# APPENDIX TO: DIRICHLET SERIES ASSOCIATED TO QUARTIC FIELDS WITH GIVEN RESOLVENT

HENRI COHEN AND FRANK THORNE

ABSTRACT. This is an appendix to our paper [1], where we give an explicit formula for the Dirichlet series $\sum_K |\mathrm{Disc}(K)|^{-s}$, where the sum is over isomorphism classes of all quartic fields whose cubic resolvent field is isomorphic to $k$.

In the present note, we give a complete proof of a theorem enumerating splitting types of certain number fields, which was stated in [1] without a complete proof. The details are somewhat long and not terribly difficult, and so we decided to leave them out of [1]. The results proved here were largely (and independently) also obtained by Martinet [2], again in unpublished work.

This is an appendix to [1], not intended for publication. Accordingly we refer to [1] for the motivation for proving Theorem 0.4. Here we simply commence with the details, although this note should be fairly readable on its own.

We also note that many of the results in this paper were obtained independently and previously in unpublished work of Martinet [2].

In [1] and the present note, we are interested in studying $A_4$- and $S_4$-quartic fields; i.e., quartic fields whose Galois closure is isomorphic to $A_4$ or $S_4$ respectively. In the $A_4$ case, $\widetilde{K}$ contains a unique cyclic cubic subfield $k$, and in the $S_4$ case, $\widetilde{K}$ contains three isomorphic noncyclic cubic subfields $k$. In either case $k$ is called the *cubic resolvent* of $K$, it is unique up to isomorphism, and it satisfies $\mathrm{Disc}(K) = \mathrm{Disc}(k)f(K)^2$ for some integer $f(K)$.

*Definition* 0.1. Given any cubic field $k$ (cyclic or not), 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 $n$ define $\mathcal{L}(k, n^2)$ to be the subset of $\mathcal{L}(k)$ of those fields with discriminant equal to $n^2\mathrm{Disc}(k)$.

Finally, we define $\mathcal{L}_{tr}(k, 64)$ to be the subset of those $L \in \mathcal{L}(k, 64)$ such that 2 is totally ramified in $L$, and we set

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

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

We introduce some standard notation for splitting types of primes in a number field. If $L$ is, say, a quartic field, and $p$ is a prime for which $(p) = \mathfrak{p}_1^2\mathfrak{p}_2$ in $L$, where $\mathfrak{p}_i$ has residue class degree $i$ for $i = 1, 2$, we say that $p$ has splitting type $(21^2)$ in $L$ (or simply that $p$ is $(21^2)$ in $L$). Other splitting types such as $(22)$, $(1111)$, $(1^4)$, etc. are defined similarly. Moreover, when 2 has type $(1^21)$ in a cubic field $k$, we say that 2 has type $(1^21)_0$ or $(1^21)_4$ depending on whether $\mathrm{Disc}(k) \equiv 0 \pmod 8$ or $\mathrm{Disc}(k) \equiv 4 \pmod 8$.

*Definition* 0.2.

(1) We will say that an element $\alpha \in k^*$ (resp., an ideal $\mathfrak{a}$ of $k$) has square norm if $\mathcal{N}(\alpha)$ (resp., $\mathcal{N}(\mathfrak{a})$) is a square in $\mathbb{Q}^*$.[1]
(2) We will say that a quadratic extension $K_6/k$ has *trivial norm* if there exists $\alpha \in k^* \backslash {k^*}^2$ of square norm such that $K_6 = k(\sqrt{\alpha})$. (Observe that this implies $\alpha \notin \mathbb{Q}$.)

Note that if the principal ideal $(\alpha)$ has square norm then $\alpha$ has either square norm or minus square norm, but since we will only be considering such elements in *cubic* fields, this means that $\pm\alpha$ has square norm for a suitable sign.

**Theorem 0.3.** *There is a correspondence between isomorphism classes of $A_4$ or $S_4$-quartic fields $K$, and pairs $(k, K_6)$, where $k$ is the cubic resolvent field of $K$, and $K_6/k$ is a quadratic extension of trivial norm. Under this correspondence we have* $\mathrm{Disc}(K) = \mathrm{Disc}(k)\mathcal{N}(\mathfrak{d}(K_6/k))$ *and more precisely the Artin relation*

$$\zeta_K(s) = \frac{\zeta(s)\zeta_{K_6}(s)}{\zeta_k(s)}. \tag{0.1}$$

*If $K$ is an $S_4$-field then this correspondence is a bijection, and $K_6$ is equal to the unique extension of $k$ with* $\mathrm{Gal}(\widetilde{K}/K_6) \simeq C_4$. *If $K$ is an $A_4$-field, then $k$ has three quadratic extensions, given by adjoining a root of $\alpha$ or either of its nontrivial conjugates, and this correspondence is* 1*-to-*3*, with any of these fields yielding the same $K$ (up to isomorphism).*

*Proof.* See [1], except for the Artin relation (which will likely be left out of the final version of [1]), which follows from the character theory of $A_4$ and $S_4$. □

In [1] is is necessary to understand the possible ways in which primes can split in various field extensions. The following is the main result of the paper, enumerating the possible ways in which primes can split in the fields $k$, $K_6$, and $L$.

**Theorem 0.4.** *Let $(k, K_6, L)$ be as described in Theorem 0.3 (with $K$ replaced by $L$), and let $p$ be a prime. The possible splittings of $p$ in the three fields is given in the tables below, where OK indicates that the splitting can occur for at least one $p$ (or for $p = 2$ in the corresponding column), and any other mark is an indication of the reason for impossibility, explained below. In one case for $p = 2$ the distinction between $(1^21)_0$ and $(1^21)_4$ is made, but in all other cases where OK is indicated, both can occur.*

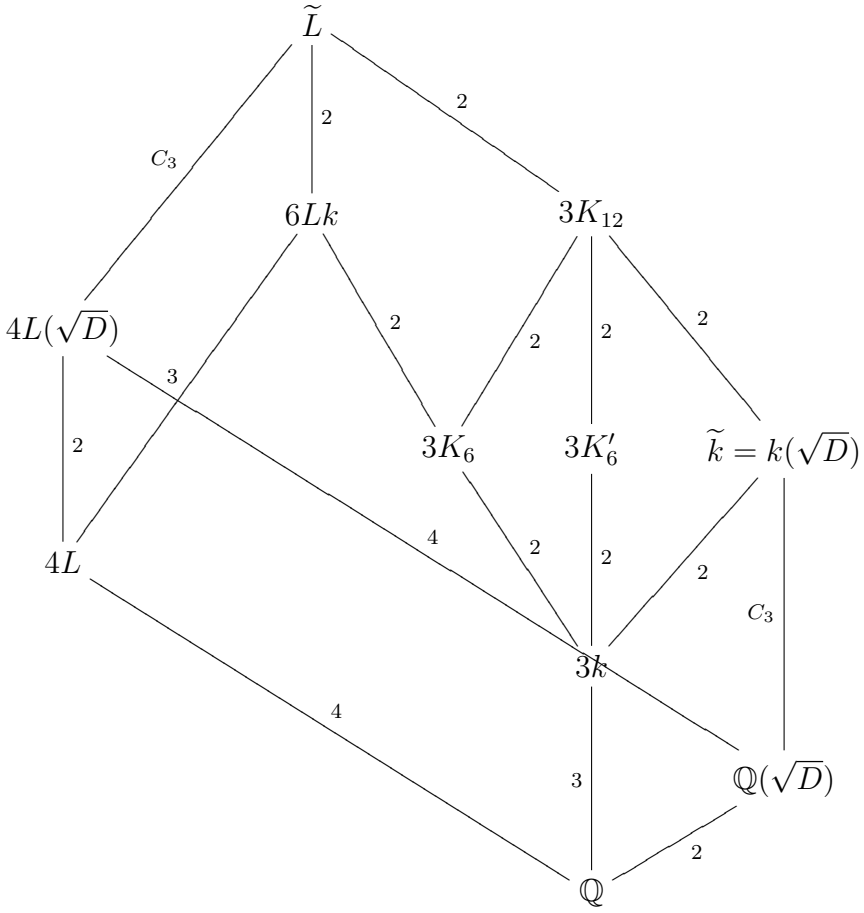
[1]Note that in [**?**] there is a misprint in the definition of square norm, where "$\mathcal{N}_{K_6/k}(\alpha)$ square in $k$" should be replaced by what we have written, i.e., simply "$\alpha$ of square norm", in other words $\mathcal{N}(\alpha)$ square in $\mathbb{Q}^*$.

| $k$-split | $K_6$-split | $L$-split | Possible for $p \neq 2$ ? | Possible for $p = 2$ ? |
|---|---|---|---|---|
| (3) | (6) | — | ZETA | ZETA |
| (3) | (33) | (31) | OK | OK |
| (3) | $(3^2)$ | $(1^4)$ | SQN | OK |
| (21) | (42) | (4) | OK | OK |
| (21) | (411) | — | ZETA | ZETA |
| (21) | $(41^2)$ | — | ZETA | ZETA |
| (21) | (222) | (22) | STICK | STICK |
| (21) | (2211) | (211) | OK | OK |
| (21) | $(221^2)$ | $(21^2)$ | SQN | GRP(1) |
| (21) | $(2^22)$ | $(2^2)$ | OK | OK |
| (21) | $(2^211)$ | $(1^31)$ | RAM | RAM |
| (21) | $(2^211)$ | $(1^21^2)$ | OK | OK |
| (21) | $(2^21^2)$ | $(1^4)$ | SQN | OK |

| $k$-split | $K_6$-split | $L$-split | Possible for $p \neq 2$ ? | Possible for $p = 2$ ? |
|---|---|---|---|---|
| (111) | (222) | — | ZETA | ZETA |
| (111) | (2211) | (22) | OK | OK |
| (111) | $(221^2)$ | — | ZETA | ZETA |
| (111) | (21111) | (211) | STICK | STICK |
| (111) | $(2111^2)$ | $(21^2)$ | SQN | GRP(2) |
| (111) | $(21^21^2)$ | $(2^2)$ | OK | OK |
| (111) | (111111) | (1111) | OK | OK |
| (111) | $(1^21111)$ | $(1^211)$ | SQN | GRP(3) |
| (111) | $(1^21^211)$ | $(1^21^2)$ | OK | OK |
| (111) | $(1^21^211)$ | $(1^31)$ | RAM | RAM |
| (111) | $(1^21^21^2)$ | $(1^4)$ | SQN | OK |

| $k$-split | $K_6$-split | $L$-split | Possible for $p \neq 2$ ? | Possible for $p = 2$ ? |
|---|---|---|---|---|
| $(1^2 1)$ | $(2^2 2)$ | — | ZETA | ZETA |
| $(1^2 1)$ | $(2^2 11)$ | $(21^2)$ | OK | OK |
| $(1^2 1)$ | $(2^2 1^2)$ | $(2^2)$ | SQN | GRP(4) |
| $(1^2 1)$ | $(1^2 1^2 2)$ | $(21^2)$ | GRP(5) | GRP(5) |
| $(1^2 1)$ | $(1^2 1^2 11)$ | $(1^2 11)$ | OK | OK |
| $(1^2 1)$ | $(1^2 1^2 1^2)$ | $(1^2 1^2)$ | SQN | GRP(6) |
| $(1^2 1)_0$ | $(1^4 2)$ | $(2^2)$ | SQN | PARITY |
| $(1^2 1)_4$ | $(1^4 2)$ | $(2^2)$ | SQN | OK |
| $(1^2 1)$ | $(1^4 11)$ | $(1^2 1^2)$ | SQN | OK |
| $(1^2 1)$ | $(1^4 1^2)$ | $(1^4)$ | OK | OK |
| $(1^3)$ | $(2^3)$ | $(2^2)$ | GRP(7) | GRP(7) |
| $(1^3)$ | $(1^3 1^3)$ | $(1^2 1^2)$ | GRP(8) | GRP(8) |
| $(1^3)$ | $(1^3 1^3)$ | $(1^3 1)$ | OK | OK |
| $(1^3)$ | $(1^6)$ | $(1^4)$ | SQN | OK |

Before starting the proof, we give the Hasse diagram of $S_4$.



In this diagram $D$ is as above the discriminant of $k$ up to a square, and the number to the left of each field is the number of conjugates inside $\widetilde{L}$. If $K_6 = k(\sqrt{\alpha})$, the field $K_6'$ is the field $k(\sqrt{\alpha D})$. Finally note that, in addition to the indicated Galois degree 2 extensions and $C_3$ extensions, we have $\mathrm{Gal}(\widetilde{L}/L) \simeq S_3$, $\mathrm{Gal}(\widetilde{L}/k) \simeq D_4$, $\mathrm{Gal}(\widetilde{L}/K_6) \simeq V_4$, $\mathrm{Gal}(\widetilde{L}/\widetilde{k}) \simeq V_4$, $\mathrm{Gal}(\widetilde{L}/K_6') \simeq C_4$, and of course $\mathrm{Gal}(K_{12}/k) \simeq V_4$.

*Proof.* Since $K_6/k$ is a quadratic extension, the possible splitting types of a prime ideal of $k$ in $K_6$ are (2), (11), and $(1^2)$. It is then easily checked that when a prime splits in $k$ as (3), (21), (111), $(1^21)$, or $(1^3)$, there are 3, 9, 10, 9, or 3 splitting types in $K_6$ respectively, given in the above tables. We first give some general tools for ruling out certain splittings.

- Using the Euler factors coming from the zeta function relation (0.1). For example, if a prime splits as (21) in $k$ then it cannot split as (411) or as $(41^2)$ in $K_6$ since in that case the inverse of the Euler factors for $\zeta_L(s)$ would be $(1+p^{-2s})(1-p^{-s})^2$ or $(1+p^{-2s})(1-p^{-s})$, which are not possible for Dedekind zeta function Euler factors. We write ZETA for this. In this case, and only in this case, we evidently do not indicate any splitting in $L$.

  Note also that the Euler factor for $\zeta_L(s)$ determines the splitting type, with the unique exception of $(1-p^{-s})^{-2}$ which can correspond to the splittings $(1^21^2)$ and $(1^31)$.
- Using Stickelberger's theorem: recall that if $F$ is a number field of degree $n$ and $p$ is a prime unramified in $F$ which splits into $g$ prime ideals, then $\left(\frac{\mathrm{Disc}(F)}{p}\right) = (-1)^{n-g}$. Thus, since $\mathrm{Disc}(L) = \mathrm{Disc}(k)f(L)^2$, it follows that when $p$ is unramified both in $k$ and $L$ the number of primes above $p$ in $k$ and $L$ must have opposite parity. For example, if a prime $p$ splits as (21) in $k$ and (222) in $K_6$, the zeta function relation shows that the inverse Euler factor is equal to $(1-p^{-2s})^2$, so the splitting in $L$ must be (22), contradicting Stickelberger. We write STICK for this.
- Using the square norm condition: recall that $\mathfrak{d}(K_6/k) = 4\mathfrak{a}/\mathfrak{c}^2$ with $\mathfrak{a}$ integral, square-free, and of square norm. Thus if $\mathfrak{p}$ is a prime ideal of $k$ not dividing 2 which is ramified in $K_6/k$, we must have $v_{\mathfrak{p}}(\mathfrak{a}) = 1$, and since $\mathfrak{a}$ has square norm it follows that

$$0 \equiv v_p(\mathcal{N}(\mathfrak{d}(K_6/k))) = v_p(\mathcal{N}(\mathfrak{a})) = \sum_{\substack{\mathfrak{p}\mid p\mathbb{Z}_k \\ \mathfrak{p}\mid\mathfrak{a}}} f(\mathfrak{p}/p)v_{\mathfrak{p}}(\mathfrak{a}) = \sum_{\substack{\mathfrak{p}\mid p\mathbb{Z}_k \\ \mathfrak{p}\mid\mathfrak{d}(K_6/k)}} f(\mathfrak{p}/p) \pmod 2 .$$

  For example, if a prime $p \neq 2$ splits as (21) in $k$ and $(221^2)$ in $K_6$, writing $p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_i$ of degree $i$, the above relation gives $1 = f(\mathfrak{p}_1/p) \equiv 0 \pmod 2$, a contradiction. We write SQN for this. Note that it is not possible to apply this to $p = 2$.
- Using divisibility by 3 of ramification degrees: assume that a prime $p$ splits as $(1^31)$ in $L/\mathbb{Q}$. With evident notation this implies that $3 \mid e(\mathfrak{p}_{\widetilde{L}}/p) = e(\mathfrak{p}_{\widetilde{L}}/\mathfrak{p}_k)e(\mathfrak{p}_k/p)$, and since $\widetilde{L}/k$ is Galois of order 4 or 8 and in particular coprime to 3, we have $3 \nmid e(\mathfrak{p}_{\widetilde{L}}/\mathfrak{p}_k)$ hence $3 \mid e(\mathfrak{p}_k/p)$, and since $k$ is a cubic field this means that $p$ splits as $(1^3)$ in $k$. We write RAM for this.
- In the following special case we reason as follows: assume that $p = 2$ splits as $(1^21)$ in $k$, $(1^42)$ in $K_6$, and $(2^2)$ in $L$. We have $v_2(\mathrm{Disc}(L)) = 4$ or 6 (see Lemma **??**), and since $\mathrm{Disc}(L) = \mathrm{Disc}(k)f(L)^2$ we thus have $v_2(\mathrm{Disc}(k)) \equiv v_2(\mathrm{Disc}(L)) \equiv 0 \pmod 2$,

hence $v_2(\mathrm{Disc}(k)) = 2$ since 2 is ramified in $k$, so $\mathrm{Disc}(k) \equiv 4 \pmod 8$. We write PARITY for this.

For the remaining impossibility proofs, we use a case-by-case study, in general using the decomposition and/or inertia groups. We write GRP(i) for this, with i ranging from 1 to 8. First recall the following well-known facts.

- Let $p$ be a prime, $\mathfrak{P}$ a prime ideal of $\widetilde{L}$ above $p$, and write $[\widetilde{L} : \mathbb{Q}] = efg$ with the usual meaning. If $D = D(\mathfrak{P}/p)$ and $I = I(\mathfrak{P}/p)$ denote the decomposition and inertia group, then $|D| = ef$, $|I| = e$, there is an unramified prime $\mathfrak{p}_D$ of degree 1 in $\widetilde{L}^D/\mathbb{Q}$, which we write as $e(\mathfrak{p}_D/p) = f(\mathfrak{p}_D/p) = 1$, $g(\mathfrak{p}_D/p) = g$, the prime ideal below $\mathfrak{P}$ in $\widetilde{L}^D$ stays inert in the extension $\widetilde{L}^I/\widetilde{L}^D$, which we write as $e(\mathfrak{p}_I/p_D) = g(\mathfrak{p}_I/\mathfrak{p}_D) = 1$, $f(\mathfrak{p}_I/\mathfrak{p}_D) = f$, and finally the prime ideal below $\mathfrak{P}$ in $\widetilde{L}^I$ totally ramifies in $\widetilde{L}/\widetilde{L}^I$, which we write as $f(\mathfrak{P}/\mathfrak{p}_I) = g(\mathfrak{P}/\mathfrak{p}_I) = 1$, $e(\mathfrak{P}/\mathfrak{p}_I) = e$. The fields $\widetilde{L}^D$ and $\widetilde{L}^I$ will be called the *decomposition field* and *inertia field* of $\mathfrak{P}$ above $p$. We have $[\widetilde{L}^D : \mathbb{Q}] = g$, $[\widetilde{L}^I : \widetilde{L}^D] = f$, and $[\widetilde{L} : \widetilde{L}^I] = e$. Finally, note that all decomposition groups and all inertia groups are conjugate, so all decomposition fields and all inertia fields of $\widetilde{L}$ for $p$ are also conjugate.

  **Lemma 0.5.** *(1) Let $K \subset \widetilde{L}$ and assume that $g \mid [K : \mathbb{Q}]$ and that there exists a prime ideal $\mathfrak{p}$ of $K$ above $p$ such that $e(\mathfrak{p}/p) = f(\mathfrak{p}/p) = 1$. Then $[K : \mathbb{Q}] = g$ and $K$ is a decomposition field for $p$.*
  *(2) Let $K \subset \widetilde{L}$ and assume that $fg \mid [K : \mathbb{Q}]$ and that there exists a prime ideal $\mathfrak{p}$ of $K$ above $p$ such that $e(\mathfrak{p}/p) = 1$. Then $[K : \mathbb{Q}] = fg$ and $K$ is an inertia field for $p$.*

  *Proof.* Immediate from the definitions and the transitivity of $e$ and $f$, and left to the reader. □

- Using the description on the subgroups of $A_4$ and $S_4$ it is immediate to see that the only quartic subfields of $\widetilde{L}$ are the conjugates of $L$, in the $S_4$ case the only quadratic subfield is $\mathbb{Q}(\sqrt{\mathrm{Disc}(k)})$, and in the $A_4$ case there is no quadratic subfield. The other fields are given for $S_4$ in the Hasse diagram above.
- If $p$ is not totally ramified, recall also that the splitting of $p$ in $k$ determines that of $p$ in $\widetilde{k}$: if $k$ is noncyclic and $p$ splits as (3), (21), (111), and $(1^21)$ in $k$ then it splits as (33), (222), (111111), and $(1^21^21^2)$ in $\widetilde{k}$ respectively. This is *not* true if $p$ is totally ramified, i.e., splits as $(1^3)$ in $k$.
- No prime is totally ramified in a $V_4$-extension.
- If $k$ is cyclic then $p$ must be (111), (3), or $(1^3)$ in $k$.

GRP(1) Assume that $p$ is (21) in $k$ (in the $S_4$ case only), $(221^2)$ in $K_6$, and $(21^2)$ in $L$. We have $2 \mid e$ and $2 \mid f$. If $\mathfrak{P}$ is an ideal of $\widetilde{L}$ above the ideal $\mathfrak{p}$ of $L$ with $f(\mathfrak{p}/p) = 2$, we have $e(\mathfrak{P}/\mathfrak{p}) \mid [\widetilde{L} : L] = 6$, and since $e(\mathfrak{p}/p) = 1$ it follows that $e = e(\mathfrak{P}/p) \mid 6$, so that $e = 2$. Similarly, by considering the ideal $\mathfrak{p}$ of $L$ with $e(\mathfrak{p}/p) = 2$ we see that $f = 2$. Thus the decomposition fields are quartic fields, and since the only quartic subfields

of $\widetilde{L}$ are the conjugates of $L$, it follows that $L$ is a decomposition field, a contradiction since none of the prime ideals $\mathfrak{p}$ of $L$ above $p$ satisfy $e(\mathfrak{p}/p) = f(\mathfrak{p}/p) = 1$.

GRP(2) Assume that $p$ is (111) in $k$, ($2111^2$) in $K_6$, and ($21^2$) in $L$. In the $S_4$ case $p$ is (111111) in $\widetilde{k}$, we have $2 \mid e$, $2 \mid f$, and $6 \mid g$, so $e = f = 2$ and $g = 6$. By Lemma 0.5 it follows that $\widetilde{k}$ and $K_6$ are decomposition fields, a contradiction since they are not conjugate. In the $A_4$ case we have $2 \mid e$, $2 \mid f$, and $3 \mid g$, so $e = f = 2$ and $g = 3$. However, since there exists a prime ideal $\mathfrak{p}$ of $K_6$ such that $e(\mathfrak{p}/p) = f(\mathfrak{p}/p) = 1$ it follows from Lemma 0.5 that $[K_6 : \mathbb{Q}] = 3$, a contradiction.

GRP(3) Assume that $p$ is (111) in $k$, ($1^21111$) in $K_6$, and ($1^211$) in $L$. We thus have $2 \mid e$ and $6 \mid g$. If we had $ef = 4$ the decomposition fields would be sextic. However, in view of the splittings of $p$ in $\widetilde{k}$ and in $K_6$, both of these fields would be decomposition fields, which is absurd since they are not conjugate, the decomposition of $p$ being different. Thus $ef = 2$, i.e., $f = 1$ and $e = 2$. But then the decomposition fields would be of degree 12. This is clearly impossible in the $A_4$ case since $p$ is ramified. In the $S_4$ case, since $p$ is (111111) in $\widetilde{k}$, there must be a decomposition field containing $\widetilde{k}$, which by the Hasse diagram must be conjugate to $K_{12}$; however, writing $p\mathbb{Z}_L = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$ in $L$, since the ramification indices cannot exceed 2 there must be a prime $\mathfrak{p}_2'$ of $Lk$ above $\mathfrak{p}_2$ with $e(\mathfrak{p}_2'/\mathfrak{p}_2) = f(\mathfrak{p}_2'/\mathfrak{p}_2) = 1$, so that by Lemma 0.5 $Lk$ is a decomposition field for $p$. This is again absurd since $K_{12}$ and $Lk$ are not conjugate.

GRP(4) Assume that $p$ is ($1^21$) in $k$, ($2^21^2$) in $K_6$, and ($2^2$) in $L$. We have $2 \mid e$, $2 \mid f$, and since $p$ is ($1^21^21^2$) in $\widetilde{k}$ we have $3 \mid g$. Thus $|I| = e = 2$ or 4. Assume first that $|I| = 2$, so that the inertia fields have degree 12. Note that all ideals above $p$ are ramified in $K_6$, hence also in $K_{12}$, and the unique ideal of above $p$ in $L$ is ramified, so also in $Lk$. Since all degree 12 subfields are conjugate to $K_{12}$ or to $Lk$ we obtain a contradiction. Assume now that $|I| = e = 4$, so that the inertia fields have degree 6. Because of the ramification in $K_6$ and $\widetilde{k}$, the only possibility is that the inertia fields are conjugate to $K_6'$, so $I = \mathrm{Gal}(\widetilde{L}/K_6')$ with a suitable choice of conjugate. However this Galois group is cyclic, while the Galois group of $\widetilde{L}/K_6$ is isomorphic to $V_4$, a contradiction.

GRP(5) Assume that $p$ is ($1^21$) in $k$, ($1^21^22$) in $K_6$, and ($21^2$) in $L$. Then again $2 \mid e$, $2 \mid f$, and since $p$ is $1^21^21^2$ in $\widetilde{k}$ we have $3 \mid g$. Thus, if $I$ denotes an inertia group, we have $|I| = 2$ or 4. Assume first that $|I| = e = 2$. We then have $|D| = ef = 4$ or 8. If $|D| = 8$ then the decomposition fields are cubic hence conjugate to $k$, so $D \simeq \mathrm{Gal}(\widetilde{L}/k) \simeq D_4$, while $I$ is generated by a transposition, absurd since $I$ is a normal subgroup of $D$. Thus $|D| = 4$, so the decomposition fields are sextic. However it cannot be conjugate to $K_6$ since no prime ideal $\mathfrak{p}$ above $p$ of this field satisfies $e(\mathfrak{p}/p) = f(\mathfrak{p}/p) = 1$, and for the same reason it cannot be $\widetilde{k}$. Finally it cannot be $K_6'$: if $\mathfrak{p}_1$ is the unique prime ideal of $k$ above $p$ which is unramified, it is ($1^2$) in $\widetilde{k}/k$, (2) in $K_6/k$, hence necessarily ($1^2$) in $K_6'$, the third quadratic subextension of the $V_4$-extension $K_{12}/k$. Thus we cannot have $|I| = 2$.

Assume now that $|I| = e = 4$, so that $f = 2$, $|D| = ef = 8$, and $g = 3$. As $[\widetilde{L} : K_6] = |I|$, the prime ideal of degree 2 above $p$ in $K_6$ is unramified over $\mathbb{Q}$ and

hence totally ramified in the extension $\widetilde{L}/K_6$. This is absurd since this extension has Galois group $V_4$, and no prime ideal can be totally ramified in such an extension.

GRP(6) Assume that $p = 2$ is $(1^21)$ in $k$, $(1^21^21^2)$ in $K_6$, and $(1^21^2)$ in $L$. We now have $2 \mid e$ and $3 \mid g$. Let $\mathfrak{p}$ denote the prime ideal of $k$ which is unramified above $p$. Since $\mathrm{Gal}(K_{12}/k) \simeq V_4$, the ideal $\mathfrak{p}$ cannot be totally ramified in $K_{12}/k$, so if $\mathfrak{P}$ is an ideal of $\widetilde{L}$ above $\mathfrak{p}$ we have $e = e(\mathfrak{P}/p) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/p) \mid 4$. It follows that $e = 2$ or 4, and since the only difference with the GRP(4) case is that the ramified prime above $p$ in $k$ is split in $K_6/k$ instead of being inert, the proof of impossibility of $e = 2$ and $e = 4$ is the same.

GRP(7) Assume that $p$ is $(1^3)$ in $k$, $(2^3)$ in $K_6$, and $(2^2)$ in $L$. We thus have $3 \mid e$ (because of $k$), $2 \mid e$ (because of $L$), and $2 \mid f$, so $6 \mid e$ and $2 \mid f$. Thus in particular $2 \mid fg = [\widetilde{L} : \mathbb{Q}]/e \mid 4$. It follows that the inertia fields are either quadratic or quartic. If $\mathfrak{q}$ is a prime ideal above $p$ of such a field we have $e(\mathfrak{q}/p) = 1$. Since quartic subfields are conjugate to $L$ and $p$ splits as $(2^2)$ in $L$ the inertia field cannot be quartic. Thus it is quadratic, so we are in the $S_4$ case and the field is $\mathbb{Q}(\sqrt{\mathrm{Disc}(k)})$, hence $e = 12$, $f = 2$, and $g = 1$. The decomposition field is thus $\mathbb{Q}$ itself, so $p$ is inert in $\mathbb{Q}(\sqrt{\mathrm{Disc}(k)})$. Thus $p$ splits as $(2^3)$ in $\widetilde{k}$, and in particular the extension $\widetilde{k}/k$ is unramified at $p$. Since $K_6/k$ is also unramified at $p$, it follows that the degree 12 compositum $K_{12}/k$ is unramified at $p$, so that $e \mid 6$, a contradiction.

GRP(8) Assume that $p$ is $(1^3)$ in $k$, $(1^31^3)$ in $K_6$, and $(1^21^2)$ in $L$. Then as above $6 \mid e$ and $2 \mid g$, so the decomposition fields and inertia fields are either quadratic or quartic, they cannot be quartic since all primes of $L$ above $p$ are ramified, so we are in the $S_4$ case, the decomposition and inertia fields are both equal to $\mathbb{Q}(\sqrt{\mathrm{Disc}(k)})$, hence $e = 12$, $g = 2$, and $f = 1$. Since $p$ is unramified in this decomposition field and $f = 1$, it is split, hence the prime $\mathfrak{p}$ above $p$ in $k$ splits in $\widetilde{k}$. Since it also splits in $K_6$ it follows that it is totally split in the degree 12 compositum $K_{12}/k$ of $\widetilde{k}$ and $K_6$, hence that $4 \mid g$, a contradiction.

To finish the proof of Theorem 0.4, we simply need to find an occurrence of the given splittings in all entries of the table marked OK. This is done by an easy computer search. Note that almost all of the needed examples for $p = 2$ are given in the table of Proposition **??** below: the only missing ones are those for which $K_6$ cannot be generated by a totally positive virtual unit coprime to 2, namely for $(k, K_6, L)$ split as $((111), (1^21^21^2), (1^4))$ and $((1^21)_4, (1^41^2), (1^4))$, for which (random) examples of suitable $P_\alpha(x)$ are $x^3 + 3x^2 - 10x - 16$ and $x^3 - 4x^2 - 10x - 4$ respectively. □

By inspection of the tables, we immediately obtain the following corollaries:

**Corollary 0.6.**

*(1) A prime $p$ is $(1^4)$ 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 $(1^4)$ in $L$ only if $p$ is $(1^21)$ in $k$.*

**Corollary 0.7.** *Let $L$ be an $A_4$ or $S_4$-quartic field, and let $k$ be its cubic resolvent. Suppose first that $p \geq 3$ is a prime number.*

*1. If $p$ is $(3)$ in $k$, then $p$ is $(31)$ in $L$.*
*2. If $p$ is $(21)$ in $k$, then $p$ is $(4)$, $(211)$, $(2^2)$, or $(1^21^2)$ in $L$.*
*3. If $p$ is $(111)$ in $k$, then $p$ is $(1111), (22), (2^2)$, or $(1^21^2)$ in $L$.*
*4. If $p$ is $(1^21)$ in $k$, then $p$ is $(21^2)$, $(1^211)$, or $(1^4)$ in $L$.*
*5. If $p$ is $(1^3)$ in $k$, then $p$ is $(1^31)$ in $L$.*

*If $p = 2$, then in addition to the above decomposition types, in all cases 2 can be $(1^4)$ in $L$, if 2 is $(1^21)$ in $k$ then 2 can also be $(1^21^2)$ in $L$, and if 2 is $(1^21)_4$ in $k$ then 2 can also be $(2^2)$ in $L$.*

## References

[1] H. Cohen and F. Thorne, *Dirichlet Series Associated to Quartic Fields with Given Cubic Resolvent*, preprint.
[2] J. Martinet, *Quartic Fields*, unpublished preprint.

Université Bordeaux I, Institut de Mathématiques, U.M.R. 5251 du C.N.R.S, 351 Cours de la Libération, 33405 TALENCE Cedex, FRANCE
*E-mail address*: Henri.Cohen@math.u-bordeaux1.fr

Department of Mathematics, University of South Carolina, 1523 Greene Street, Columbia, SC 29208, USA
*E-mail address*: thorne@math.sc.edu