2$

5 The Quartic A_4 Case

5.1 General Results

We begin by the simplest case, that of quartic A_4-extensions. Here k is a cyclic cubic field. In particular k is totally real ($r_2(k) = 0$), 2 can be only either inert or totally split, and the other primes can also be totally ramified. In particular, we have $z_k(\mathfrak{c}) = 2$ if and only if $\mathfrak{c} = 2\mathbb{Z}_k$, and

$$F_k(\chi, s) = \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{\chi(\mathfrak{p}_1\mathfrak{p}_2) + \chi(\mathfrak{p}_1\mathfrak{p}_3) + \chi(\mathfrak{p}_2\mathfrak{p}_3)}{p^s}\right) .$$

We define Euler factors at 2 as follows:

Definition 5.1 *We set*

$$M_{2,1}(s) = \begin{cases} 1 + 3/2^{3s} & \text{if } 2 \text{ is inert in } k\ , \\ 1 + 3/2^{2s} + 6/2^{3s} + 6/2^{4s} & \text{if } 2 \text{ is totally split in } k\ , \end{cases}$$

Proposition 5.2 *If k is a cyclic cubic field, the contribution of the trivial characters is equal to*

$$\frac{1}{3} M_{2,1}(s) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p \neq 2} \left(1 + \frac{3}{p^s}\right) .$$

In particular, this is equal to $\Phi_k(s)$ *if and only if* $2 \nmid h(k)$.

Proof. By what we have just said, the contribution of the trivial characters is equal to

$$\frac{S}{3} \prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2} \left(1+\frac{3}{p^s}\right)\ ,$$

with

$$S = \frac{1}{2^{3s-2}} \sum_{\mathfrak{c}\mid 2\mathbb{Z}_k} \mathcal{N}(\mathfrak{c})^{s-1} z_k(\mathfrak{c}) \prod_{\mathfrak{p}\mid\mathfrak{c}} \left(1-\frac{1}{\mathcal{N}(\mathfrak{p})^s}\right) T_{\mathfrak{c},2}(s)\ ,$$

where $T_{\mathfrak{c},2}(s) = 1$ unless 2 is totally split in k as $2\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, and either $\mathfrak{c} = \mathbb{Z}_k$, in which case $T_{\mathfrak{c},2}(s) = 1 + 3/2^s$, or $\mathfrak{c} = \mathfrak{p}_i$, in which case $T_{\mathfrak{c},2}(s) = 1 + 1/2^s$. Thus, if 2 is inert we have

$$S = 1/2^{3s-2} + 1 - 1/2^{3s} = 1 + 3/2^{3s}\ ,$$

while if 2 is totally split we have

$$\begin{aligned} S = 1/2^{3s-2}\big(&1 + 3/2^s + 3\cdot 2^{s-1}(1-1/2^s)(1+1/2^s) + 3\cdot 2^{2s-2}(1-1/2^s)^2 \\ &+ 2^{3s-2}(1-1/2^s)^3\big) = 1 + 3/2^{2s} + 6/2^{3s} + 6/2^{4s}\ , \end{aligned}$$

proving the first part of the proposition. The second part follows from Proposition 4.8 and looking at the constant terms, see the more general proof of Proposition 6.2 (2) for details. □

Proposition 5.3 *If* k *is a cyclic cubic field,* $\mathrm{rk}_2(k)$ *is* even *and* $\mathrm{rk}_2^+(k) = \mathrm{rk}_2(k)$.

Proof. Since in the cyclic cubic case $Cl(k)$ and $Cl^+(k)$ are trivially $\mathbb{Z}[\zeta_3]$-modules, it follows that their 2-ranks are even, proving the first statement, and the second follows since $0 \le \mathrm{rk}_2^+(k) - \mathrm{rk}_2(k) \le 1$. □

Definition 5.4 *Given any cubic field* k *(cyclic or not), we let* $\mathcal{L}(k)$ *be the set of isomorphism classes of quartic fields whose resolvent cubic is isomorphic to* k*, with the additional restriction that the quartic is totally real when* k *is such. Furthermore, for any* n *we define* $\mathcal{L}(k,n^2)$ *to be the subset of* $\mathcal{L}(k)$ *of those fields with discriminant equal to* $n^2\operatorname{disc}(k)$.

Recall that if k is totally real the elements of $\mathcal{L}(k)$ are totally real or totally complex, while if k is complex the elements of $\mathcal{L}(k)$ have mixed signature $r_1 = 2$, $r_2 = 1$.

Conjecture 5.5 *Let k be a cyclic cubic field.*

1. *If $\operatorname{rk}_2(k) = 0$ we have $|\mathcal{L}(k,1)| = 0$, if $\operatorname{rk}_2(k) = 2$ we have $|\mathcal{L}(k,1)| = 1$, and more generally we have $|\mathcal{L}(k,1)| = (2^{\operatorname{rk}_2(k)} - 1)/3$.*
2. *If L is an A_4 quartic field with resolvent cubic k and discriminant equal to $\operatorname{disc}(k)$ then L is totally real, hence $L \in \mathcal{L}(k,1)$.*

We also have the following additional conjecture:

Conjecture 5.6 *If $\operatorname{rk}_2(k) = 4$ and 2 is totally split in k, then 2 is totally split in exactly one of the five quartic A_4-extensions with resolvent cubic k, and splits as $2\mathbb{Z}_L = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_i$ of degree 2 in the four others.*

We define Euler factors at 2 as follows:

Definition 5.7 1. *We define*

$$M_{2,1}(s) = \begin{cases} 1 + 3/2^{3s} & \text{if 2 is inert in } k\ , \\ 1 + 3/2^{2s} + 6/2^{3s} + 6/2^{4s} & \text{if 2 is totally split in } k\ . \end{cases}$$

2. *If $L \in \mathcal{L}(k,1)$ we define*

$$M_{2,2,L}(s) = \begin{cases} 1 + 3/2^{3s} & \text{if 2 is inert in } k\ , \\ 1 + 3/2^{2s} + 2\omega_L(2)/2^{3s} + 2\omega_L(2)/2^{4s} & \text{if 2 is totally split in } k\ . \end{cases}$$

The general conjecture in the cyclic cubic case is as follows:

Conjecture 5.8 (Main Conjecture for A_4 Quartics) *We have*

$$\Phi_k(s) = \frac{1}{3} M_{2,1}(s) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p \neq 2} \left(1 + \frac{3}{p^s}\right)$$
$$+ \sum_{L \in \mathcal{L}(k,1)} M_{2,2,L}(s) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p \neq 2} \left(1 + \frac{\omega_L(p)}{p^s}\right)\ .$$

Note that since we are in an Abelian situation, the splitting behavior of primes in k can be read on congruence conditions.

A demontrer par H.C.

See Section 8 below for examples in each possible case.

6 The Quartic S_4 Case

6.1 Contribution of the Trivial Characters

We now study quartic S_4-extensions. The situation is not really that different from the A_4 case, except that the splitting types are more numerous, and of course k is a noncyclic cubic field.

Using the abbreviations introduced above, which we use from now on, we define the following Euler factors at 2:

Definition 6.1 *We set*

$$M_{2,1}(s)=\begin{cases}1+3/2^{3s} & \text{if } 2 \text{ is } \mathrm{IN},\\ 1+1/2^{2s}+4/2^{3s}+2/2^{4s} & \text{if } 2 \text{ is } \mathrm{PS},\\ 1+3/2^{2s}+6/2^{3s}+6/2^{4s} & \text{if } 2 \text{ is } \mathrm{TS},\\ 1+1/2^{s}+2/2^{3s}+4/2^{4s} & \text{if } 2 \text{ is } \mathrm{PR}_0\ ,\\ 1+1/2^{s}+2/2^{2s}+4/2^{4s} & \text{if } 2 \text{ is } \mathrm{PR}_4\ ,\\ 1+1/2^{s}+2/2^{3s} & \text{if } 2 \text{ is } \mathrm{TR},\end{cases}$$

where the notation PR_0 *and* PR_4 *has been introduced in Definition 4.7.*

Proposition 6.2 *1. The contribution of the trivial characters is equal to*

$$\frac{1}{2^{r_2(k)}}M_{2,1}(s)\prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2,\ p\neq 2}\left(1+\frac{1}{p^s}\right)\prod_{p\mathbb{Z}_k=\mathfrak{p}_1^2\mathfrak{p}_2,\ p\neq 2}\left(1+\frac{1}{p^s}\right)\cdot$$
$$\cdot\prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2}\left(1+\frac{3}{p^s}\right)\ .$$

2. In particular, this is equal to $\Phi_k(s)$ if and only if k is totally real and $2\nmid h^+(k)$.

Proof. (1). By Theorem 4.6, the contribution of the trivial characters is equal to

$$\frac{S}{2^{r_2(k)}}\prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2,\ p\neq 2}\left(1+\frac{1}{p^s}\right)\prod_{p\mathbb{Z}_k=\mathfrak{p}_1^2\mathfrak{p}_2,\ p\neq 2}\left(1+\frac{1}{p^s}\right)\prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2}\left(1+\frac{3}{p^s}\right)\ ,$$

where
$$S=\frac{1}{2^{3s-2}}\sum_{\mathfrak{c}\mid 2\mathbb{Z}_k}\mathcal{N}(\mathfrak{c})^{s-1}z_k(\mathfrak{c})\prod_{\mathfrak{p}\mid\mathfrak{c}}\left(1-\frac{1}{\mathcal{N}(\mathfrak{p})^s}\right)T_{\mathfrak{c},2}(s)\ ,$$
for suitable $T_{\mathfrak{c},2}(s)$ detailed below.

We distinguish all the possible splitting types of 2 in k as above.

1. $2\mathbb{Z}_k=\mathfrak{p}_1$, i.e. 2 inert. Here $T_{\mathfrak{c},2}(s)=1$ for all $\mathfrak{c}$, so that
$$S=(1/2^{3s-2})(1+2^{3s-2}(1-1/2^{3s}))=1+3/2^{3s}\ .$$
2. $2\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2$, p_2 of degree 2. Here $T_{\mathfrak{c},2}(s)=1+1/2^s$ if $\mathfrak{c}=\mathbb{Z}_k$ or $\mathfrak{c}=\mathfrak{p}_1$, and $T_{\mathfrak{c},2}(s)=1$ otherwise. Thus,
$$\begin{aligned}S=&(1/2^{3s-2})(1+1/2^s+2^{s-1}(1-1/2^s)(1+1/2^s)+2^{2s-2}(1-1/2^{2s})\\&+2^{3s-2}(1-1/2^s)(1-1/2^{2s}))=1+1/2^{2s}+4/2^{3s}+2/2^{4s}\ .\end{aligned}$$
3. $2\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, i.e., 2 totally split. Here $T_{\mathfrak{c},2}(s)=1+3/2^s$ for $\mathfrak{c}=\mathbb{Z}_k$, $1+1/2^s$ for $\mathfrak{c}=\mathfrak{p}_i$, and 1 otherwise. Thus,
$$\begin{aligned}S=&(1/2^{3s-2})(1+3/2^s+3\cdot 2^{s-1}(1-1/2^s)(1+1/2^s)+3\cdot 2^{2s-2}(1-1/2^s)^2\\&+2^{3s-2}(1-1/2^s)^3)=1+3/2^{2s}+6/2^{3s}+6/2^{4s}\ .\end{aligned}$$
4. $2\mathbb{Z}_k=\mathfrak{p}_1^2\mathfrak{p}_2$ and $\mathrm{disc}(k)\equiv 0\pmod 8$. Here $T_{\mathfrak{c},2}(s)=1+1/2^s$ for $\mathfrak{c}=\mathbb{Z}_k$ and 1 otherwise. Thus,
$$\begin{aligned}S=&(1/2^{3s-2})(1+1/2^s+2\cdot 2^{s-1}(1-1/2^s)+2^{2s-2}(1-1/2^s)\\&+2^{2s-1}(1-1/2^s)^2+2^{3s-2}(1-1/2^s)^2)=1+1/2^s+2/2^{3s}+4/2^{4s}\ .\end{aligned}$$
5. $2\mathbb{Z}_k=\mathfrak{p}_1^2\mathfrak{p}_2$ and $\mathrm{disc}(k)\equiv 4\pmod 8$. Here $T_{\mathfrak{c},2}(s)=1+1/2^s$ for $\mathfrak{c}=\mathbb{Z}_k$ and 1 otherwise. Thus,
$$\begin{aligned}S=&(1/2^{3s-2})(1+1/2^s+2^{s-1}(1-1/2^s)+2^s(1-1/2^s)+2^{2s-2}(1-1/2^s)\\&+2^{2s-1}(1-1/2^s)^2+2^{3s-2}(1-1/2^s)^2)=1+1/2^s+2/2^{2s}+4/2^{4s}\ .\end{aligned}$$
6. $2\mathbb{Z}_k=\mathfrak{p}_1^3$, i.e., 2 totally ramified. Here $T_{\mathfrak{c},2}(s)=1$ for all $\mathfrak{c}$, so that
$$\begin{aligned}S=&(1/2^{3s-2})(1+2^{s-1}(1-1/2^s)+2^{2s-1}(1-1/2^s)\\&+2^{3s-2}(1-1/2^s))=1+1/2^s+2/2^{3s}\ ,\end{aligned}$$
proving (1).

(2) By Proposition 4.8, if k is totally real and $2 \nmid h^+(k)$ there are no nontrivial characters. Conversely, assume that we have equality, and consider the terms in $1/1^s$ of both sides. The term in $1/1^s$ of the formula in (1) is equal to $2^{-r_2(k)}$. On the other hand, the term in $1/1^s$ of $\Phi_k(s)$ is equal to

$$1 + |\{K \in \mathcal{F}(k),\ f(K) = 1\}| = 1 + |\{K_6/k,\ \mathfrak{d}(K_6/k) = \mathbb{Z}_k\}|\ .$$

This shows first that $r_2(k) = 0$, i.e., that k is totally real, and second that k has no quadratic extension unramified outside infinity, which means by class field theory that $2 \nmid h^+(k)$. □

Remark 6.3 *The values $8M_{2,1}(1/2)$ are equal to the constants $c_2(k)$ in Theorem 1.2 of [1]. Since loc. cit. shows clearly that these constants are correct, this is a strong indication that the above formulas are also correct.*

6.2 Properties of Cubic and Quartic Fields

From now on we specifically assume that k is an S_3 cubic field.

We begin by recalling from [2] the notion of the 2-*Selmer group* of a number field:

Definition 6.4 *Let k be a number field.*

1. *We say that an element $\alpha \in k^*$ is a 2-virtual unit if $\alpha\mathbb{Z}_k = \mathfrak{q}^2$ for some ideal $\mathfrak{q}$ of k, or equivalently, if $v_\mathfrak{p}(\alpha) \equiv 0 \pmod{2}$ for all prime ideals $\mathfrak{p}$. We let $V_2(k)$ be the group of virtual units, and $V_2^+(k)$ the subgroup of totally positive ones.*

2. *We define the 2-Selmer group (or simply the Selmer group) $S_2(k)$ of k as $S_2(k) = V_2(k)/k^{*2}$, and $S_2^+(k) = V_2^+(k)/k^{*2}$.*

Note that an element $\alpha \in k^*$ is said to be totally positive when its image by all the *real* embeddings of k is positive.

Proposition 6.5 *We have the following exact sequence of $\mathbb{F}_2$-vector spaces:*

$$1 \longrightarrow U(k)/U(k)^2 \longrightarrow S_2(k) \longrightarrow Cl(k)[2] \longrightarrow 1\ ,$$

so that $S_2(k) \simeq (U(k)/U(k)^2) \oplus Cl(k)[2]$*, and similarly*

$$1 \longrightarrow U^+(k)/U(k)^2 \longrightarrow S_2^+(k) \longrightarrow Cl^+(k)[2] \longrightarrow 1 \ ,$$

so that $S_2^+(k) \simeq (U^+(k)/U(k)^2) \oplus Cl^+(k)[2]$*, where* $U^+(k)$ *is the group of totally positive units and* $Cl^+(k)$ *is the narrow class group.*

Note that if k is a cubic field then for any $\alpha \in k^*$ either α or $-\alpha$ has positive norm. In addition, if k is complex, α totally positive means that $\sigma(\alpha) > 0$ for the unique real embedding σ of k, so equivalently that $\mathcal{N}(\alpha) > 0$, which can be achieved by changing α into $-\alpha$ if necessary. The following corollary immediately follows:

Corollary 6.6 *Let* k *be a cubic field, let* $(\varepsilon_i)_{1\le i\le r^+}$ *be representatives of a basis of* $U^+(k)/U(k)^2$ *(so that* $r^+ \le 2$*), write* $Cl^+(k) = \bigoplus_j (\mathbb{Z}/d_j\mathbb{Z})[\mathfrak{a}_j]$*, let* $(\alpha_j)_{1\le j\le \mathrm{rk}_2^+(k)}$ *be generators of* $\mathfrak{a}_j^{d_j}$ *for all even* d_j*, and let* $(\beta_i)_{1\le i\le \mathrm{rk}_2^+(k)+r^+}$ *be the union of the* ε_i *and the* α_j*. Then the* (β_i) *form a system of representatives of an* $\mathbb{F}_2$*-basis of* $S_2^+(k)$*, so that in particular* $|S_2^+(k)| = 2^{\mathrm{rk}_2^+(k)+r^+}$.

For simply of notation we introduce the following sets:

Definition 6.7 *Recall from 5.4 the definition of the sets* $\mathcal{L}(k,n^2)$*. We define* $\mathcal{L}_{tr}(k,64)$ *to be the set of* $L \in \mathcal{L}(k,64)$ *such that 2 is totally ramified in* L*, and we set*

$$\mathcal{L}_2(k) = \mathcal{L}_{tr}(k,64) \cup \mathcal{L}(k,16) \cup \mathcal{L}(k,4) \cup \mathcal{L}(k,1) \ .$$

Note that this is evidently a disjoint union.

The point of this definition is the following crucial result:

Theorem 6.8 *We have* $L \in \mathcal{L}_2(k)$ *if and only if the corresponding extension of square norm as explained above is of the form* $K_6 = k(\sqrt{\beta})$*, where* β *is a totally positive virtual unit.*

Proof. Assume first that β is a totally positive virtual unit, so that $\beta\mathbb{Z}_k = \mathfrak{q}^2$. By [2], we have $\mathfrak{d}(K_6/k) = 4/\mathfrak{c}^2$, so $\mathcal{N}(\mathfrak{d}(K_6/k)) = \mathrm{disc}(L)/\mathrm{disc}(k) = 64/\mathcal{N}(\mathfrak{c})^2$. Since β is totally positive, when k is totally real so will K_6 and the Galois closure of L, so L is totally real. If $\mathfrak{c} \neq \mathbb{Z}_k$ we have $64/\mathcal{N}(\mathfrak{c})^2 = 1$, 4, or 16, so $L \in \mathcal{L}_2(k)$. Thus assume that $\mathfrak{c} = \mathbb{Z}_k$, so that $\mathrm{disc}(L) = 64\,\mathrm{disc}(k)$

and $\mathfrak{d}(K_6/k) = 4$. This implies that all the primes above 2 in k are ramified in K_6/k, so by Corollary 4.2 the prime 2 is totally ramified in L.

Conversely, let $L \in \mathcal{L}_2(k)$ and $K_6 = k(\sqrt{\alpha})$ for some α of square norm the corresponding extension, and write $\alpha\mathbb{Z}_k = \mathfrak{a}\mathfrak{q}^2$, where $\mathfrak{a}$ is unique if we choose it integral and squarefree. Note that if k is totally real then so is L and hence K_6, so α will automatically be totally positive. Since α has square norm, so does $\mathfrak{a}$. Since $\mathfrak{d}(K_6/k) = 4\mathfrak{a}/\mathfrak{c}^2$ with $\mathfrak{c} \mid 2\mathbb{Z}_k$ coprime to $\mathfrak{a}$ and $\mathcal{N}(\mathfrak{d}(K_6/k)) = \operatorname{disc}(L)/\operatorname{disc}(k) = 2^{2j}$ for $0 \le j \le 3$, it follows that $\mathfrak{a}$ is a product of distinct prime ideals above 2, whose product of norms is a square. If $\mathfrak{a} = \mathbb{Z}_k$ then α is a virtual unit, so there is nothing more to prove, so assume by contradiction that $\mathfrak{a} \ne \mathbb{Z}_k$. Considering the five possible splitting types of 2 in k and using the fact that $\mathcal{N}(\mathfrak{a}) \le \mathcal{N}(\mathfrak{c}^2)$, it is immediate to see that the only remaining possibilities are as follows:

1. $2\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_2$ of degree 2, $\mathfrak{a} = \mathfrak{p}_2$, $\mathfrak{c} = \mathfrak{p}_1$, $\mathfrak{d}(K_6/k) = \mathfrak{p}_2^3$, hence $L \in \mathcal{L}(k, 64)$. Then $\mathfrak{p}_1$ is not ramified in K_6/k so by Corollary 4.2 2 is not totally ramified in L, a contradiction.

2. $2\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2$, $\mathfrak{c} = \mathfrak{p}_3$, $\mathfrak{d}(K_6/k) = (\mathfrak{p}_1\mathfrak{p}_2)^3$, hence $L \in \mathcal{L}(k, 64)$. Similarly, here $\mathfrak{p}_3$ does not ramify in K_6/k, so 2 is not totally ramified in L, again a contradiction and proving the theorem.

□

Corollary 6.9 *1. We have* $|\mathcal{L}_2(k)| = |S_2^+(k)| - 1$.

2. In particular, if k is complex we have $|\mathcal{L}_2(k)| = 2^{\operatorname{rk}_2(k)+1} - 1$.

Proof. For (1), note that the field $k(\sqrt{\beta})$ depends only on the class of β in $S_2^+(k)$, distinct elements of $S_2^+(k)$ give nonisomorphic L, and the unit element must be excluded since it gives a trivial extension. (2) follows since in the complex case the rank r^+ of the group of totally positive units (which here means having its unique real embedding positive, or equivalently of positive norm) modulo squares is equal to 1. □

Corollary 6.10 *Assume that* $2 \nmid h(k)$, *i.e., that* $\operatorname{rk}_2(k) = 0$.

1. If k is a complex cubic field we have $|\mathcal{L}_2(k)| = 1$ *and* $|\mathcal{L}(k, 1)| = 0$.

2. *If k is a totally real cubic field, we have $|\mathcal{L}_2(k)| = 0$ or 1. In addition, the following properties are equivalent:*

   (a) $|\mathcal{L}_2(k)| = 1$.

   (b) *There exists a nonsquare totally positive unit in k.*

   (c) $2 \mid h^+(k)$.

   (d) *There exists a quartic field L having cubic resolvent k with the same discriminant, but which is totally complex (so $L \notin \mathcal{L}(k, 1)$).*

Proof. If k is complex, the first statement is the above corollary, and the second is equivalent to $2 \nmid h(k)$. Thus assume that k is totally real. It is known that if $2 \nmid h(k)$ there cannot exist two independent nonsquare totally positive units (reference?), so $|U^+(k)/U^2(k)| = 1$ or 2. Changing the fundamental units into their opposites if necessary, we may assume that they are of positive norm. If one of the fundamental units is totally positive (signature $(1, 1, 1)$) the other is necessarily of signature $(1, -1, -1)$. If no fundamental unit is totally positive then one of the fundamental units has signature $(1, -1, -1)$, the other has signature $(-1, 1, -1)$ up to permutation of the places, and the product has signature $(-1, -1, 1)$, so in that case $|\mathcal{L}_2(k)| = 0$. The equivalence of the existence of a nonsquare totally positive unit with $2 \mid h(k)$ follows from the definition, as does the last statement. □

From computer experiments, we conjecture the following additional results:

Conjecture 6.11 *If k is a cyclic cubic field then $\mathcal{L}_2(k) = \mathcal{L}(k, 1)$, in other words $\mathcal{L}_{tr}(k, 64) = \mathcal{L}(k, 16) = \mathcal{L}(k, 4) = 0$.*

Proof. This must be easy and classical, and is a special case of Conjecture 6.17 below. □

Proposition 6.12 *Let k be a complex cubic field. If $2 \mid h(k)$ we have $|\mathcal{L}_2(k)| \geq 3$.*

Proof. Follows immediately from Corollary 6.9. □

In addition we have the following partial generalization of Conjectures 5.5 and Corollary 6.10:

Conjecture 6.13 *If k is complex then $|\mathcal{L}(k,1)| = 2^{\mathrm{rk}_2(k)} - 1$. In particular $|\mathcal{L}_{tr}(k,64) \cup \mathcal{L}(k,16) \cup \mathcal{L}(k,4)| = 2^{\mathrm{rk}_2(k)} \geq 1$.*

Note that the second statement follows from the first and Corollary 6.9.

Proposition 6.14 *If k is a cubic field then 2 is totally ramified in k if and only if $\mathrm{disc}(k) \equiv 20 \pmod{32}$, and partially ramified if and only if $\mathrm{disc}(k) \equiv 8$ or $12 \pmod{16}$. In particular we have $v_2(\mathrm{disc}(k)) \leq 3$, and we cannot have $\mathrm{disc}(k) \equiv 4 \pmod{32}$.*

Proof. We have $\mathrm{disc}(k) = Df^2$ for D a fundamental discriminant, and by Proposition 2.5 we cannot have $p^2 \mid f$ or $p \mid \gcd(D, f)$ unless possibly $p = 3$. Thus if f is even we must have $2 \nmid D$ so then $v_2(Df^2) = 2$, while if f is odd we have $v_2(Df^2) = v_2(D) \leq 3$. By Proposition 2.5 the prime 2 is totally ramified if and only if $2 \mid f$, and since $2^2 \nmid f$ we can write $f = 2f_1$ with f_1 odd, so $f^2 = 4f_1^2 \equiv 4 \pmod{32}$. On the other hand, D is an odd fundamental discriminant, so $D \equiv 1 \pmod 4$, so it follows already that $Df^2 \equiv 4 \pmod{16}$. We claim that we cannot have $D \equiv 1 \pmod 8$. This is in fact a result of class field theory: if $D \equiv 1 \pmod 8$ then 2 is split in $K_2 = \mathbb{Q}(\sqrt{D})$ as $2\mathbb{Z}_{K_2} = \mathfrak{p}_1\mathfrak{p}_2$, so $\mathfrak{p}_i \mid f$, which is the conductor of the cyclic cubic extension k^g/K_2, so by Proposition 3.3.18 of [2], since $\mathcal{N}(\mathfrak{p}_i) = 2$ we have $\mathfrak{p}_i^2 \mid f$, in other words $4 \mid f$, a contradiction which proves our claim.

On the other hand, if 2 is partially ramified we have f odd so $f^2 \equiv 1 \pmod 8$, and D even, so $D \equiv 8$ or $12 \pmod{16}$, so $Df^2 \equiv 8$ or $12 \pmod{16}$. ∎

Conjecture 6.15 *Assume that $2 \nmid h(k)$ and that $|\mathcal{L}_2(k)| = 1$. Then:*

1. *If 2 is totally split in k, then $|\mathcal{L}(k,16)| = 1$.*
2. *If 2 is inert in k, then $|\mathcal{L}_{tr}(k,64)| = 1$.*
3. *If 2 is partially split in k then either $|\mathcal{L}_{tr}(k,64)| = 1$ or $|\mathcal{L}(k,16)| = 1$.*
4. *If 2 is totally ramified in k then $\mathrm{disc}(k) \equiv 4 \pmod 8$, and either $|\mathcal{L}_{tr}(k,64)| = 1$ or $|\mathcal{L}(k,4)| = 1$.*
5. *If 2 is partially ramified in k and $\mathrm{disc}(k) \equiv 0 \pmod 8$ then either $|\mathcal{L}_{tr}(k,64)| = 1$ or $|\mathcal{L}(k,4)| = 1$.*

6. *If 2 is partially ramified in k and* $\operatorname{disc}(k) \equiv 4 \pmod 8$ *then either* $|\mathcal{L}_{tr}(k,16)| = 1$ *or* $|\mathcal{L}(k,4)| = 1$.

The above conjecture leads to the following, which we have checked for 100000 fields and is necessary for the consistency of the subsequent results:

Conjecture 6.16 *Without any assumption on $h(k)$ we have the following decomposition types of 2 in k:*

1. *If $\mathcal{L}_{tr}(k,64) \neq \emptyset$ then 2 is either inert, partially split, totally ramified, or partially ramified when* $\operatorname{disc}(k) \equiv 0 \pmod 8$.
2. *If $\mathcal{L}(k,16) \neq \emptyset$ then 2 is either totally split, partially split, or partially ramified when* $\operatorname{disc}(k) \equiv 4 \pmod 8$.
3. *If $\mathcal{L}(k,4) \neq \emptyset$ then 2 is totally or partially ramified.*

In addition, if one of $\mathcal{L}_{tr}(k,64)$, $\mathcal{L}(k,16)$, or $\mathcal{L}(k,4)$ is nonempty then the other two are empty.

It follows from the last part of this conjecture that if k is a cubic field then either $\mathcal{L}_{tr}(k,64) = \mathcal{L}(k,16) = \mathcal{L}(k,4) = \emptyset$ (which is the case if k is cyclic by Conjecture 6.11), or exactly one is nonempty. Although not needed, it is interesting to see how to distinguish a priori between these four types of cubic fields:

Conjecture 6.17 *Let k be a cubic field, and let $(\alpha_i)_{1\le i\le \operatorname{rk}_2^+(k)+r^+}$ be an $\mathbb{F}_2$-basis of $S_2^+(k)$ (see Corollary 6.6).*

1. *We have $\mathcal{L}_{tr}(k,64) = \mathcal{L}(k,16) = \mathcal{L}(k,4) = \emptyset$ if and only if k is totally real and* $\operatorname{rk}_2^+(k) = \operatorname{rk}_2(k)$, *i.e., if and only if there does not exist a nonsquare totally positive unit.*

   From now on, assume that k is complex or that k is totally real and $\operatorname{rk}_2^+(k) > \operatorname{rk}_2(k)$, *so that one and exactly one of $\mathcal{L}_{tr}(k,64)$, $\mathcal{L}(k,16)$, and $\mathcal{L}(k,4)$ is nonempty.*

2. *If 2 is inert in k, then $\mathcal{L}_{tr}(k,64) \neq \emptyset$.*
3. *If 2 is totally split in k then $\mathcal{L}(k,16) \neq \emptyset$.*

4. *If 2 is partially split in k, write $2\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_i$ of degree i. Then if $v_{\mathfrak{p}_1}(\alpha_i - 1) = 1$ for at least one index i we have $\mathcal{L}(k,16) = \emptyset$ and $\mathcal{L}_{tr}(k,64) \neq \emptyset$, otherwise the reverse is true.*

5. *If 2 is totally ramified, write $2\mathbb{Z}_k = \mathfrak{p}^3$. Then if $v_{\mathfrak{p}}(\alpha_i - 1) = 1$ for at least one index i we have $\mathcal{L}(k,4) = \emptyset$ and $\mathcal{L}_{tr}(k,64) \neq \emptyset$, otherwise the reverse is true.*

6. *If 2 is partially ramified and $\operatorname{disc}(k) \equiv 0 \pmod 8$, write $2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$. Then if $v_{\mathfrak{p}_1}(\alpha_i - 1) = 1$ for at least one index i we have $\mathcal{L}(k,4) = \emptyset$ and $\mathcal{L}_{tr}(k,64) \neq \emptyset$, otherwise the reverse is true.*

7. *If 2 is partially ramified and $\operatorname{disc}(k) \equiv 4 \pmod 8$, write $2\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2$. Then if $v_{\mathfrak{p}_1}(\alpha_i - 1) = 1$ for at least one index i we have $\mathcal{L}(k,4) = \emptyset$ and $\mathcal{L}_{tr}(k,16) \neq \emptyset$, otherwise the reverse is true.*

Proof. By Theorem 6.8, we know that $K_6 = k(\sqrt{\alpha})$ for a totally positive virtual unit α, we have $\operatorname{disc}(L)/\operatorname{disc}(k) = \mathcal{N}(\mathfrak{d}(K_6/k))$, and $\mathfrak{d}(K_6/k) = 4/\mathfrak{c}^2$, where $\mathfrak{c}$ is the largest ideal dividing $2\mathbb{Z}_k$ (for divisibility) such that the congruence $x^2 \equiv \alpha \pmod{{}^*\mathfrak{c}^2}$ has a solution. Thus $L \in \mathcal{L}(k,1)$ if and only if $\mathfrak{c} = 2\mathbb{Z}_k$.

(2). If 2 is inert, then $\mathfrak{c} = \mathbb{Z}_k$ or $2\mathbb{Z}_k$, and since we assume $L \notin \mathcal{L}(k,1)$ we have $\mathfrak{c} \neq 2\mathbb{Z}_k$, so $\mathfrak{c} = \mathbb{Z}_k$ and $\mathcal{N}(\mathfrak{d}(K_6/k)) = 64$, i.e., $L \in \mathcal{L}(k,64)$, hence $L \in \mathcal{L}_{tr}(k,64)$ by what we have seen in Theorem 6.8.

(3). If $2\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ is totally split, then again since we assume $L \notin \mathcal{L}(k,1)$, up to permutation of the $\mathfrak{p}_i$ we have either $\mathfrak{c} = \mathbb{Z}_k$, $\mathfrak{c} = \mathfrak{p}_1$, or $\mathfrak{c} = \mathfrak{p}_1\mathfrak{p}_2$.

To be done. ◻

6.3 The General Conjecture

We are thus led to set the following definition:

Definition 6.18 *1. We define $M_{2,1}(s)$ as in Definition 6.1.*

2. *Let $L \in \mathcal{L}_{tr}(k,64)$. We set*

$$M_{2,2,L}(s) = \begin{cases} 1 - 1/2^{3s} & \text{if } 2 \text{ is IN in } k\ , \\ 1 - 1/2^{2s} & \text{if } 2 \text{ is PS in } k\ , \\ 1 - 1/2^{s} & \text{if } 2 \text{ is } \mathrm{PR}_0 \text{ or } \mathrm{TR}_4 \text{ in } k\ . \end{cases}$$

3. Let $L \in \mathcal{L}(k,16)$. We set

$$M_{2,2,L}(s) = \begin{cases} 1 + 1/2^{2s} - 4/2^{3s} + 2/2^{4s} & \text{if } 2 \text{ is PS in } k \text{ and } \mathrm{PR}_2 \text{ in } L\ , \\ 1 + 1/2^{2s} - 2/2^{4s} & \text{if } 2 \text{ is PS in } k \text{ and } \mathrm{PR}_{2,2} \text{ in } L\ , \\ 1 - 1/2^{2s} - 2/2^{3s} + 2/2^{4s} & \text{if } 2 \text{ is TS in } k \text{ and } \mathrm{PR}_2 \text{ in } L\ , \\ 1 - 1/2^{2s} + 2/2^{3s} - 2/2^{4s} & \text{if } 2 \text{ is TS in } k \text{ and } \mathrm{PR}_{2,2} \text{ in } L\ , \\ 1 - 1/2^{s} & \text{if } 2 \text{ is PR in } k\ . \end{cases}$$

4. Let $L \in \mathcal{L}(k,4)$. We set

$$M_{2,2,L}(s) = \begin{cases} 1 + 1/2^{s} - 2/2^{3s} & \text{if } 2 \text{ is } \mathrm{PR}_0 \text{ or } \mathrm{TR}_4 \text{ in } k\ , \\ 1 + 1/2^{s} - 2/2^{2s} & \text{if } 2 \text{ is } \mathrm{PR}_4 \text{ in } k\ . \end{cases}$$

5. Let $L \in \mathcal{L}(k,1)$. We set

$$M_{2,2,L}(s) = \begin{cases} 1 + 3/2^{3s} & \text{if } 2 \text{ is IN in } k\ , \\ 1 + 1/2^{2s} - 2/2^{4s} & \text{if } 2 \text{ is PS in } k \text{ and IN in } L\ , \\ 1 + 4/2^{3s} + 2/2^{4s} & \text{if } 2 \text{ is PS in } k \text{ and } \mathrm{PS}_{2,1,1} \text{ in } L\ , \\ 1 + 3/2^{2s} + 6/2^{3s} + 6/2^{4s} & \text{if } 2 \text{ is TS in } k \text{ and TS in } L\ , \\ 1 + 3/2^{2s} - 2/2^{3s} - 2/2^{4s} & \text{if } 2 \text{ is TS in } k \text{ and } \mathrm{PS}_{2,2} \text{ in } L\ , \\ 1 + 1/2^{s} + 2/2^{3s} & \text{if } 2 \text{ is TR in } k\ , \\ 1 + 1/2^{s} + 2/2^{3s} - 4/2^{4s} & \text{if } 2 \text{ is } \mathrm{PR}_0 \text{ in } k \text{ and } \mathrm{PR}_{2,1} \text{ in } L\ , \\ 1 + 1/2^{s} + 2/2^{3s} + 4/2^{4s} & \text{if } 2 \text{ is } \mathrm{PR}_0 \text{ in } k \text{ and } \mathrm{PR}_{2,1,1} \text{ in } L\ , \\ 1 + 1/2^{s} + 2/2^{2s} - 4/2^{4s} & \text{if } 2 \text{ is } \mathrm{PR}_4 \text{ in } k \text{ and } \mathrm{PR}_{2,1} \text{ in } L\ , \\ 1 + 1/2^{s} + 2/2^{2s} + 4/2^{4s} & \text{if } 2 \text{ is } \mathrm{PR}_4 \text{ in } k \text{ and } \mathrm{PR}_{2,1,1} \text{ in } L\ . \end{cases}$$

The general conjecture is as follows:

Conjecture 6.19 (Main Conjecture for S_4 Quartics) *We have*

$$2^{r_2(k)}\Phi_k(s) = M_{2,1}(s) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2,\ p\neq 2} \left(1 + \frac{1}{p^s}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1^2\mathfrak{p}_2,\ p\neq 2} \left(1 + \frac{1}{p^s}\right) \cdot$$
$$\cdot \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2} \left(1 + \frac{3}{p^s}\right)$$
$$+ \sum_{L \in \mathcal{L}_2(k)} M_{2,2,L}(s) \prod_{p \neq 2} \left(1 + \frac{\omega_L(p)}{p^s}\right)\ .$$

Remarks 6.20 *1. When $2 \nmid h(k)$ the constant terms (i.e., in $1/1^s$) of the two sides agree: if k is totally real and $|\mathcal{L}_2(k)| = 0$ then $\mathcal{L}_2(k) = \mathcal{L}(k,1) = \emptyset$, so by definition the constant term of the LHS is equal to 1, also equal to that of the RHS. If $|\mathcal{L}_2(k)| = |\mathcal{L}(k,1)| = 1$, the constant term of the LHS is equal to 2, also equal to that of the RHS. If k is complex, by Corollary 6.10 we have $|\mathcal{L}(k,1)| = 0$ and $|\mathcal{L}_2(k)| = 1$, so the constant term of the LHS is equal to 2, equal to that of the RHS.*

2. If we assume Conjecture 6.11, this conjecture is an exact generalization of Conjecture 5.8 given for cyclic cubic fields.

3. The above conjecture is true for the first 10000 totally real and the first 10000 complex cubic fields.

See Section 9 below for examples in each possible case.

PART III: EXAMPLES

7 Examples for the Cubic Case

7.1 $D \in \mathcal{D}^-$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (0,0)$

In this case, there are no cubic fields of discriminant D^* or $-27D$.

$$\Phi_1(s) = \frac{1}{2}\left(1 + \frac{2}{3^{2s}}\right) \prod_{\left(\frac{-3}{p}\right)=1} \left(1 + \frac{2}{p^s}\right) ,$$

$$\Phi_{-4}(s) = \frac{1}{2}\left(1 + \frac{2}{3^{2s}}\right) \prod_{\left(\frac{12}{p}\right)=1} \left(1 + \frac{2}{p^s}\right) ,$$

$$\Phi_{-15}(s) = \frac{1}{2}\left(1 + \frac{2}{3^{s}}\right) \prod_{\left(\frac{45}{p}\right)=1} \left(1 + \frac{2}{p^s}\right) ,$$

$$\Phi_{-39}(s) = \frac{1}{2}\left(1 + \frac{2}{3^{s}} + \frac{6}{3^{2s}}\right) \prod_{\left(\frac{117}{p}\right)=1} \left(1 + \frac{2}{p^s}\right) .$$

7.2 $D \in \mathcal{D}^-$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (1, 0)$.

In this case there are no cubic fields of discriminant D^* and a unique cubic field of discriminant $-27D$.

$$\Phi_{-23}(s) = \frac{1}{2}\left(1+\frac{2}{3^{2s}}\right)\prod_{\left(\frac{69}{p}\right)=1}\left(1+\frac{2}{p^s}\right)$$
$$+\left(1-\frac{1}{3^{2s}}\right)\prod_p\left(1+\frac{\omega_{L621}(p)}{p^s}\right),$$
$$\Phi_{-87}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}\right)\prod_{\left(\frac{261}{p}\right)=1}\left(1+\frac{2}{p^s}\right)$$
$$+\left(1-\frac{1}{3^{s}}\right)\prod_p\left(1+\frac{\omega_{L2349}(p)}{p^s}\right),$$
$$\Phi_{-255}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right)\prod_{\left(\frac{6885}{p}\right)=1}\left(1+\frac{2}{p^s}\right)$$
$$+\left(1-\frac{1}{3^{s}}\right)\prod_p\left(1+\frac{\omega_{L6885}(p)}{p^s}\right),$$

where the indicated cubic fields are given as follows:

Cubic field	Discriminant	Defining polynomial
$L621$	$3^3 \cdot 23$	$x^3 - 6x - 3$
$L2349$	$3^3 \cdot 87$	$x^3 - 12x - 13$
$L6885$	$3^3 \cdot 255$	$x^3 - 12x - 1$

7.3 $D \in \mathcal{D}^-$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (1, 1)$.

In this case there is a unique cubic field of discriminant D^* and no cubic fields of discriminant $-27D$.

$$
\begin{aligned}
\Phi_{-107}(s) &= \frac{1}{2}\left(1+\frac{2}{3^{2s}}\right) \prod_{\left(\frac{321}{p}\right)=1} \left(1+\frac{2}{p^s}\right) \\
&\quad + \left(1+\frac{2}{3^{2s}}\right) \prod_{p} \left(1+\frac{\omega_{L321}(p)}{p^s}\right) , \\
\Phi_{-771}(s) &= \frac{1}{2}\left(1+\frac{2}{3^{s}}\right) \prod_{\left(\frac{2313}{p}\right)=1} \left(1+\frac{2}{p^s}\right) \\
&\quad + \left(1+\frac{2}{3^{s}}\right) \prod_{p\neq 3} \left(1+\frac{\omega_{L257}(p)}{p^s}\right) , \\
\Phi_{-687}(s) &= \frac{1}{2}\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right) \prod_{\left(\frac{2061}{p}\right)=1} \left(1+\frac{2}{p^s}\right) \\
&\quad + \left(1+\frac{2}{3^{s}}-\frac{3}{3^{2s}}\right) \prod_{p\neq 3} \left(1+\frac{\omega_{L229}(p)}{p^s}\right) , \\
\Phi_{-3387}(s) &= \frac{1}{2}\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right) \prod_{\left(\frac{10161}{p}\right)=1} \left(1+\frac{2}{p^s}\right) \\
&\quad + \left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right) \prod_{p\neq 3} \left(1+\frac{\omega_{L1129}(p)}{p^s}\right) ,
\end{aligned}
$$

where the indicated cubic fields are given as follows:

Cubic field	Discriminant	Defining polynomial
$L321$	$3 \cdot 107$	$x^3 - x^2 - 4x + 1$
$L257$	$771/3$	$x^3 - x^2 - 4x + 3$
$L229$	$687/3$	$x^3 - 4x - 1$
$L1129$	$3387/3$	$x^3 - 7x - 3$

7.4 $D \in \mathcal{D}^-$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (2, 1)$.

In this case there is a unique cubic field of discriminant D^* and three cubic fields of discriminant $-27D$.

$$\Phi_{-3299}(s) = \frac{1}{2}\left(1+\frac{2}{3^{2s}}\right)\prod_{\left(\frac{9897}{p}\right)=1}\left(1+\frac{2}{p^s}\right)$$
$$+\left(1+\frac{2}{3^{2s}}\right)\prod_{p}\left(1+\frac{\omega_{L9897}(p)}{p^s}\right)$$
$$+\left(1-\frac{1}{3^{2s}}\right)\sum_{1\le i\le 3}\prod_{p}\left(1+\frac{\omega_{L89073_i}(p)}{p^s}\right)\ ,$$
$$\Phi_{-5703}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}\right)\prod_{\left(\frac{17109}{p}\right)=1}\left(1+\frac{2}{p^s}\right)$$
$$+\left(1+\frac{2}{3^{s}}\right)\prod_{p\neq 3}\left(1+\frac{\omega_{L1901}(p)}{p^s}\right)$$
$$+\left(1-\frac{1}{3^{s}}\right)\sum_{1\le i\le 3}\prod_{p}\left(1+\frac{\omega_{L153981_i}(p)}{p^s}\right)\ ,$$
$$\Phi_{-8751}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right)\prod_{\left(\frac{26253}{p}\right)=1}\left(1+\frac{2}{p^s}\right)$$
$$+\left(1+\frac{2}{3^{s}}-\frac{3}{3^{2s}}\right)\prod_{p\neq 3}\left(1+\frac{\omega_{L2917}(p)}{p^s}\right)$$
$$+\left(1-\frac{1}{3^{s}}\right)\sum_{1\le i\le 3}\prod_{p}\left(1+\frac{\omega_{L236277_i}(p)}{p^s}\right)\ ,$$
$$\Phi_{-42591}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right)\prod_{\left(\frac{127773}{p}\right)=1}\left(1+\frac{2}{p^s}\right)$$
$$+\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right)\prod_{p\neq 3}\left(1+\frac{\omega_{L14197}(p)}{p^s}\right)$$
$$+\left(1-\frac{1}{3^{s}}\right)\sum_{1\le i\le 3}\prod_{p}\left(1+\frac{\omega_{L1149957_i}(p)}{p^s}\right)\ ,$$

where the indicated cubic fields are given as follows:

Cubic field	Discriminant	Defining polynomial
$L9897$	$3 \cdot 3299$	$x^3 - x^2 - 28x + 1$
$L89073_1$	$3^3 \cdot 3299$	$x^3 - 69x - 213$
$L89073_2$	$3^3 \cdot 3299$	$x^3 - 45x - 101$
$L89073_3$	$3^3 \cdot 3299$	$x^3 - 81x - 256$
$L1901$	$5703/3$	$x^3 - x^2 - 9x - 4$
$L153981_1$	$3^3 \cdot 5703$	$x^3 - 72x - 63$
$L153981_2$	$3^3 \cdot 5703$	$x^3 - 102x + 121$
$L153981_3$	$3^3 \cdot 5703$	$x^3 - 57x - 68$
$L2917$	$8751/3$	$x^3 - x^2 - 13x + 20$
$L236277_1$	$3^3 \cdot 8751$	$x^3 - 138x + 413$
$L236277_2$	$3^3 \cdot 8751$	$x^3 - 129x - 532$
$L236277_3$	$3^3 \cdot 8751$	$x^3 - 90x - 171$
$L14197$	$42591/3$	$x^3 - 16x - 9$
$L1149957_1$	$3^3 \cdot 42591$	$x^3 - 66x - 1$
$L1149957_2$	$3^3 \cdot 42591$	$x^3 - 156x - 721$
$L1149957_3$	$3^3 \cdot 42591$	$x^3 - 210x - 1153$

7.5 $D \in \mathcal{D}^-$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (2, 2)$.

In this case there are four cubic fields of discriminant D^* and none of discriminant $-27D$. Also recall from Proposition 2.4 above that if $D \equiv 6 \pmod 9$, 3 is totally split in one of them and inert in the other three, so one of the cubic fields of discriminant D^*, which we include first, is distinguished by the fact that 3 is totally split.

$$\Phi_{-34603}(s) = \frac{1}{2}\left(1+\frac{2}{3^{2s}}\right) \prod_{\left(\frac{103809}{p}\right)=1} \left(1+\frac{2}{p^s}\right)$$

$$+\left(1+\frac{2}{3^{2s}}\right) \sum_{1\leq i\leq 4} \prod_{p} \left(1+\frac{\omega_{L103809_i}(p)}{p^s}\right) ,$$

$$\Phi_{-96027}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}\right) \prod_{\left(\frac{288081}{p}\right)=1} \left(1+\frac{2}{p^s}\right)$$

$$+\left(1+\frac{2}{3^{s}}\right) \sum_{1\leq i\leq 4} \prod_{p\neq 3} \left(1+\frac{\omega_{L32009_i}(p)}{p^s}\right) ,$$

$$\Phi_{-128451}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right) \prod_{\left(\frac{385353}{p}\right)=1} \left(1+\frac{2}{p^s}\right)$$

$$+\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right) \prod_{p\neq 3} \left(1+\frac{\omega_{L42817_1}(p)}{p^s}\right)$$

$$+\left(1+\frac{2}{3^{s}}-\frac{3}{3^{2s}}\right) \sum_{2\leq i\leq 4} \prod_{p\neq 3} \left(1+\frac{\omega_{L42817_i}(p)}{p^s}\right) ,$$

where the indicated cubic fields are given as follows:

Cubic field	Discriminant	Defining polynomial
$L103809_1$	$3 \cdot 34603$	$x^3 - x^2 - 84x + 261$
$L103809_2$	$3 \cdot 34603$	$x^3 - x^2 - 64x + 91$
$L103809_3$	$3 \cdot 34603$	$x^3 - x^2 - 92x - 204$
$L103809_4$	$3 \cdot 34603$	$x^3 - x^2 - 62x - 15$
$L32009_1$	$96027/3$	$x^3 - 41x - 95$
$L32009_2$	$96027/3$	$x^3 - x^2 - 52x + 159$
$L32009_3$	$96027/3$	$x^3 - x^2 - 34x - 24$
$L32009_4$	$96027/3$	$x^3 - x^2 - 20x - 1$
$L42817_1$	$128451/3$	$x^3 - 25x - 27$
$L42817_2$	$128451/3$	$x^3 - 61x - 179$
$L42817_3$	$128451/3$	$x^3 - x^2 - 34x - 55$
$L42817_4$	$128451/3$	$x^3 - x^2 - 38x - 32$

7.6 $D \in \mathcal{D}^+$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (0, 0)$.

In this case there are no cubic fields of discriminant D^* and a unique cubic field of discriminant $-27D$.

$$
\begin{aligned}
3\Phi_{-3}(s) &= \frac{1}{2}\left(1+\frac{2}{3^s}+\frac{6}{3^{2s}}\right)\prod_{p\neq 3}\left(1+\frac{2}{p^s}\right) \\
&\quad + \left(1-\frac{1}{3^s}\right)\prod_{p\equiv\pm1 \pmod 9}\left(1+\frac{2}{p^s}\right)\prod_{p\equiv\pm2,\pm4 \pmod 9}\left(1-\frac{1}{p^s}\right)\ , \\
3\Phi_{5}(s) &= \frac{1}{2}\left(1+\frac{2}{3^{2s}}\right)\prod_{\left(\frac{-15}{p}\right)=1}\left(1+\frac{2}{p^s}\right) \\
&\quad + \left(1-\frac{1}{3^{2s}}\right)\prod_{p}\left(1+\frac{\omega_{LM135}(p)}{p^s}\right)\ , \\
3\Phi_{12}(s) &= \frac{1}{2}\left(1+\frac{2}{3^{s}}\right)\prod_{\left(\frac{-36}{p}\right)=1}\left(1+\frac{2}{p^s}\right) \\
&\quad + \left(1-\frac{1}{3^{s}}\right)\prod_{p}\left(1+\frac{\omega_{LM324}(p)}{p^s}\right)\ , \\
3\Phi_{24}(s) &= \frac{1}{2}\left(1+\frac{2}{3^s}+\frac{6}{3^{2s}}\right)\prod_{\left(\frac{-72}{p}\right)=1}\left(1+\frac{2}{p^s}\right) \\
&\quad + \left(1-\frac{1}{3^{s}}\right)\prod_{p}\left(1+\frac{\omega_{LM648}(p)}{p^s}\right)\ ,
\end{aligned}
$$

where the indicated cubic fields are given as follows:

Cubic field	Discriminant	Defining polynomial
$LM135$	$-3^3 \cdot 5$	x^3+3x-1
$LM324$	$-3^3 \cdot 12$	x^3-3x-4
$LM648$	$-3^3 \cdot 24$	$x^3-3x-10$

7.7 $D \in \mathcal{D}^+$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (0,1)$.

In this case there is a unique cubic field of discriminant D^* and no cubic field of discriminant $-27D$.

$$3\Phi_{29}(s) = \frac{1}{2}\left(1+\frac{2}{3^{2s}}\right)\prod_{\left(\frac{-87}{p}\right)=1}\left(1+\frac{2}{p^s}\right)$$

$$+\left(1+\frac{2}{3^{2s}}\right)\prod_{p}\left(1+\frac{\omega_{LM87}(p)}{p^s}\right)\ ,$$

$$3\Phi_{93}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}\right)\prod_{\left(\frac{-279}{p}\right)=1}\left(1+\frac{2}{p^s}\right)$$

$$+\left(1+\frac{2}{3^{s}}\right)\prod_{p\neq 3}\left(1+\frac{\omega_{LM31}(p)}{p^s}\right)\ ,$$

$$3\Phi_{69}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right)\prod_{\left(\frac{-207}{p}\right)=1}\left(1+\frac{2}{p^s}\right)$$

$$+\left(1+\frac{2}{3^{s}}-\frac{3}{3^{2s}}\right)\prod_{p\neq 3}\left(1+\frac{\omega_{LM23}(p)}{p^s}\right)\ ,$$

$$3\Phi_{717}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right)\prod_{\left(\frac{-2151}{p}\right)=1}\left(1+\frac{2}{p^s}\right)$$

$$+\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right)\prod_{p\neq 3}\left(1+\frac{\omega_{LM239}(p)}{p^s}\right)\ ,$$

where the indicated cubic fields are given as follows:

Cubic field	Discriminant	Defining polynomial
$LM87$	$-3\cdot 29$	x^3-x^2+2x+1
$LM31$	$-93/3$	x^3+x-1
$LM23$	$-69/3$	x^3-x^2+1
$LM239$	$-717/3$	x^3-x-3

7.8 $D\in\mathcal{D}^+$ and $(\mathrm{rk}_3(D),\mathrm{rk}_3(D^*))=(1,1)$.

In this case there is a unique cubic field of discriminant D^* and three cubic fields of discriminant $-27D$.

$$
\begin{aligned}
3\Phi_{229}(s) = \frac{1}{2}\left(1+\frac{2}{3^{2s}}\right) &\prod_{\left(\frac{-687}{p}\right)=1}\left(1+\frac{2}{p^s}\right) \\
&+\left(1+\frac{2}{3^{2s}}\right)\prod_{p}\left(1+\frac{\omega_{LM687}(p)}{p^s}\right) \\
&+\left(1-\frac{1}{3^{2s}}\right)\sum_{1\le i\le 3}\prod_{p}\left(1+\frac{\omega_{LM6183_i}}{p^s}\right)\ , \\
3\Phi_{993}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}\right) &\prod_{\left(\frac{-2979}{p}\right)=1}\left(1+\frac{2}{p^s}\right) \\
&+\left(1+\frac{2}{3^{s}}\right)\prod_{p\neq 3}\left(1+\frac{\omega_{LM331}(p)}{p^s}\right) \\
&+\left(1-\frac{1}{3^{s}}\right)\sum_{1\le i\le 3}\prod_{p}\left(1+\frac{\omega_{LM26811_i}}{p^s}\right)\ , \\
3\Phi_{321}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right) &\prod_{\left(\frac{-963}{p}\right)=1}\left(1+\frac{2}{p^s}\right) \\
&+\left(1+\frac{2}{3^{s}}-\frac{3}{3^{2s}}\right)\prod_{p\neq 3}\left(1+\frac{\omega_{LM107}(p)}{p^s}\right) \\
&+\left(1-\frac{1}{3^{s}}\right)\sum_{1\le i\le 3}\prod_{p}\left(1+\frac{\omega_{LM8667_i}}{p^s}\right)\ , \\
3\Phi_{5073}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right) &\prod_{\left(\frac{-15219}{p}\right)=1}\left(1+\frac{2}{p^s}\right) \\
&+\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right)\prod_{p\neq 3}\left(1+\frac{\omega_{LM1691}(p)}{p^s}\right) \\
&+\left(1-\frac{1}{3^{s}}\right)\sum_{1\le i\le 3}\prod_{p}\left(1+\frac{\omega_{LM136971_i}}{p^s}\right)\ ,
\end{aligned}
$$

where the indicated cubic fields are given as follows:

Cubic field	Discriminant	Defining polynomial
$LM687$	$-3 \cdot 229$	$x^3 - x^2 + 4x + 3$
$LM6183_1$	$-3^3 \cdot 229$	$x^3 - 9x - 32$
$LM6183_2$	$-3^3 \cdot 229$	$x^3 + 3x - 15$
$LM6183_3$	$-3^3 \cdot 229$	$x^3 + 9x - 11$
$LM331$	$-993/3$	$x^3 - x^2 + 3x - 4$
$LM26811_1$	$-3^3 \cdot 993$	$x^3 + 6x - 31$
$LM26811_2$	$-3^3 \cdot 993$	$x^3 + 36x - 45$
$LM26811_3$	$-3^3 \cdot 993$	$x^3 - 18x - 99$
$LM107$	$-321/3$	$x^3 - x^2 + 3x - 2$
$LM8667_1$	$-3^3 \cdot 321$	$x^3 + 18x - 45$
$LM8667_2$	$-3^3 \cdot 321$	$x^3 + 6x - 17$
$LM8667_3$	$-3^3 \cdot 321$	$x^3 + 15x - 28$
$LM1691$	$-5073/3$	$x^3 - x^2 + x - 24$
$LM136971_1$	$-3^3 \cdot 5073$	$x^3 + 6x - 71$
$LM136971_2$	$-3^3 \cdot 5073$	$x^3 + 24x - 55$
$LM136971_3$	$-3^3 \cdot 5073$	$x^3 - 12x - 73$

7.9 $D \in \mathcal{D}^+$ and $(\mathrm{rk}_3(D), \mathrm{rk}_3(D^*)) = (1, 2)$.

In this case there is are four cubic fields of discriminant D^* and no cubic fields of discriminant $-27D$. However one of the cubic fields of discriminant D^*, which we include first, is distinguished by the fact that 3 is totally split.

$$3\Phi_{1901}(s) = \frac{1}{2}\left(1+\frac{2}{3^{2s}}\right) \prod_{\left(\frac{-5703}{p}\right)=1} \left(1+\frac{2}{p^s}\right) + \left(1+\frac{2}{3^{2s}}\right) \sum_{1\le i\le 4} \prod_{p} \left(1+\frac{\omega_{LM5703_i}}{p^s}\right) ,$$

$$3\Phi_{12081}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}\right) \prod_{\left(\frac{-36243}{p}\right)=1} \left(1+\frac{2}{p^s}\right) + \left(1+\frac{2}{3^{s}}\right) \sum_{1\le i\le 4} \prod_{p\neq 3} \left(1+\frac{\omega_{LM4027_i}}{p^s}\right) ,$$

$$3\Phi_{9897}(s) = \frac{1}{2}\left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right) \prod_{\left(\frac{-29691}{p}\right)=1} \left(1+\frac{2}{p^s}\right) + \left(1+\frac{2}{3^{s}}+\frac{6}{3^{2s}}\right) \prod_{p\neq 3} \left(1+\frac{\omega_{LM3299_1}(p)}{p^s}\right) + \left(1+\frac{2}{3^{s}}-\frac{3}{3^{2s}}\right) \sum_{2\le i\le 4} \prod_{p\neq 3} \left(1+\frac{\omega_{LM3299_i}}{p^s}\right) ,$$

where the indicated cubic fields are given as follows:

Cubic field	Discriminant	Defining polynomial
$LM5703_1$	$-3\cdot 1901$	$x^3-x^2+2x+43$
$LM5703_2$	$-3\cdot 1901$	$x^3-x^2+18x+27$
$LM5703_3$	$-3\cdot 1901$	$x^3+21x-23$
$LM5703_4$	$-3\cdot 1901$	$x^3-x^2-18x+48$
$LM4027_1$	$-12081/3$	$x^3-8x-15$
$LM4027_2$	$-12081/3$	x^3-x^2+7x+8
$LM4027_3$	$-12081/3$	$x^3-x^2-7x-12$
$LM4027_4$	$-12081/3$	$x^3+10x-1$
$LM3299_1$	$-9897/3$	$x^3-16x-27$
$LM3299_2$	$-9897/3$	x^3-x^2+9x-8
$LM3299_3$	$-9897/3$	$x^3+2x-11$
$LM3299_4$	$-9897/3$	$x^3-x^2+3x+10$

8 Examples for the Quartic A_4 Case

$\mathrm{rk}_2(k) = 0$ **and** 2 **inert in** k**:**
k cyclic cubic of discriminant $49 = 7^2$, defined by $x^3 - x^2 - 2x + 1 = 0$.

$$\Phi_k(s) = \frac{1}{3}\left(1 + \frac{3}{2^{3s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{3}{p^s}\right) = \frac{1}{3}\left(1 + \frac{3}{2^{3s}}\right) \prod_{p \equiv \pm 1 \pmod 7} \left(1 + \frac{3}{p^s}\right) .$$

As mentioned above, the second equality comes from the fact that we are in an Abelian situation, so such equalities also exist in all the subsequent formulas, but it is not necessary to give them explicitly.

$\mathrm{rk}_2(k) = 0$ **and** 2 **totally split in** k**:**
k cyclic cubic of discriminant $961 = 31^2$, defined by $x^3 - x^2 - 10x + 8 = 0$.

$$\Phi_k(s) = \frac{1}{3}\left(1 + \frac{3}{2^{2s}} + \frac{6}{2^{3s}} + \frac{6}{2^{4s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p \neq 2} \left(1 + \frac{3}{p^s}\right) .$$

$\mathrm{rk}_2(k) = 2$ **and** 2 **inert in** k**:**
k cyclic cubic of discriminant $26569 = 163^2$, defined by $x^3 - x^2 - 54x + 169 = 0$.

$$\Phi_k(s) = \frac{1}{3}\left(1 + \frac{3}{2^{3s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{3}{p^s}\right) + \left(1 + \frac{3}{2^{3s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{\omega_L(p)}{p^s}\right) ,$$

where L is the unique quartic A_4 field with cubic resolvent k, defined by $x^4 - x^3 - 7x^2 + 2x + 9 = 0$.

$\mathrm{rk}_2(k) = 2$ **and** 2 **totally split in** k**. Case 1:** $2\mathbb{Z}_L = \mathfrak{p}_1\mathfrak{p}_2$
k cyclic cubic of discriminant $76729 = 277^2$, defined by $x^3 - x^2 - 92x - 236 = 0$.

$$\Phi_k(s) = \frac{1}{3}\left(1 + \frac{3}{2^{2s}} + \frac{6}{2^{3s}} + \frac{6}{2^{4s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p \neq 2} \left(1 + \frac{3}{p^s}\right) + \left(1 + \frac{3}{2^{2s}} - \frac{2}{2^{3s}} - \frac{2}{2^{4s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p \neq 2} \left(1 + \frac{\omega_L(p)}{p^s}\right) ,$$

where L is the unique quartic A_4 field with cubic resolvent k, defined by $x^4 - x^3 - 11x^2 + 4x + 12 = 0$.

$\mathrm{rk}_2(k) = 2$ **and** 2 **totally split in** k**. Case 2:** 2 **totally split in** L

k cyclic cubic of discriminant $36954241 = 6079^2$, defined by $x^3 - x^2 - 2026x + 1576 = 0$.

$$\Phi_k(s) = \frac{1}{3}\left(1 + \frac{3}{2^{2s}} + \frac{6}{2^{3s}} + \frac{6}{2^{4s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2} \left(1 + \frac{3}{p^s}\right)$$
$$+ \left(1 + \frac{3}{2^{2s}} + \frac{6}{2^{3s}} + \frac{6}{2^{4s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2} \left(1 + \frac{\omega_L(p)}{p^s}\right) \ ,$$

where L is the unique quartic A_4 field with cubic resolvent k, defined by $x^4 - 2x^3 - 81x^2 - 38x + 992 = 0$.

$\mathrm{rk}_2(k) = 4$ **and** 2 **inert in** k**:**

k cyclic cubic of discriminant $59089969 = 7687^2$, defined by $x^3 - x^2 - 2562x + 48969 = 0$.

$$\Phi_k(s) = \frac{1}{3}\left(1 + \frac{3}{2^{3s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2} \left(1 + \frac{3}{p^s}\right)$$
$$+ \left(1 + \frac{3}{2^{3s}}\right) \sum_{1\le i\le 5} \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2} \left(1 + \frac{\omega_{L_i}(p)}{p^s}\right) \ ,$$

where the L_i are the five quartic A_4 field with cubic resolvent k, defined by the respective equations $x^4 - x^3 - 79x^2 + 286x + 49 = 0$, $x^4 - x^3 - 64x^2 - 99x + 324 = 0$, $x^4 - 2x^3 - 61x^2 - 55x + 358 = 0$, $x^4 - x^3 - 52x^2 + 61x + 400 = 0$, and $x^4 - 2x^3 - 49x^2 + 47x + 417 = 0$.

$\mathrm{rk}_2(k) = 4$ **and** 2 **totally split in** k**:**

k cyclic cubic of discriminant $1019077929 = 31923^2$, defined by $x^3 - 10641x - 227008 = 0$.

$$\Phi_k(s) = \frac{1}{3}\left(1+\frac{3}{2^{2s}}+\frac{6}{2^{3s}}+\frac{6}{2^{4s}}\right)\prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2}\left(1+\frac{3}{p^s}\right)$$
$$+\left(1+\frac{3}{2^{2s}}+\frac{6}{2^{3s}}+\frac{6}{2^{4s}}\right)\prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2}\left(1+\frac{\omega_{L_1}(p)}{p^s}\right)$$
$$+\left(1+\frac{3}{2^{2s}}-\frac{2}{2^{3s}}-\frac{2}{2^{4s}}\right)\sum_{2\le i\le 5}\prod_{p\mathbb{Z}_k=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3,\ p\neq 2}\left(1+\frac{\omega_{L_i}(p)}{p^s}\right)\ ,$$

where the L_i are the five quartic A_4 field with cubic resolvent k, defined by the respective equations $x^4-2x^3-279x^2-1276x+2132$, $x^4-2x^3-207x^2-108x+4464$, $x^4-2x^3-201x^2+154x+4537$, $x^4-2x^3-255x^2-40x+13223$, $x^4-x^3-237x^2+132x+13908$, and L_1 is distinguished by being the only one of the five fields in which 2 is totally split.

9 Examples for the Quartic S_4 Case

Since there are so many types, we simply give basic information for each case for which $|\mathcal{L}_2(k)|\le 1$, and the reader can immediately reconstruct the formulas from what we have given above.

k	$\mathcal{L}_2(k)$	k split	L split	disc(k)	polynomial for k
real	$\emptyset$	IN	–	321	x^3-x^2-4x+1
real	$\emptyset$	PS	–	469	x^3-x^2-5x+4
real	$\emptyset$	TS	–	7441	$x^3-x^2-22x-16$
real	$\emptyset$	PR_0	–	568	x^3-x^2-6x-2
real	$\emptyset$	PR_4	–	316	x^3-x^2-4x+2
real	$\emptyset$	TR	–	148	x^3-x^2-3x+1
real	$\mathcal{L}_{tr}(k,64)=\{L\}$	IN	–	257	x^3-x^2-4x+3
real	$\mathcal{L}_{tr}(k,64)=\{L\}$	PS	–	229	x^3-4x-1
real	$\mathcal{L}_{tr}(k,64)=\{L\}$	PR_0	–	1016	x^3-x^2-6x+2
real	$\mathcal{L}_{tr}(k,64)=\{L\}$	TR_4	–	788	x^3-x^2-7x-3
real	$\mathcal{L}(k,16)=\{L\}$	PS	PR_2	2429	$x^3-x^2-14x-4$
real	$\mathcal{L}(k,16)=\{L\}$	PS	$\mathrm{PR}_{2,2}$	1229	x^3-x^2-7x+6
real	$\mathcal{L}(k,16)=\{L\}$	TS	PR_2	2089	$x^3-13x-4$
real	$\mathcal{L}(k,16)=\{L\}$	TS	$\mathrm{PR}_{2,2}$	4481	$x^3-17x-8$
real	$\mathcal{L}(k,16)=\{L\}$	PR_4	–	892	$x^3-x^2-8x+10$
real	$\mathcal{L}(k,4)=\{L\}$	PR_0	–	10216	$x^3-22x-8$
real	$\mathcal{L}(k,4)=\{L\}$	PR_4	–	1436	$x^3-11x-12$
real	$\mathcal{L}(k,4)=\{L\}$	TR	–	1556	$x^3-x^2-9x+11$
real	$\mathcal{L}(k,1)=\{L\}$	IN	–	2777	$x^3-x^2-14x+23$
real	$\mathcal{L}(k,1)=\{L\}$	PS	IN	1957	$x^3-x^2-9x+10$
real	$\mathcal{L}(k,1)=\{L\}$	PS	$\mathrm{PS}_{2,1,1}$	24197	$x^3-20x-17$
real	$\mathcal{L}(k,1)=\{L\}$	TS	TS	500033	$x^3-143x+370$
real	$\mathcal{L}(k,1)=\{L\}$	TS	$\mathrm{PS}_{2,2}$	35401	$x^3-x^2-34x-16$
real	$\mathcal{L}(k,1)=\{L\}$	TR	–	8468	$x^3-x^2-27x-43$
real	$\mathcal{L}(k,1)=\{L\}$	PR_0	$\mathrm{PR}_{2,1}$	13768	$x^3-x^2-18x-14$
real	$\mathcal{L}(k,1)=\{L\}$	PR_0	$\mathrm{PR}_{2,1,1}$	44648	$x^3-x^2-58x+186$
real	$\mathcal{L}(k,1)=\{L\}$	PR_4	$\mathrm{PR}_{2,1}$	11324	$x^3-x^2-20x-22$
real	$\mathcal{L}(k,1)=\{L\}$	PR_4	$\mathrm{PR}_{2,1,1}$	59468	$x^3-59x-168$

Examples for k totally real

k	$\mathcal{L}_2(k)$	k split	L split	disc(k)	polynomial for k
complex	$\emptyset$	–	–	–	cannot happen
complex	$\mathcal{L}_{tr}(k, 64) = \{L\}$	IN	–	-23	$x^3 - x^2 + 1$
complex	$\mathcal{L}_{tr}(k, 64) = \{L\}$	PS	–	-59	$x^3 + 2x - 1$
complex	$\mathcal{L}_{tr}(k, 64) = \{L\}$	PR_0	–	-104	$x^3 - x - 2$
complex	$\mathcal{L}_{tr}(k, 64) = \{L\}$	TR_4	–	-44	$x^3 - x^2 + x + 1$
complex	$\mathcal{L}(k, 16) = \{L\}$	PS	PR_2	-83	$x^3 - x^2 + x - 2$
complex	$\mathcal{L}(k, 16) = \{L\}$	PS	$\mathrm{PR}_{2,2}$	-547	$x^3 - x^2 - 3x - 4$
complex	$\mathcal{L}(k, 16) = \{L\}$	TS	PR_2	-431	$x^3 - x - 8$
complex	$\mathcal{L}(k, 16) = \{L\}$	TS	$\mathrm{PR}_{2,2}$	-1727	$x^3 - x - 16$
complex	$\mathcal{L}(k, 16) = \{L\}$	PR_4	–	-116	$x^3 - x^2 - 2$
complex	$\mathcal{L}(k, 4) = \{L\}$	PR_0	–	-856	$x^3 - x^2 + x + 11$
complex	$\mathcal{L}(k, 4) = \{L\}$	PR_4	–	-212	$x^3 - x^2 + 4x - 2$
complex	$\mathcal{L}(k, 4) = \{L\}$	TR	–	-172	$x^3 - x^2 - x + 3$
complex	$\mathcal{L}(k, 1)$	–	–	–	cannot happen

Examples for k complex

The cases "cannot happen" follow immediately from Corollary 6.9, the first directly from (2), and the second since if $|\mathcal{L}_2(k)| = 1$ we must have $\mathrm{rk}_2(k) = 0$, i.e., $2 \nmid h(k)$, so $\mathcal{L}(k, 1) = \emptyset$.

References

[1] H. Cohen, *Counting A_4 and S_4 number fields with given resolvent cubic*, Proceedings Banff Conference in honor of Hugh Williams, Fields Inst. Comm. **41** (2004), 159–168.

[2] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Math. **193**, Springer-Verlag (2000).

[3] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Counting A_4 and S_4 extensions of number fields*, unpublished preprint.

[4] H. Cohen and A. Morra, *Counting cubic extensions with given quadratic resolvent*, J. Algebra **325** (2011), 461–478.

[5] H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage*, Math. Zeit. **31** (1930), 565–582, and Math. Abhandlungen, Walter de Gruyter (1975), 423–440.