HANS ROSKAM

Artin’s primitive root conjecture for quadratic fields

Journal de Théorie des Nombres de Bordeaux, tome 14, nº 1 (2002), p. 287-324

<http://www.numdam.org/item?id=JTNB_2002__14_1_287_0>

Journal de Théorie des Nombres de Bordeaux **14** (2002), 287–324

Artin's primitive root conjecture for quadratic fields

par HANS ROSKAM

RÉSUMÉ. Soit α fixé dans un corps quadratrique K. On note S l'ensemble des nombres premiers p pour lesquels α admet un ordre maximal modulo p. Sous G.R.H., on montre que S a une densité. Nous donnons aussi des conditions nécessaires et suffisantes pour que cette densité soit strictement positive.

ABSTRACT. Fix an element α in a quadratic field K. Define S as the set of rational primes p, for which α has maximal order modulo p. Under the assumption of the generalized Riemann hypothesis, we show that S has a density. Moreover, we give necessary and sufficient conditions for the density of S to be positive.

1. introduction

In 1927, in a conversation with Helmut Hasse, Emil Artin made the following conjecture [1, preface; 2, page 476]: for any integer α, not equal to ± 1 or a square, the natural density

$$(1) \qquad \lim_{x\to\infty} \frac{\#\{p \text{ prime} : p \le x \text{ and } \langle\alpha\rangle = \mathbf{F}_p^*\}}{\#\{p \text{ prime} : p \le x\}}$$

of the set of primes p for which α is a primitive root modulo p inside the set of all prime numbers exists and is positive. Artin based this conjecture on the observation that α is a primitive root modulo p if and only if for all primes l, the prime p does not split completely in $\mathbf{Q}(\zeta_l, \sqrt[l]{\alpha})/\mathbf{Q}$. Here ζ_l denotes a primitive l-th root of unity. By Chebotarev's density theorem, the density of the set of primes that do split completely in $\mathbf{Q}(\zeta_l, \sqrt[l]{\alpha})/\mathbf{Q}$ is equal to $[\mathbf{Q}(\zeta_l, \sqrt[l]{\alpha}) : \mathbf{Q}]^{-1}$. Using the principle of inclusion and exclusion, one expects the limit (1) to be equal to

$$(2) \qquad \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbf{Q}(\zeta_k, \sqrt[k]{\alpha}) : \mathbf{Q}]}.$$

Manuscrit reçu le 2 septembre 2000.

It is not clear from this expression whether the density is positive. However, one can show that the infinite sum is equal to a positive rational multiple $c_\alpha \cdot A$ of Artin's constant

$$A = \sum_{n=1}^{\infty} \frac{\mu(n)}{n\varphi(n)} = \prod_{l \text{ prime}} (1 - \frac{1}{l(l-1)}) \approx 0.3739558136.$$

In 1967 Hooley [5] proved that the density (1) is indeed equal to the sum (2), if the generalized Riemann hypothesis (GRH) holds true. Furthermore, he explicitly determined c_α in terms of the prime factorization of α.

Over arbitrary number fields, there are two ways in which Artin's conjecture can be generalized. We fix a number field K with ring of integers $\mathcal{O}$ and a non-zero element $\alpha \in \mathcal{O}$ which is not a root of unity. If we replace $\mathbf{Q}$ by K in the above discussion, we expect the following generalization to hold: the set of primes $\mathfrak{p}$ of K for which α generates $(\mathcal{O}/\mathfrak{p}\mathcal{O})^*$ has a density inside the set of all primes of K. Note that $(\mathcal{O}/\mathfrak{p}\mathcal{O})^*$ is indeed a cyclic group for all primes $\mathfrak{p}$. Moreover, the situation is highly similar to the rational case, as the set of primes $\mathfrak{p}$ of K for which $(\mathcal{O}/\mathfrak{p}\mathcal{O})^*$ is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^*$ has density 1. In 1975 Cooke and Weinberger [3, see also 12] proved that if GRH holds, this generalization of Artin's conjecture is indeed true and the density is given by (2) with $\mathbf{Q}$ replaced by K. Lenstra [4] gave a finite criterion to decide whether this density is zero. Note that we can force the density to vanish by choosing an algebraic integer α, and defining K to be equal to $\mathbf{Q}(\zeta_l, \sqrt[l]{\alpha})$ for some prime l.

The second generalization of Artin's conjecture is in a 'rational' direction: the set of rational primes p for which the order of α in $(\mathcal{O}/p\mathcal{O})^*$ is equal to the exponent of this group, *maximal* for short, has a density inside the set of all rational primes. In this paper we will prove that, modulo the generalized Riemann hypothesis, this conjecture holds for quadratic fields K. The reason for restricting to quadratic fields is twofold. As the exponent of $(\mathcal{O}/p\mathcal{O})^*$ depends on the splitting behaviour of p in $K/\mathbf{Q}$, a proof of the conjecture needs to distinguish between separate cases, one for each splitting type. Quadratic fields admit only two unramified splitting types, and already in this case a fair amount of non-trivial Galois theory is needed to deal with the inert primes. More serious however is the fact that the analytic part of our proof of the conjecture in the quadratic case does not readily generalize to higher degree fields. Such a generalization to fields of degree $k \geq 3$ implies that the set of primes dividing a 'generic' k-th order linear recurrent sequence has a positive lower density [9].

Fix a quadratic field K with ring of integers $\mathcal{O}$ and $\alpha \in K^*$. The *generic* primes are by definition those odd rational primes p that are unramified in $K/\mathbf{Q}$ and for which there are no primes in $\mathcal{O}$ above p in the fractional ideal factorization of $\alpha\mathcal{O}$. As we are interested in density questions, we can disregard the finite set of non-generic primes.

For a generic prime p, the image of α in $(\mathcal{O}/p\mathcal{O})^*$ is well defined. If p is a generic prime that is inert in $K/\mathbf{Q}$, the group $(\mathcal{O}/p\mathcal{O})^*$ is cyclic of order $p^2 - 1$. For these primes we can ask whether α is a generator of $(\mathcal{O}/p\mathcal{O})^*$. We define the set S^- as

$$S^- = \{p \text{ generic prime} : p \text{ is inert in } K/\mathbf{Q} \text{ and } \langle\alpha\rangle = (\mathcal{O}/p\mathcal{O})^*\}.$$

If p is a generic prime that splits in $K/\mathbf{Q}$, the group $(\mathcal{O}/p\mathcal{O})^*$ is no longer cyclic, but isomorphic to $\mathbf{F}_p^* \times \mathbf{F}_p^*$. This group has exponent $p-1$, so we define the set S^+ as

$$S^+ = \{p \text{ generic prime} : p \text{ splits in } K/\mathbf{Q} \text{ and } \alpha \text{ has order } p-1 \text{ in } (\mathcal{O}/p\mathcal{O})^*\}.$$

Before we state theorem 1 we make two more remarks.

1. The generalization of Artin's conjecture that was proved by Cooke and Weinberger does not imply the existence of the density of S^+; it is possible that p is in S^+ while α does not generate $(\mathcal{O}/\mathfrak{p}\mathcal{O})^*$ for either of the primes $\mathfrak{p}$ above p.

2. We say that α and its conjugate $\bar{\alpha}$ are *multiplicatively independent* if the subgroup $\langle\alpha, \bar{\alpha}\rangle \subset K^*$ is free of rank 2, or equivalently, if the map $\mathbf{Z}^2 \longrightarrow K^*$ sending (a, b) to $\alpha^a\bar{\alpha}^b$ is injective.

Theorem 1. *Let K be a quadratic field and fix an element $\alpha \in K^*$. Define the sets S^+ and S^- as above and suppose the generalized Riemann hypothesis holds. Then S^+ and S^- both have a natural density inside the set of all rational primes. Moreover, there exist rational numbers c_α^+ and c_α^-, depending on α, such that*

$$\delta(S^+) = \begin{cases} c_\alpha^+ \cdot \prod_{l \text{ prime}}(1 - \frac{1}{l^2(l-1)}) & \textit{if } \alpha \textit{ and its conjugate } \bar{\alpha} \textit{ are multiplicatively independent;} \\ c_\alpha^+ \cdot \prod_{l \text{ prime}}(1 - \frac{1}{l(l-1)}) & \textit{otherwise,} \end{cases}$$

and

$$\delta(S^-) = c_\alpha^- \cdot \prod_{\substack{l \text{ odd} \\ \text{prime}}} (1 - \frac{2}{l(l-1)}).$$

We are not able to prove the existence of the density unconditionally. Even in the case of Artin's original conjecture it is not known whether, for a given non-square integer $a \neq -1$, the set of primes p for which a is a primitive root modulo p is infinite.

To explain the significance of the rational numbers c_α^+ and c_α^-, we first sketch the proof of the theorem. In section 2 we characterize the primes in S^+ and S^- in terms of splitting conditions in the fields

$$L_l = K(\zeta_l, \sqrt[l]{\alpha}, \sqrt[l]{\bar{\alpha}}),$$

where l ranges over the prime numbers. The fields L_l are the analogues of the fields $\mathbf{Q}(\zeta_l, \sqrt[l]{\alpha})$ occurring in the proof of Artin's original conjecture.

To express the densities as infinite sums similar to (2), we adapt Hooley's arguments to our situation. This is straightforward for the set S^+; for the inert primes additional arguments are needed. In order to prove that these infinite sums are equal to the Euler products in theorem 1, we need to know the obstruction for the fields $\{L_l\}_l$, with l ranging over the primes, to be linearly disjoint over K. Here and in the rest of this paper, we say that a collection of subfields $\{L_i\}_{i\in I}$ of some field $\bar{L}$ is *linearly disjoint over* a subfield K of $\bar{L}$, if the following holds: for all $j \in I$, the intersection of L_j and the compositum of the fields $\{L_i\}_{i\in I, i\neq j}$ is equal to K. In addition, we have to compute the degrees of the fields L_l. In propositions 8 and 10 we determine a finite set of primes I such that the fields $\{L_l\}_{l\notin I}$ are of 'generic' degree and linearly disjoint over K. The rational numbers c_α^+ and c_α^- take care of the remaining primes, and can be seen as 'correction factors'.

In Artin's original conjecture, the density of the set of primes p for which α is a primitive root vanishes if and only if α is -1 or a square, the if-part being obvious. In our situation there are also some more or less obvious situations of zero density.

Proposition 2. *Let K, α, S^+ and S^- be as in theorem 1.*

a. *In each of the following cases, the set S^+ is finite:* (i) *α is a root of unity;* (ii) *α is a square in K^*;* (iii) *$K = \mathbf{Q}(\zeta_3)$ and α is a cube in K^*.*
b. *In each of the following cases, the set S^- is finite:* (i) *α and $\bar{\alpha}$ are multiplicatively dependent;* (ii) *α is a cube in K^*;* (iii) *$\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is a square in $\mathbf{Q}^*$;* (iv) *$K = \mathbf{Q}(\zeta_3)$ and $\frac{\alpha}{\bar{\alpha}}$ is a cube in K^*.*

Proof. a. If α is a root of unity, the set S^+ is clearly finite. Now assume that α is a square in K^* and that p is a generic prime that splits in $K/\mathbf{Q}$. As p is odd, the exponent of $(\mathcal{O}/p\mathcal{O})^*$ is even, so the order of α in this group divides $(p-1)/2$. We find $p \notin S^+$ and the set S^+ is empty. If K is equal to $\mathbf{Q}(\zeta_3)$ and p splits in $K/\mathbf{Q}$, the exponent $p-1$ of the group $(\mathcal{O}/p\mathcal{O})^*$ is divisible by 3. In case α is a cube in K^*, its order modulo $p\mathcal{O}$ is at most $(p-1)/3$ and hence S^+ is empty.
b. Let p be a generic prime, inert in $K/\mathbf{Q}$. Assume that α and $\bar{\alpha}$ are multiplicatively dependent, say $\alpha^a\bar{\alpha}^b = 1$ for integers a and b with a nonzero. Taking the norm to $\mathbf{Q}$ yields $\mathrm{N}_{K/\mathbf{Q}}(\alpha)^{a+b} = 1$. In case that $a+b=0$, we find α^a to be rational, so the order of α in $(\mathcal{O}/p\mathcal{O})^*$ divides $a(p-1)$. Otherwise, we have $\mathrm{N}_{K/\mathbf{Q}}(\alpha) = \pm 1$ and, as $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is congruent to α^{p+1} modulo $p\mathcal{O}$, the order of α in $(\mathcal{O}/p\mathcal{O})^*$ is at most $2(p+1)$. The set S^- is clearly finite in both cases.

For a generic prime $p \neq 3$ that is inert in $K/\mathbf{Q}$, the order p^2-1 of the cyclic group $(\mathcal{O}/p\mathcal{O})^*$ is divisible by 3. If α is a cube in K^*, its order in $(\mathcal{O}/p\mathcal{O})^*$ divides $(p^2-1)/3$, hence S^- is a finite set.

If α has order p^2-1 in $(\mathcal{O}/p\mathcal{O})^*$, we find that $\mathrm{N}_{K/\mathbf{Q}}(\alpha) \equiv \alpha^{p+1} \bmod p\mathcal{O}$ has order $p-1$ in $\mathbf{F}_p^*$. As p is odd, this implies that $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is not a square in $\mathbf{Q}^*$. In other words, if $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is a square in $\mathbf{Q}^*$ then S^- is empty.

Finally assume K is equal to $\mathbf{Q}(\zeta_3)$ and p is a generic prime that is inert in $K/\mathbf{Q}$, so $p \equiv 2 \bmod 3$. Write $\alpha/\bar{\alpha} = \beta^3$ for some $\beta \in K^*$. As β has norm 1, its order modulo $p\mathcal{O}$ divides $p+1$ and hence the order of $\alpha/\bar{\alpha} \bmod p\mathcal{O}$ divides $(p+1)/3$. Using the congruence $\alpha/\bar{\alpha} \equiv \alpha^{1-p} \bmod p\mathcal{O}$ we find that the order of $\alpha \bmod p\mathcal{O}$ is at most $(p^2-1)/3$, hence S^- is empty. □

Apart from the cases listed in proposition 2, there are other situations in which one of the densities vanishes. To state them, we let D be the discriminant of K and we assume that α is not a cube in K^*. This last assumption implies that at least one of the elements $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ or $\alpha/\bar{\alpha}$ is *not* a cube in K^*, and the field k_3 below is well defined. For each prime l define the field k_l as follows:

$$k_l = \begin{cases} \mathbf{Q}(\sqrt{\mathrm{N}_{K/\mathbf{Q}}(\alpha)}) & \text{if } l=2 \text{ and } L_2/\mathbf{Q} \text{ is dihedral of order 8;} \\ \mathbf{Q}(\zeta_3) & \text{if } l=3 \text{ and } \mathrm{N}_{K/\mathbf{Q}}(\alpha) \text{ is a cube in } K^*; \\ \mathbf{Q}(\sqrt{-3D}) & \text{if } l=3 \text{ and } \alpha/\bar{\alpha} \text{ is a cube in } K^*; \\ \mathbf{Q}(\sqrt{5}) & \text{if } l=5 \text{ and } \alpha \text{ is a fifth power in } K^*; \\ K & \text{in all other cases.} \end{cases}$$

For $K \neq \mathbf{Q}(\zeta_3)$ these are quadratic fields. In section 6 we prove the following theorem.

Theorem 3. *Let K, α, S^+ and S^- be as in theorem 1.*

a. *The set S^+ has density* 0*, and is actually finite, if one of the following statements holds:*
   - i. *α satisfies one of the conditions of proposition* 2*a;*
   - ii. *$K = \mathbf{Q}(\sqrt{5})$, α is a* 15*-th power in K^* and $K(\sqrt{\alpha})$ is equal to the maximal real subfield of* $\mathbf{Q}(\zeta_{15})$.

b. *Define the fields k_2, k_3 and k_5 as above. The set S^- has density* 0*, and is actually finite, if one of the following statements holds:*
   - i. *α satisfies one of the conditions of proposition* 2*b;*
   - ii. *Among the fields K, k_2, k_3 and k_5, there exist three different fields whose compositum has degree* 4 *over* $\mathbf{Q}$.

If the generalized Riemann hypothesis holds, these are the only cases in which the density of S^+ or S^- is zero.

We have chosen not to give an explicit formula for c_α^+ and c_α^-, as such a formula will be complicated and not very enlightening. To get a feeling for the problems involved in computing these constants, we will treat some explicit examples in section 7. We gave precise formulas for the density of related sets in [8].

There is an infinite set of α's for which the constants c_α^+ and c_α^- are easily computed. Hooley proved that in the original conjecture the equality $c_\alpha = 1$ holds if and only if α is not a power in $\mathbf{Q}^*$ and the prime 2 is ramified in $\mathbf{Q}(\sqrt{\alpha})$. We have the following similar result.

Theorem 4. *Let K be a quadratic field with composite discriminant and let μ_K be the torsion subgroup of K^*. We assume that α and $\bar{\alpha}$ are multiplicatively independent, that $K^*/\langle\mu_K, \alpha, \bar{\alpha}\rangle$ is torsion free and that the prime 2 is totally ramified in $L_2 = K(\sqrt{\alpha}, \sqrt{\bar{\alpha}})$. If GRH holds, then the densities of S^+ and S^- are given by the following formulas:*

$$\delta(S^+) = \frac{1}{2} \prod_{l \text{ prime}} (1 - \frac{1}{l^2(l-1)}) \approx 0.3487506792,$$

$$\delta(S^-) = \frac{1}{4} \prod_{\substack{l \text{ odd} \\ \text{prime}}} (1 - \frac{2}{l(l-1)}) \approx 0.1337767532.$$

Independently, Yen-Mei J. Chen and Jing Yu have recently proved that, modulo GRH, the set S^- has a density for a restrictive set of imaginary quadratic integers α (private communication, unpublished). For some very specific α's, they showed that this density equals a positive rational multiple of an Euler product as in theorem 1 and 4.

The paper is organized as follows. In section 2, we characterize the primes in S^+ and S^- in terms of their splitting behaviour in the extensions $L_l/\mathbf{Q}$, where l ranges over all primes. These fields $\{L_l\}_l$ tend to be linearly disjoint over K. To make this precise, we study the composita L_n of the fields $\{L_l\}_{l|n}$ in section 3. Here and in the rest of the paper, *the index variable l will always range over prime numbers*. Section 4 contains the analytic part of the proof of theorems 1 and 4: if GRH holds then both S^+ and S^- have a density which is given by an infinite sum similar to (2). The proof of the theorems 1 and 4 is completed in section 5 and theorem 3 is proved in section 6. Finally, in section 7 we compute for some α's the rational constants c_α^- and c_α^+.

2. Splitting conditions

In this section we characterize the primes in S^+ and S^- in terms of their splitting behavior in certain number fields. The order of α modulo a generic prime p is non-maximal if and only if the there exists a prime l such that

(3) l divides $\#(\mathcal{O}/p\mathcal{O})^*$ and α is an l-th power in $(\mathcal{O}/p\mathcal{O})^*$.

Namely, if l satisfies (3) then l divides the exponent of $(\mathcal{O}/p\mathcal{O})^*$ and α has non-maximal order modulo p. To prove the other implication, we assume that the order of α modulo $p\mathcal{O}$ is non-maximal. If p is inert in $K/\mathbf{Q}$, the group $(\mathcal{O}/p\mathcal{O})^*$ is cyclic and any prime divisor $l \mid [(\mathcal{O}/p\mathcal{O})^* : \langle\alpha\rangle]$ satisfies (3). If p splits in $K/\mathbf{Q}$, the group $(\mathcal{O}/p\mathcal{O})^*$ is of exponent $p-1$ as it is isomorphic to the product of two cyclic groups, both of order $p-1$. As α is non-maximal modulo p, there exists a prime $l \mid p-1$ such that the order of α in $(\mathcal{O}/p\mathcal{O})^*$ divides $(p-1)/l$. Therefore, α is an l-th power modulo both primes $\mathfrak{p} \mid p$ in K and l satisfies (3).

If we define the sets

$$S_l^- = \{p \text{ generic prime, inert in } K/\mathbf{Q} \text{ and either } l \nmid \#(\mathcal{O}/p\mathcal{O})^* \\ \text{or } \alpha \notin (\mathcal{O}/p\mathcal{O})^{*l}\}$$

and

$$S_l^+ = \{p \text{ generic prime, splits in } K/\mathbf{Q} \text{ and either } l \nmid \#(\mathcal{O}/p\mathcal{O})^* \\ \text{or } \alpha \notin (\mathcal{O}/p\mathcal{O})^{*l}\}$$

where $(\mathcal{O}/p\mathcal{O})^{*l}$ denotes the subgroup of l-th powers in $(\mathcal{O}/p\mathcal{O})^*$, we find the following equalities:

$$S^- = \bigcap_{l \text{ prime}} S_l^-, \tag{4}$$

$$S^+ = \bigcap_{l \text{ prime}} S_l^+. \tag{5}$$

We can reformulate statement (3) as the complete splitting of $X^l - \alpha$ modulo the prime(s) in $\mathcal{O}$ above p. The set of these prime(s) is stable under the non-trivial automorphism of K. Therefore, if $X^l - \alpha$ splits completely modulo these primes, so does $X^l - \bar{\alpha}$. Here $\bar{\alpha}$ denotes the conjugate of α over $\mathbf{Q}$. This gives the following characterization of the primes which are not in S_l^- or S_l^+.

Proposition 5. *Let l be a prime and define the field L_l as*

$$L_l = K(\zeta_l, \sqrt[l]{\alpha}, \sqrt[l]{\bar{\alpha}}).$$

a. *For a generic prime p that splits in $K/\mathbf{Q}$ the following equivalence holds:*

$$p \notin S_l^+ \iff p \text{ splits completely in } L_l/\mathbf{Q}.$$

b. *For a generic prime p that is inert in $K/\mathbf{Q}$ the following equivalence holds:*

$$p \notin S_l^- \iff p\mathcal{O} \text{ splits completely in } L_l/K.$$

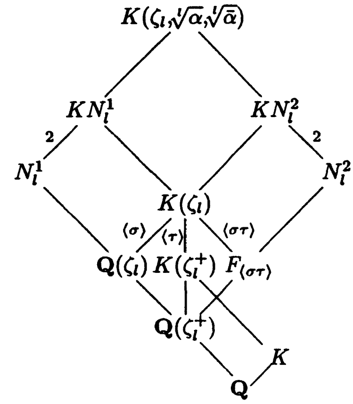
By Chebotarev's density theorem and this proposition, we conclude that the sets S_l^+ and S_l^- have a density in the set of all primes. The same conclusion holds for the finite intersections $S_n^+ = \bigcap_{l|n} S_l^+$ and $S_n^- = \bigcap_{l|n} S_l^-$ for all

$n \in \mathbf{Z}_{>1}$, as the primes in these sets are characterized in terms of their splitting behaviour in the number field L_n, the compositum of the fields $\{L_l\}_{l|n}$. Because of the equalities (4) and (5), the primes in S^+ and S^- are characterized by splitting conditions in the infinite extension L_∞, the compositum of the fields L_l where l ranges over all prime numbers. One would like to prove the existence of the densities of S^+ and S^- by applying a theorem analogous to Chebotarev's density theorem to the field L_∞. However, even the formulation of such a theorem is non-obvious; all primes of L_∞ which do not lie above 2 are ramified and therefore do not have a well-defined Frobenius element.

Our proof of the existence of the density of S^+ and S^- is analogous to Hooley's proof of Artin's original conjecture. The key observation is the following. As S^+ can be seen as a 'limit' of the sets S_n^+, one expects the density of S^+ to be equal to the limit of the densities of the sets S_n^+. A similar observation holds for the set S^-. In section 4 we will adapt Hooley's arguments to our situation, and prove that this limit argument is indeed valid if we assume GRH. This is straightforward for the set S^+, but causes some difficulties for the set S^-. Proposition 5 characterizes the primes p in S_l^- by the property that the Frobenius class of the prime $p\mathcal{O}_K$ of K in L_l/K is non-trivial. In order to adapt Hooley's analytic arguments, we have to characterize the primes in S_l^- as those primes which have a non-trivial Frobenius in extensions of $\mathbf{Q}$.

Proposition 6. *Suppose p is a generic prime, inert in $K/\mathbf{Q}$. Define for each prime l the field $N_l^1 = \mathbf{Q}(\zeta_l, \sqrt[l]{\mathrm{N}_{K/\mathbf{Q}}(\alpha)})$.*

a. *Let l be an odd prime and assume that K is not the quadratic subfield of $\mathbf{Q}(\zeta_l)$. Let N_l^2 be the unique extension of $\mathbf{Q}(\zeta_l + \zeta_l^{-1})$ that contains neither K nor ζ_l and such that $KN_l^2 = K(\zeta_l, \sqrt[l]{\alpha/\bar{\alpha}})$. The fields N_l^1 and N_l^2 are normal over $\mathbf{Q}$ and drawn in the diagram below.*



with:

$$\zeta_l^+ = \zeta_l + \zeta_l^{-1}$$
$$KN_l^1 = K(\zeta_l, \sqrt[l]{\mathrm{N}_{K/\mathbf{Q}}(\alpha)})$$
$$KN_l^2 = K(\zeta_l, \sqrt[l]{\alpha/\bar{\alpha}})$$

The following equivalence holds:

(6) $p \notin S_l^- \iff p$ *splits completely in either* $N_l^1/\mathbf{Q}$ *or* $N_l^2/\mathbf{Q}$.

b. *Assume* $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ *is not a square in* $\mathbf{Q}^*$. *If* $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ *is a square in* K^*, *then* p *is in* S_2^-. *If* $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ *is not a square in* K^*, *then the following equivalence holds:*

$$p \notin S_2^- \iff p \text{ splits completely in } N_2^1/\mathbf{Q}.$$

Proof. We first give a different formulation of proposition 5b in case $p \neq l$. Fix a prime l, and let $p \neq l$ be a generic prime that is inert in $K/\mathbf{Q}$. All primes $\mathfrak{p}$ above p in L_l are unramified, so their Frobenius automorphisms $(\mathfrak{p}, L_l/\mathbf{Q})$ are well-defined. The order of $(\mathfrak{p}, L_l/\mathbf{Q})$ is equal to the residue class degree of $\mathfrak{p}$ in $L_l/\mathbf{Q}$ and independent of the choice of $\mathfrak{p}$ above p. We reformulate proposition 5b for an inert prime $p \neq l$ as follows:

(7) $p \notin S_l^- \iff \exists\, \mathfrak{p} \mid p$ prime in L_l with $(\mathfrak{p}, L_l/\mathbf{Q})$ of order 2.

a. Let l be an odd prime. Because of the equivalence above, we first characterize the elements in $\mathrm{Gal}(L_l/\mathbf{Q})$ of order 2 that are non-trivial on K. Assume ρ is such an element. The restriction $\rho|_{K(\zeta_l)}$ also has order 2 and therefore lies in $\mathrm{Gal}(K(\zeta_l)/\mathbf{Q}(\zeta_l^+))$, the maximal exponent 2 subgroup of $\mathrm{Gal}(K(\zeta_l)/\mathbf{Q})$. Here ζ_l^+ denotes a generator of the maximal real subfield of $\mathbf{Q}(\zeta_l)$. Let τ and σ denote the generators of $\mathrm{Gal}(K(\zeta_l)/K(\zeta_l^+))$ and $\mathrm{Gal}(K(\zeta_l)/\mathbf{Q}(\zeta_l))$ respectively. The assumption $K \not\subset \mathbf{Q}(\zeta_l)$ implies that $\mathrm{Gal}(K(\zeta_l)/\mathbf{Q}(\zeta_l^+)) \cong \langle\sigma\rangle \times \langle\tau\rangle$ is isomorphic to Klein's four group. As ρ is non-trivial on K, we find that $\rho|_{K(\zeta_l)}$ equals σ or $\sigma\tau$. Fix an element $\bar\rho \in \{\sigma, \sigma\tau\}$ and define $F_{\bar\rho}$ as the fixed field of $\bar\rho$. Consider the following exact sequence:

$$1 \longrightarrow \mathrm{Gal}(L_l/K(\zeta_l)) \longrightarrow \mathrm{Gal}(L_l/F_{\bar\rho}) \longrightarrow \mathrm{Gal}(K(\zeta_l)/F_{\bar\rho}) = \langle\bar\rho\rangle \longrightarrow 1.$$

The group $\mathrm{Gal}(L_l/K(\zeta_l))$ has odd exponent, hence any element of order 2 in $\mathrm{Gal}(L_l/F_{\bar\rho})$ restricts to $\bar\rho$. This proves that the sequence splits and that there indeed exist elements $\rho \in \mathrm{Gal}(L_l/\mathbf{Q})$ of order 2 that are non-trivial on K. We fix an isomorphism

$$\mathrm{Gal}(L_l/F_{\bar\rho}) \cong \mathrm{Gal}(L_l/K(\zeta_l)) \rtimes \langle\bar\rho\rangle.$$

The abelian group $G = \mathrm{Gal}(L_l/K(\zeta_l))$ is a module over the group ring $\mathbf{F}_l[\langle\bar\rho\rangle]$. Because l is odd, there is a decomposition $G = H_{\bar\rho}^+ \times H_{\bar\rho}^-$, with

$$H_{\bar\rho}^+ = \{h \in G : h^{1-\bar\rho} = \mathrm{id}\} \quad\text{and}\quad H_{\bar\rho}^- = \{h \in G : h^{1+\bar\rho} = \mathrm{id}\}.$$

The element $\bar\rho$ acts trivially on $H_{\bar\rho}^+$ and by inversion on $H_{\bar\rho}^-$. We conclude that $\rho \in \mathrm{Gal}(L_l/\mathbf{Q})$ is of order 2 and non-trivial on K if and only if

(8) $$\bar\rho = \rho|_{K(\zeta_l)} \in \{\sigma, \sigma\tau\} \quad\text{and}\quad \rho \in H_{\bar\rho}^- \rtimes \langle\bar\rho\rangle.$$

By definition of $H_{\bar{\rho}}^{-}$, the group $G/(H_{\bar{\rho}}^{-} \rtimes \langle\bar{\rho}\rangle)$ is the maximal quotient of G that is abelian of exponent l. In particular, $H_{\bar{\rho}}^{-} \rtimes \langle\bar{\rho}\rangle$ is a characteristic subgroup of G and therefore normal in $\mathrm{Gal}(L_l/\mathbf{Q})$.

Now we are able to prove the equivalence (6). Define the normal fields N_l^1 and N_l^2 as the fixed fields of $H_\sigma^- \rtimes \langle\sigma\rangle$ and $H_{\sigma\tau}^- \rtimes \langle\sigma\tau\rangle$, respectively. Let $p \neq l$ be a generic prime that is inert in $K/\mathbf{Q}$ and choose a prime $\mathfrak{p}$ above p in L_l. By the equivalence (7) and the characterization (8), we find that $p \notin S_l^-$ if and only if the Frobenius automorphism of $\mathfrak{p}$ in $L_l/\mathbf{Q}$ lies either in $H_\sigma^- \rtimes \langle\sigma\rangle$ or in $H_{\sigma\tau}^- \rtimes \langle\sigma\tau\rangle$. In other words, the prime p is not in S_l^- if and only if p splits completely in either $N_l^1/\mathbf{Q}$ or $N_l^2/\mathbf{Q}$. If $p = l$ is generic and inert in $K/\mathbf{Q}$, then l does not divide $\#(\mathcal{O}/l\mathcal{O})^*$ and is therefore contained in S_l^-. On the other hand, the prime l ramifies in both $N_l^1/\mathbf{Q}$ and $N_l^2/\mathbf{Q}$, hence does not split completely in either of these extensions.

To determine the fields N_l^1 and N_l^2, we have to understand the conjugation action of σ and $\sigma\tau$ on $\mathrm{Gal}(L_l/K(\zeta_l))$. This can be done by considering the Galois equivariant, bilinear and non-degenerate Kummer pairing:

$$\begin{array}{ccc} \mathrm{Gal}(L_l/K(\zeta_l)) \times \langle\alpha,\bar{\alpha}\rangle K(\zeta_l)^{*l}/K(\zeta_l)^{*l} & \longrightarrow & \langle\zeta_l\rangle \\ (h,x) & \longmapsto & \langle h,x\rangle = \frac{h(\sqrt[l]{x})}{\sqrt[l]{x}} \end{array}$$

Using the fact that σ acts trivially on ζ_l and interchanges α and $\bar{\alpha}$, we find for $h \in \mathrm{Gal}(L_l/K(\zeta_l))$ the following equivalences:

$$\begin{aligned} h^{1+\sigma} = \mathrm{id} &\Longleftrightarrow \langle h^{1+\sigma}, \alpha^a\bar{\alpha}^b\rangle = 1 \ \ \forall a,b \in \mathbf{Z} \\ &\Longleftrightarrow \langle h, \alpha^a\bar{\alpha}^b\rangle \cdot \sigma\langle h, \sigma(\alpha^a\bar{\alpha}^b)\rangle = 1 \ \ \forall a,b \in \mathbf{Z} \\ &\Longleftrightarrow \langle h, \alpha^a\bar{\alpha}^b\rangle \cdot \langle h, \alpha^b\bar{\alpha}^a\rangle = 1 \ \ \forall a,b \in \mathbf{Z} \\ &\Longleftrightarrow \langle h, \mathrm{N}_{K/\mathbf{Q}}(\alpha)\rangle^{a+b} = 1 \ \ \forall a,b \in \mathbf{Z} \\ &\Longleftrightarrow \langle h, \mathrm{N}_{K/\mathbf{Q}}(\alpha)\rangle = 1. \end{aligned}$$

Therefore, the group H_σ^- corresponds to the field $K(\zeta_l, \sqrt[l]{\mathrm{N}_{K/\mathbf{Q}}(\alpha)})$. Taking the invariants under σ yields $N_l^1 = \mathbf{Q}(\zeta_l, \sqrt[l]{\mathrm{N}_{K/\mathbf{Q}}(\alpha)})$.

As τ fixes α and inverts ζ_l we find:

$$\begin{aligned} h^{1+\sigma\tau} = \mathrm{id} &\Longleftrightarrow \langle h^{1+\sigma\tau}, \alpha^a\bar{\alpha}^b\rangle = 1 \ \ \forall a,b \in \mathbf{Z} \\ &\Longleftrightarrow \langle h, \alpha^a\bar{\alpha}^b\rangle \cdot \sigma\tau\langle h, \sigma\tau(\alpha^a\bar{\alpha}^b)\rangle = 1 \ \ \forall a,b \in \mathbf{Z} \\ &\Longleftrightarrow \langle h, \alpha^a\bar{\alpha}^b\rangle \cdot \langle h, \alpha^b\bar{\alpha}^a\rangle^{-1} = 1 \ \ \forall a,b \in \mathbf{Z} \\ &\Longleftrightarrow \langle h, \frac{\alpha}{\bar{\alpha}}\rangle^{a+b} = 1 \ \ \forall a,b \in \mathbf{Z} \\ &\Longleftrightarrow \langle h, \frac{\alpha}{\bar{\alpha}}\rangle = 1. \end{aligned}$$

The fixed field $K(\zeta_l, \sqrt[l]{\frac{\alpha}{\bar\alpha}})$ of $H^-_{\sigma\tau}$ is a quadratic extension of N_l^2. As $\sigma\tau$ is non-trivial on both K and ζ_l, the field N_l^2 does contain neither of them and $KN_l^2 = K(\zeta_l, \sqrt[l]{\frac{\alpha}{\bar\alpha}})$. On the other hand, any extension N of $\mathbf{Q}(\zeta_l^+)$ that contains neither K nor ζ_l and for which $[K(\zeta_l, \sqrt[l]{\frac{\alpha}{\bar\alpha}}) : N] = 2$ is an exponent l extension of $F_{\sigma\tau}$ and hence equal to N_l^2. This concludes the proof of 6a.

b. Assume p is a generic prime, inert in $K/\mathbf{Q}$. The degree of $L_2 = K(\sqrt{\alpha}, \sqrt{\bar\alpha})$ divides 8. If $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is a square in K^* but not a square in $\mathbf{Q}^*$, then $L_2/\mathbf{Q}$ is cyclic of degree 4. The Frobenius of all $\mathfrak{p} \mid p$ in $L_2/\mathbf{Q}$ have order 4 and the equivalence (7) implies that p is an element of S_2^-.

If $\mathrm{N}(\alpha) = \mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is not a square in K^*, then $L_2/\mathbf{Q}$ is dihedral of degree 8, and the Galois group of both L_2/K and $L_2/\mathbf{Q}(\sqrt{\mathrm{N}(\alpha)})$ is isomorphic to Klein's four group. If p splits in $\mathbf{Q}(\sqrt{\mathrm{N}(\alpha)})$, all $\mathfrak{p} \mid p$ in L_2 have a Frobenius of order 2 and p is not an element of S_2^-. On the other hand, if p is inert in $K/\mathbf{Q}$ and in $\mathbf{Q}(\sqrt{\mathrm{N}(\alpha)})/\mathbf{Q}$, it splits in the third quadratic field $\mathbf{Q}(\sqrt{D \cdot \mathrm{N}(\alpha)}) \subset K(\sqrt{\mathrm{N}(\alpha)})$, where D denotes the discriminant of K. As $L_2/\mathbf{Q}(\sqrt{D \cdot \mathrm{N}(\alpha)})$ is cyclic of order 4 and the primes above p are inert in $K(\sqrt{\mathrm{N}(\alpha)})/\mathbf{Q}(\sqrt{D \cdot \mathrm{N}(\alpha)})$, the Frobenius of all $\mathfrak{p} \mid p$ in $L_2/\mathbf{Q}$ have order 4 and p is in S_2^-. □

The proof of proposition 6 yields the following corollary, which we need in the proof of proposition 19 in section 6.

Corollary 7. *Let l be an odd prime and let $\rho \in \mathrm{Gal}(L_l/\mathbf{Q})$ be non-trivial on K such that $\rho|_{K(\zeta_l)}$ has order 2. Furthermore define the set*

$$C_l = \{\lambda \in \mathrm{Gal}(L_l/\mathbf{Q}) : \lambda|_K \neq id \text{ and } \lambda^2 = id\}.$$

If K is not contained in $\mathbf{Q}(\zeta_l)$ then the following equivalence holds:

$$\rho \in C_l \Longleftrightarrow \rho|_{N_{l,\rho}} = \mathrm{id},$$

where $N_{l,\rho}$ is the unique field in $\{N_l^1, N_l^2\}$ that contains the fixed field of $\rho|_{K(\zeta_l)}$. The set C_l has cardinality

$$c(l) = [L_l : K(\zeta_l, \sqrt[l]{\mathrm{N}_{K/\mathbf{Q}}(\alpha)}] + [L_l : K(\zeta_l, \sqrt[l]{\frac{\alpha}{\bar\alpha}})].$$

Proof. We use the notation from the proof of proposition 6. Let $\rho \in \mathrm{Gal}(L_l/\mathbf{Q})$ be non-trivial on K, and of order 2 when restricted to $K(\zeta_l)$. By construction exactly one of the fields N_l^1 and N_l^2 contains the fixed field of $\rho|_{K(\zeta_l)}$, so $N_{l,\rho}$ is well defined. In the proof of proposition 6 we saw that ρ has order 2 if and only if ρ is trivial on N_l^1 or N_l^2. As K is contained in the compositum of these fields, the element ρ can not be trivial on both, and the equivalence is proved.

To compute $c(l)$, we use the characterization (8) of elements in C_l and find $c(l) = \#H^-_\sigma + \#H^-_{\sigma\tau}$. The orders of H^-_σ and $H^-_{\sigma\tau}$ are equal to the degrees of L_l over KN_l^1 and KN_l^2 respectively. Using the definitions of N_l^1 and N_l^2 yields the desired result. □

By Chebotarev's density theorem and proposition 5 we find for each prime l the following formulas:

$$\text{(9)} \qquad \begin{aligned}\delta(S_l^+) &= \frac{\#\{\sigma \in \mathrm{Gal}(L_l/\mathbf{Q}) : \sigma|_K = \mathrm{id} \text{ and } \sigma \neq \mathrm{id}\}}{[L_l : \mathbf{Q}]}\\ &= \frac{1}{2}(1 - \frac{1}{[L_l : K]}).\end{aligned}$$

$$\text{(10)} \qquad \begin{aligned}\delta(S_l^-) &= \frac{\#\{\sigma \in \mathrm{Gal}(L_l/\mathbf{Q}) : \sigma|_K \neq \mathrm{id} \text{ and } \sigma^2 \neq \mathrm{id}\}}{[L_l : \mathbf{Q}]}\\ &= \frac{\#\{\sigma \in \mathrm{Gal}(L_l/\mathbf{Q}) : \sigma|_K \neq \mathrm{id}\} - c(l)}{[L_l : \mathbf{Q}]}\\ &= \frac{1}{2}(1 - \frac{c(l)}{[L_l : K]}).\end{aligned}$$

Here $c(l)$ denotes the cardinality of the set C_l, which was defined in corollary 7. In the proof of theorem 1, we need to know the values of these densities. It turns out that for all but finitely many primes l, these densities have a generic description in terms of l.

Proposition 8. *Let r be the free rank of $\langle \alpha, \bar{\alpha} \rangle$ and let t be the order of the torsion subgroup of $K^*/\langle \alpha, \bar{\alpha} \rangle$.*

a. *In each of the following cases $\delta(S_l^+)$ is positive:* (i) *$l \geq 5$ prime;* (ii) *$l = 3$ and $K \neq \mathbf{Q}(\zeta_3)$;* (iii) *$l = 2$ and $\alpha \notin K^{*2}$.*
For all primes $l \nmid 2t$ such that $K \not\subset \mathbf{Q}(\zeta_l)$ we have $[L_l : K] = (l-1)l^r$.

b. *In each of the following cases $\delta(S_l^-)$ is positive:* (i) *$l \geq 5$ prime;* (ii) *$l = 3$, $K \neq \mathbf{Q}(\zeta_3)$ and $\alpha \notin K^{*3}$;* (iii) *$l = 2$ and $\mathrm{N}_{K/\mathbf{Q}}(\alpha) \notin \mathbf{Q}^{*2}$.*
If r equals 2 and $l \nmid 2t$ is a prime such that $K \not\subset \mathbf{Q}(\zeta_l)$, then we have $\frac{c(l)}{[L_l:K]} = \frac{2}{l(l-1)}$ and both N_l^1 and N_l^2 are of degree $l(l-1)$ over $\mathbf{Q}$.

Proof. a. As $\mathbf{Q}(\zeta_l)$ is contained in L_l , we have $[L_l : K] \geq [K(\zeta_l) : K] \geq 2$ for all primes $l \geq 5$. The same inequality holds for $l = 3$, provided K is not equal to $\mathbf{Q}(\zeta_3)$. If α is not a square in K^*, the extension L_2/K is also of degree at least 2. In all these cases, the set S_l^+ has positive density by formula (9).

The fact the t is finite is well known. Let $l \nmid 2t$ be a prime such that K is not contained in $\mathbf{Q}(\zeta_l)$. The last condition on l implies $[L_l : K] = [L_l : K(\zeta_l)][K(\zeta_l) : K] = (l-1)[L_l : K(\zeta_l)]$. By Kummer theory, the degree $[L_l : K(\zeta_l)]$ equals the cardinality of the image of $W = \langle \alpha, \bar{\alpha} \rangle$ in $K(\zeta_l)^*/K(\zeta_l)^{*l}$. We compute this cardinality in two steps.

First we show that the map

$$K^*/K^{*l} \longrightarrow K(\zeta_l)^*/K(\zeta_l)^{*l}$$

is injective. Namely, if $x \bmod K^{*l}$ is in the kernel, we can write $x = y^l$ for some $y \in K(\zeta_l)^*$. Applying the norm map from $K(\zeta_l)$ to K yields the equality $x^{[K(\zeta_l):K]} = \mathrm{N}_{K(\zeta_l)/K}(y)^l$. We find that x is trivial in K^*/K^{*l}, as its order divides both l and $[K(\zeta_l) : K]$.

If we can write $w = y^l$ for some $w \in W$ and $y \in K^*$, the image of y in K^*/W is an l-torsion element. As we assumed that l does not divide the order of the torsion subgroup of K^*/W , we find that y is in W and the map

$$W/W^l \longrightarrow K^*/K^{*l},$$

is injective.

With these two observations, we find that the degree $[L_l : K(\zeta_l)]$ is equal to the index $[W : W^l]$. As K is by assumption not contained in $\mathbf{Q}(\zeta_l)$ and l is odd, the group W has no non-trivial l-torsion. Therefore we have $[W : W^l] = l^r$ and we conclude that L_l is of degree $(l-1)l^r$ over K.

b. Let l be an odd prime and assume that K is not contained in $\mathbf{Q}(\zeta_l)$. By corollary 7 we have

$$\frac{c(l)}{[L_l : K]} = \frac{1}{(l-1)[K(\zeta_l, \sqrt[l]{\mathrm{N}_{K/\mathbf{Q}}(\alpha)}) : K(\zeta_l)]} + \frac{1}{(l-1)[K(\zeta_l, \sqrt[l]{\frac{\alpha}{\bar\alpha}}) : K(\zeta_l)]}.$$

This implies the inequalities $\frac{c(l)}{[L_l:K]} \le \frac{1}{2}$ for $l \ge 5$. In case α is not a cube in K^*, at least one of the elements $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ or $\frac{\alpha}{\bar\alpha}$ is not a cube in K^* and we find the upper bound $c(3)/[L_3 : K] \le 2/3$. Using formula (10), we see that in these cases S_l^- has positive density. The result for $\delta(S_2^-)$ follows immediately from proposition 6b.

If α and $\bar\alpha$ are multiplicatively independent and the prime l does not divide $2t$, then $\{\alpha, \bar\alpha\}$ forms an $\mathbf{F}_l$-basis for $WK(\zeta_l)^{*l}/K(\zeta_l)^{*l}$ by the proof of proposition 8a. In particular, neither $\alpha\bar\alpha$ nor $\frac{\alpha}{\bar\alpha}$ is an l-th power in $K(\zeta_l)^*$ and by Kummer theory, both $KN_l^1 = K(\zeta_l, \sqrt[l]{\mathrm{N}_{K/\mathbf{Q}}(\alpha)})$ and $KN_l^2 = K(\zeta_l, \sqrt[l]{\frac{\alpha}{\bar\alpha}})$ are of degree l over $K(\zeta_l)$. Substituting this in the above equality yields the result for $c(l)/[L_l : K]$. The field K is linearly disjoint from both N_l^1 and $\mathbf{Q}(\zeta_l)$ so we find $[N_l^1 : \mathbf{Q}] = [KN_l^1 : K] = l \cdot [K(\zeta_l) : K] = l(l-1)$. The same equality holds if we replace N_l^1 by N_l^2.

To conclude the proof of proposition 8b, we have to prove $\delta(S_l^-) > 0$ in case K is contained in $\mathbf{Q}(\zeta_l)$ for some prime $l \ge 5$. This is left to the reader. □

3. The Galois structure of $L_n/\mathbf{Q}$

As we already noted in the last section, the finite intersections $S_n^+ = \bigcap_{l|n} S_l^+$ and $S_n^- = \bigcap_{l|n} S_l^-$ have a density. These can can be computed by Chebotarev's density theorem, in the same way as we computed $\delta(S_l^+)$ and $\delta(S_l^-)$ in (9) and (10). Using the principle of inclusion and exclusion, we find the following formulas:

$$\delta(S_n^+) = \sum_{d|n} \frac{\mu(d)}{[L_d : \mathbf{Q}]}, \tag{11}$$

with L_d the compositum of the fields $\{L_l\}_{l|d}$ and $L_1 = K$, and

$$\delta(S_n^-) = \sum_{d|n} \frac{\mu(d)c(d)}{[L_d : \mathbf{Q}]}, \tag{12}$$

with $c(d) = \#\{\sigma \in \mathrm{Gal}(L_d/\mathbf{Q}) : \sigma|_K \neq \mathrm{id} \text{ and } \sigma^2 = \mathrm{id}\}$. In the next section, we will prove that if GRH is true, these formulas also hold if we take the limit $n = \prod_{l<x} l \to \infty$, thereby proving the existence of $\delta(S^+)$ and $\delta(S^-)$. It is not clear from (11) and (12), whether these densities are positive. If the fields $\{L_l/K\}_{l|d}$ are linearly disjoint over K, the summands of (11) and (12) are multiplicative in d and we obtain product expressions for the densities of S_n^+ and S_n^-. In this case it is easy to conclude whether these densities vanish. However, the fields $\{L_l/K\}_{l|d}$ are not in general linearly disjoint over K. For example, if $K = \mathbf{Q}(\sqrt{-15})$ the field $\mathbf{Q}(\sqrt{5}, \sqrt{-3})$ is contained in both L_3 and L_5.

Proposition 10 below shows that the fields $\{L_l\}_l$ are not too far from being linearly disjoint over K. We will need the following lemma.

Lemma 9. *Let $F/\mathbf{Q}$ be a finite abelian extension of exponent e. If n and m are relatively prime integers then $F(\zeta_n) \cap F(\zeta_m)$ is also of exponent e over $\mathbf{Q}$.*

Proof. As F is contained in the intersection, it is sufficient to prove that the exponent of $F(\zeta_n) \cap F(\zeta_m)$ divides e. Recall that the character group $X(L)$ of an abelian number field L is defined as the group of homomorphisms $\mathrm{Gal}(L/\mathbf{Q}) \to \mathbf{C}^*$, and that $X(L)$ is (non-canonically) isomorphic to $\mathrm{Gal}(L/\mathbf{Q})$. It is therefore sufficient to prove that the order of ψ divides e for all $\psi \in X(F(\zeta_n) \cap F(\zeta_m))$. As ψ is both in $X(F(\zeta_n))$ and in $X(F(\zeta_m))$ we can write $\psi = \chi_1\rho_1$ and $\psi = \chi_2\rho_2$ with $\chi_1 \in X(\mathbf{Q}(\zeta_n))$, $\chi_2 \in X(\mathbf{Q}(\zeta_m))$, and $\rho_1, \rho_2 \in X(F)$. The element $\rho_1^{-1}\rho_2 = \chi_1\chi_2^{-1}$ is in $X(F)$, so its order divides e. As $\mathbf{Q}(\zeta_n)$ and $\mathbf{Q}(\zeta_m)$ are linearly disjoint over $\mathbf{Q}$, the group $X(\mathbf{Q}(\zeta_{nm}))$ is isomorphic to $X(\mathbf{Q}(\zeta_n)) \times X(\mathbf{Q}(\zeta_m))$ and the order of χ_1 divides that of $\chi_1\chi_2^{-1}$. Consequently, the order of ψ, which divides the least common multiple of the orders of χ_1 and ρ_1, divides e. □

For any number field F, we denote by F^{ab} the maximal subfield of F that is abelian over $\mathbf{Q}$. For integers k and n, we denote their greatest common divisor by (k,n).

Proposition 10. *For all positive integers n, let L_n be the compositum of the fields $\{L_l\}_{l|n}$. Define the integer f as follows:*

$$f = \begin{cases} \textit{conductor of } L_2^{\mathrm{ab}}/\mathbf{Q} & \textit{if } K \neq \mathbf{Q}(\zeta_3); \\ \textit{conductor of } L_6^{\mathrm{ab}}/\mathbf{Q} & \textit{if } K = \mathbf{Q}(\zeta_3). \end{cases}$$

For all positive squarefree integers n and m that are relatively prime, the following statements hold:

a. $L_n = K(\zeta_n, \sqrt[n]{\alpha}, \sqrt[n]{\bar{\alpha}})$.

b. $L_n \cap L_m = L_n^{\mathrm{ab}} \cap L_m^{\mathrm{ab}}$.

c. $L_n^{\mathrm{ab}} = \begin{cases} L_{(2,n)}^{\mathrm{ab}}(\zeta_n) & \textit{if } K \neq \mathbf{Q}(\zeta_3); \\ L_{(6,n)}^{\mathrm{ab}}(\zeta_n) & \textit{if } K = \mathbf{Q}(\zeta_3). \end{cases}$

d. $L_n \cap L_m$ *is abelian over* $\mathbf{Q}$ *of exponent dividing* e*, with*

$$e = \begin{cases} 6 & \textit{if } 3 \mid nm \textit{ and } K = \mathbf{Q}(\zeta_3); \\ 4 & \textit{if } 2 \mid nm \textit{ and } L_2^{\mathrm{ab}}/\mathbf{Q} \textit{ is of exponent } 4; \\ 2 & \textit{otherwise.} \end{cases}$$

e. $L_n \cap L_m = K = L_n \cap L_{2f}$*, if nm and $2f$ are relatively prime.*

f. $L_n \cap L_m = K$*, if the prime 2 ramifies completely in $L_2^{\mathrm{ab}}/\mathbf{Q}$.*

Proof. For a prime l, the field L_l is defined by $K(\zeta_l, \sqrt[l]{\alpha}, \sqrt[l]{\bar{\alpha}})$ and 10a follows immediately.

The degree $[(L_n \cap L_m) : (L_n^{\mathrm{ab}} \cap L_m^{\mathrm{ab}})]$ divides both $[L_n : L_n^{\mathrm{ab}}]$ and $[L_m : L_m^{\mathrm{ab}}]$. As L_k^{ab} contains $K(\zeta_k)$ for each squarefree integer k, we find that $[L_n : L_n^{\mathrm{ab}}]$ and $[L_m : L_m^{\mathrm{ab}}]$ divide n^2 and m^2, respectively. Using the assumption that n and m are relatively prime, this proves 10b.

In order to prove 10c, we first show that for an odd prime l the field L_l^{ab} coincides with $K(\zeta_l)$, unless both K is equal to $\mathbf{Q}(\zeta_3)$ and l is equal to 3. The extension $L_l/K(\zeta_l)$ is a Kummer extension of degree dividing l^2. The intermediate fields of this extension are of the form $K(\zeta_l, \sqrt[l]{W})$, where W is a subgroup of $\langle \alpha, \bar{\alpha} \rangle$, the multiplicative subgroup of K^* generated by α and $\bar{\alpha}$. If L_l^{ab} is strictly larger than $K(\zeta_l)$, there exists a $\beta \in \langle \alpha, \bar{\alpha} \rangle$, not an l-th power in $K(\zeta_l)^*$, such that $K(\zeta_l, \sqrt[l]{\beta})$ is abelian over $\mathbf{Q}$. As a consequence, the l-extension $K(\sqrt[l]{\beta})/K$ is normal, which forces a primitive l-th root of unity ζ_l to lie in $K(\sqrt[l]{\beta})$. Because l is relatively prime to the degree of ζ_l over K, the l-th roots of unity are contained in K. If K is not equal to $\mathbf{Q}(\zeta_3)$ or l is not 3, this is a contradiction and we find $L_l^{\mathrm{ab}} = K(\zeta_l)$. For $K = \mathbf{Q}(\zeta_3)$ we use the Kummer pairing as in the proof of proposition 6 and find that L_3^{ab} is equal to $\mathbf{Q}(\zeta_3, \sqrt[3]{W})$, with W the largest subgroup of

$\langle \alpha, \bar{\alpha} \rangle$ on which $\mathrm{Gal}(\mathbf{Q}(\zeta_3)/\mathbf{Q})$ acts by inversion. This yields the equality $L_3^{\mathrm{ab}} = \mathbf{Q}(\zeta_3, \sqrt[3]{\frac{\alpha}{\bar{\alpha}}})$, a cyclic extension of $\mathbf{Q}$ of exponent dividing 6.

For the general case, we abbreviate the compositum of the fields $\{L_l^{\mathrm{ab}}\}_{l|n}$ by M_n, which is clearly contained in L_n^{ab}. Restricting automorphisms gives the following injective map:

$$\mathrm{Gal}(L_n/M_n) \xrightarrow{\phi} \prod_{\substack{l|n \\ \text{prime}}} \mathrm{Gal}(L_l/L_l^{\mathrm{ab}}).$$

Injectivity follows from the fact that the fields $\{L_l\}_{l|n}$ generate L_n. As the intersection $L_n^{\mathrm{ab}} \cap L_l$ equals L_l^{ab} for $l \mid n$, the image of the subgroup $\mathrm{Gal}(L_n/L_n^{\mathrm{ab}}) \subset \mathrm{Gal}(L_n/M_n)$ maps surjectively to each component. For different primes l, the groups $\mathrm{Gal}(L_l/L_l^{\mathrm{ab}})$ have relatively prime orders, as L_l/L_l^{ab} is an l-extension for all l. Consequently, the group $\mathrm{Gal}(L_n/L_n^{\mathrm{ab}})$ maps surjectively to the product, the map ϕ is an isomorphism and L_n^{ab} equals M_n. This proves 10c.

The number e in 10d is well defined. Namely, if K is equal to $\mathbf{Q}(\zeta_3)$ then $L_2^{\mathrm{ab}}/\mathbf{Q}$ is of exponent 2; if L_2^{ab} would be cyclic of degree 4 over $\mathbf{Q}$, its unique quadratic subfield K would be real. To prove 10d we assume that K is not equal to $\mathbf{Q}(\zeta_3)$, that m is odd and n even; the other cases are similar and left to the reader. Using 10b and 10c we see that $L_n \cap L_m$ is contained in $L_2^{\mathrm{ab}}(\zeta_n) \cap K(\zeta_m) \subset L_2^{\mathrm{ab}}(\zeta_n) \cap L_2^{\mathrm{ab}}(\zeta_m)$. Statement 10d follows by applying lemma 9 with $F = L_2^{\mathrm{ab}}$, a field of exponent 2 or 4 over $\mathbf{Q}$

As K is contained in L_2^{ab}, the conductor D of K divides f. Note that if K is equal to $\mathbf{Q}(\zeta_3)$, then f is a multiple of 3. Assume nm and $2f$ are relatively prime, hence K is not contained in $\mathbf{Q}(\zeta_{nm})$ and the fields $K(\zeta_n)$ and $K(\zeta_m)$ are linearly disjoint over K. Using 10b and 10c we find the equality $L_n \cap L_m = K$. To prove the second equality in 10e, we first note that the definition of L_{2f} only depends on the squarefree part of $2f$. With this in mind, we again use 10b and 10c and find:

$$L_n \cap L_{2f} = L_n^{\mathrm{ab}} \cap L_{2f}^{\mathrm{ab}} \subset K(\zeta_n) \cap \mathbf{Q}(\zeta_f).$$

As n and f are relatively prime, the field K is contained in $\mathbf{Q}(\zeta_f)$ but not in $\mathbf{Q}(\zeta_n)$ and an easy computation shows that the degree of $K(\zeta_n) \cap \mathbf{Q}(\zeta_f)$ is 2. As K is contained in this intersection, we find $L_n \cap L_{2f} = K$.

To prove 10f, it is sufficient to prove the equality $L_n \cap L_{2m} = K$, for odd, squarefree and relatively prime integers n and m. Assume that the prime 2 ramifies completely in $L_2^{\mathrm{ab}}/\mathbf{Q}$, hence it ramifies in all subfields of L_2^{ab}. Therefore, the fields L_2^{ab} and $\mathbf{Q}(\zeta_{nm})$ are linearly disjoint over $\mathbf{Q}$ and, as $K \subset L_2^{\mathrm{ab}}$, so are K and $\mathbf{Q}(\zeta_{nm})$. Furthermore, as 2 is unramified in $\mathbf{Q}(\zeta_3)$, the field K is not equal to $\mathbf{Q}(\zeta_3)$. Using 10b and 10c we find the following equalities:

$$[(L_n \cap L_{2m}) : \mathbf{Q}] = [(K(\zeta_n) \cap L_2^{\mathrm{ab}}(\zeta_m)) : \mathbf{Q}] = \frac{[K(\zeta_n) : \mathbf{Q}][L_2^{\mathrm{ab}}(\zeta_m) : \mathbf{Q}]}{[L_2^{\mathrm{ab}}(\zeta_{nm}) : \mathbf{Q}]} = 2.$$

As K is a subfield of $L_n \cap L_{2m}$, this proves the last statement of the proposition. □

Corollary 11. *Let r be the free rank of $\langle \alpha, \bar{\alpha} \rangle$. There exists a positive constant κ_1, depending on α, such that for all positive squarefree integers n the following inequalities hold:*

$$\kappa_1 n^r \varphi(n) \le [L_n : K] \le n^2 \varphi(n)$$

Assume that α and $\bar{\alpha}$ are multiplicatively independent and define for each positive squarefree integer n the number $c(n) = \#\{\sigma \in \mathrm{Gal}(L_n/\mathbf{Q}) : \sigma|_K \neq \mathrm{id}, \sigma^2 = \mathrm{id}\}$. For all $\varepsilon > 0$ there exists a constant κ_2, depending on ε and α, such that for all positive squarefree integers n the following inequality holds:

$$\frac{c(n)}{[L_n : K]} \le \frac{\kappa_2}{n^{2-\varepsilon}}.$$

Proof. The upper bound for $[L_n : K]$ follows easily from proposition 10a. To obtain the lower bound, let n_0 be the maximal divisor of n prime to $2tf$. Here f is defined as in proposition 10 and t is the order of the torsion subgroup of $K^*/\langle \alpha, \bar{\alpha} \rangle$. Note that, as n is squarefree, the quotient n/n_0 is bounded by $2tf$. By proposition 10e, the fields $\{L_l\}_{l|n_0}$ are linearly disjoint over K. By Galois theory, the group $\mathrm{Gal}(L_{n_0}/\mathbf{Q})$ is canonical isomorphic to the fibred product of the groups $\{\mathrm{Gal}(L_l/\mathbf{Q})\}_{l|n_0}$ over $\mathrm{Gal}(K/\mathbf{Q})$. As a consequence we find the equalities $c(n_0) = \prod_{l|n_0} c(l)$ and $[L_{n_0} : K] = \prod_{l|n_0} [L_l : K]$. Applying proposition 8a yields

$$[L_n : K] \ge [L_{n_0} : K] = \prod_{l|n_0} l^r(l-1) = n_0^r \varphi(n_0) \ge \kappa_1 n^r \varphi(n),$$

with $\kappa_1 = (2tf)^{-r} \varphi(2tf)^{-1}$ independent of n.

Using proposition 10e and 8b we find that for each $\varepsilon > 0$ there exist constants κ_2 and κ_2' such that the following holds:

$$\frac{c(n)}{[L_n : K]} \le \frac{c(n_0)[L_n : L_{n_0}]}{[L_n : K]} = \frac{c(n_0)}{[L_{n_0} : K]} = \prod_{l|n_0} \frac{c(l)}{[L_l : K]} = \prod_{l|n_0} \frac{2}{l(l-1)}$$

$$\le \kappa_2' \prod_{l|n} \frac{2}{l(l-1)} \le \kappa_2 \prod_{l|n} \frac{1}{l^{2-\epsilon}} = \frac{\kappa_2}{n^{2-\epsilon}}.$$

□

Using proposition 10, we are now able to describe $\mathrm{Gal}(L_n/\mathbf{Q})$ in terms of the groups $\{\mathrm{Gal}(L_l/\mathbf{Q})\}_{l|n}$. This will be used in the proof of theorem 3.

Proposition 12. *Let n be a positive squarefree integer and define*

$$e = \begin{cases} 6 & \textit{if } 3 \mid n \textit{ and } K = \mathbf{Q}(\zeta_3); \\ 4 & \textit{if } 2 \mid n \textit{ and } L_2^{\mathrm{ab}}/\mathbf{Q} \textit{ is of exponent } 4; \\ 2 & \textit{otherwise.} \end{cases}$$

Let M be the compositum of the fields $\{M_l\}_{l|n}$, where M_l is the maximal subfield of L_l that is abelian over $\mathbf{Q}$ and of exponent dividing e. Then the fields $\{ML_l\}_{l|n}$ are linearly disjoint over M. Consequently, $\mathrm{Gal}(L_n/\mathbf{Q})$ *is the fibred product of the groups* $\{\mathrm{Gal}(ML_l/\mathbf{Q})\}_{l|n}$ *over* $\mathrm{Gal}(M/\mathbf{Q})$*:*

$$\text{(13)}\quad \mathrm{Gal}(L_n/\mathbf{Q}) \xrightarrow{\sim} \{(\sigma_l)_l \in \prod_{\substack{l|n \\ \textit{prime}}} \mathrm{Gal}(ML_l/\mathbf{Q}) : \sigma_l|_M \textit{ independent of } l\}.$$

Proof. Let $l \mid n$ be a prime. We have to prove the equality $[ML_l : M] \cdot [ML_{n/l} : M] = [L_n : M]$. By Galois theory, the extensions in the diagram that are indicated by the same symbol, have the same degree. Therefore, it is sufficient to prove that M is the disjoint compositum of $L_l \cap M$ and $M \cap L_{n/l}$ over $L_l \cap L_{n/l}$. The compositum of $M_l = L_l \cap M$ and $M \cap L_{n/l}$ contains the fields M_q for all primes $q \mid n$ and is therefore equal to M. By proposition 10d, we know that $L_l \cap L_{n/l}$ is abelian over $\mathbf{Q}$ of exponent dividing e. As $M_l \subset L_l$ is the maximal abelian subfield of exponent e over $\mathbf{Q}$, this intersection equals $M_l \cap L_{n/l} = M \cap L_l \cap L_{n/l}$. In other words, the field M is the disjoint compositum of $L_l \cap M$ and $M \cap L_{n/l}$ over $L_l \cap L_{n/l}$. □

$$\begin{tikzcd}
 & & L_n \arrow[dl, dash] \arrow[dr, dash] & & \\
 & ML_l \arrow[dl, dash] \arrow[dr, dash, "\parallel" marking] & & ML_{n/l} \arrow[dl, dash, "\shortmid" marking] \arrow[dr, dash] & \\
L_l \arrow[dr, dash, "\parallel" marking] & & M \arrow[dl, dash] \arrow[dr, dash] & & L_{n/l} \arrow[dl, dash, "\shortmid" marking] \\
 & L_l \cap M \arrow[dr, dash] & & M \cap L_{n/l} \arrow[dl, dash] & \\
 & & L_l \cap L_{n/l} & &
\end{tikzcd}$$

We conclude this section with a well known result that will be used in the proof of theorem 14.

Proposition 13. *There exists a constant κ_3, depending on α, such that for all $n \in \mathbf{Z}_{>1}$ and all subfields $F \subset L_n$ the following inequality holds:*

$$\log d_F^{1/[F:\mathbf{Q}]} \leq \kappa_3 \log n,$$

where d_F is the absolute value of the discriminant of F.

Proof. It is sufficient to prove the formula for $F = L_n$, as the root-discriminant $d_F^{1/[F:\mathbf{Q}]}$ is maximal for this choice of F. Let R be the set of rational primes that ramify in $L_n/\mathbf{Q}$. We write $R = R_1 \cup R_2$, with R_1 the set of primes in R that do not divide $[L_n : \mathbf{Q}]$ and $R_2 = R \backslash R_1$. If $p \in R_1$ then either p ramifies in $K/\mathbf{Q}$ or there exists a prime above p in

K in the factorization of the fractional ideal (α). The primes in R_1 are therefore bounded independently of n. Let

$$\mathcal{D}_{L_n/\mathbf{Q}} = \prod_{p \in R} \prod_{\mathfrak{p}|p} \mathfrak{p}^{a_p},$$

be the ideal factorization of the different of $L_n/\mathbf{Q}$. The integers a_p are independent of the primes $\mathfrak{p}$ above p, as L_n is normal over $\mathbf{Q}$, and satisfy the following bounds [11, page 58]:

$$\begin{array}{ll} a_p = e_p - 1 & \text{if } p \text{ is tamely ramified;} \\ a_p \le e_p - 1 + e_p v_p(e_p) & \text{if } p \text{ is wildly ramified.} \end{array}$$

Here v_p denotes the p-adic valuation and e_p is the ramification index of p in $L_n/\mathbf{Q}$. If p is wildly ramified in the Galois extension $L_n/\mathbf{Q}$, then p divides $[L_n : \mathbf{Q}]$ so that $p \in R_2$. By taking the norm of $\mathcal{D}_{L_n/\mathbf{Q}}$ to $\mathbf{Q}$, we find the following:

$$\begin{aligned} \frac{1}{[L_n : \mathbf{Q}]} \log d_{L_n} &\le \sum_{p \in R} \log p + \sum_{p \in R_2} v_p(e_p) \log p \\ &\le \sum_{p \in R_1} \log p + 2 \log [L_n : \mathbf{Q}]. \end{aligned}$$

As the primes in R_1 are bounded independently of n and the degree $[L_n : \mathbf{Q}]$ is at most $2\varphi(n)n^2$ by corollary 11, this proves the proposition. □

4. The analytic part of the proof of theorems 1 and 4

The proof of theorems 1 and 4 is in two steps. Theorem 14 below is the analytic heart of the proof: both S^+ and S^- have a density if we assume GRH. As we mentioned in the introduction, the proof is along the lines of Hooley's proof of Artin's original conjecture [5, see also 7]. In the next section we finish the proof of both theorems: the formulas for the densities in theorem 14 below are equal to Euler products. This part is more algebraic and does not require GRH.

Theorem 14. *Assume the generalized Riemann hypothesis holds. If α is not a root of unity, then the density of S^+ exists and equals*

$$\delta(S^+) = \sum_{n=1}^{\infty} \frac{\mu(n)}{[L_n : \mathbf{Q}]}.$$

If α and its conjugate $\bar{\alpha}$ are multiplicatively independent, then the density of S^- exists and equals

$$\delta(S^-) = \sum_{n=1}^{\infty} \frac{\mu(n)c(n)}{[L_n : \mathbf{Q}]},$$

with $c(n) = \#\{\sigma \in \mathrm{Gal}(L_n/\mathbf{Q}) : \sigma|_K \ne \mathrm{id}, \sigma^2 = \mathrm{id}\}$.

As the proofs for the existence of $\delta(S^+)$ and $\delta(S^-)$ are similar, we will prove the existence of the latter and leave the easier case, the existence of $\delta(S^+)$, to the reader.

We assume that α and $\bar{\alpha}$ are multiplicatively independent. We are interested in the growth rate for $x \to \infty$ of

$$S^-(x) = \#\{p : p \leq x \text{ and } p \in \bigcap_{l \text{ prime}} S_l^-\}$$

in comparison with $\pi(x)$, the number of primes up to x. The key idea for computing this quantity is the following. By formula (10) and corollary 8b, for large l the density of S_l^- is close to $\frac{1}{2}$. In other words, we get a good approximation of $S^-(x)$ by ignoring the primes up to x that are not in $\bigcap_{l \geq y} S_l^-$ for some 'large' y. To make this precise, we define for $x, y \in \mathbf{R}_{>0}$ the numbers

$$S^-(x,y) = \#\{p : p \leq x \text{ and } p \in \bigcap_{\substack{l \leq y \\ \text{prime}}} S_l^-\}$$

and, for $z \in \mathbf{R} \cup \{\infty\}$ with $z > y$,

$$M^-(x,y,z) = \#\left\{p \leq x : \begin{array}{l} p \text{ inert in } K/\mathbf{Q} \text{ and } p \notin S_l^- \\ \text{for some prime } l \text{ with } y \leq l \leq z \end{array}\right\}.$$

For each $y \in \mathbf{R}_{>0}$, we have the following inequalities:

$$S^-(x,y) - M^-(x,y,\infty) \leq S^-(x) \leq S^-(x,y). \tag{14}$$

We will prove that with $y = \frac{1}{17}\log x$, the limit $\delta^- = \lim_{x\to\infty} S^-(x,y)/\pi(x)$ exists and that the error term $M^-(x,y,\infty)$ is $o(\pi(x))$ for $x \to \infty$. With the inequalities (14) this shows that the density of S^- exists and equals δ^-.

First we focus on $S^-(x,y)$. By the principle of inclusion and exclusion we find

$$S^-(x,y) = \sum_{n|P(y)} \mu(n)\pi^-(x,n), \tag{15}$$

where $P(y)$ is the product of all primes up to y, and

$$\begin{aligned}\pi^-(x,n) &= \#\{p \leq x \text{ with } p \text{ inert in } K/\mathbf{Q} \text{ and } p \notin S_l^- \text{ for all primes } l \mid n\} \\ &= \#\{p \leq x \text{ with } p \text{ inert in } K/\mathbf{Q} \text{ and } p \text{ splits completely in } L_n/K\}.\end{aligned}$$

The last equality follows from proposition 5b. To estimate $\pi^-(x,n)$, we need an effective version of Chebotarev's density theorem. The known versions of such a theorem all have error terms in their statements which are too large for our purpose. However, we have the following conditional result of Lagarias-Odlyzko, in the formulation of Serre [10, page 333].

Theorem 15. *Let $F/\mathbf{Q}$ be a normal extension with Galois group G, let C be a union of conjugacy classes of G, and denote the absolute value of the discriminant of F by d_F. Define $\pi_C(x)$ as follows*

$$\pi_C(x) = \#\{p \leq x \text{ with } p \text{ unramified in } F/\mathbf{Q} \text{ and } (p, F/\mathbf{Q}) \subset C\},$$

where $(p, F/\mathbf{Q})$ denotes the Frobenius class of p in $F/\mathbf{Q}$. If we assume the generalized Riemann hypothesis, then there exists an absolute constant κ_4 such that for $x \geq 2$ the following inequality holds:

$$|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)| \leq \kappa_4 |C| \sqrt{x} (\log d_F{}^{1/[F:\mathbf{Q}]} + \log x),$$

with $\mathrm{Li}(x) = \int_2^\infty \frac{dt}{\log t}$ the logarithmic integral.

To approximate $\pi^-(x,n)$, we apply theorem 15 with $F = L_n$ and

$$C = C(n) = \{\sigma \in \mathrm{Gal}(L_n/\mathbf{Q}) : \sigma|_K \neq \mathrm{id} \text{ and } \sigma^2 = \mathrm{id}\}.$$

If we assume GRH and use proposition 13 for the estimate of the discriminant of L_n, we find

$$\pi^-(x,n) = \frac{c(n)}{[L_n : \mathbf{Q}]}\mathrm{Li}(x) + O(c(n)\sqrt{x}\log(nx)), \tag{16}$$

where $c(n)$ is the cardinality of $C(n)$, and the implied constant only depends on α. If we substitute (16) into (15) with $y = \frac{1}{17}\log x$, we find for $x \to \infty$ the following:

$$S^-(x, \frac{1}{17}\log x) = \sum_{n | P(\frac{1}{17}\log x)} \frac{\mu(n)c(n)}{[L_n : \mathbf{Q}]} \cdot \mathrm{Li}(x) + O(\frac{x}{\log^2 x}). \tag{17}$$

Here we use the notation $\log^2 x$ for $(\log x)^2$. To derive formula (17), we used the trivial bound $c(n) \leq [L_n : \mathbf{Q}] \leq 2n^3$, and the inequality $P(y) \leq e^{2y}$. The constant $\kappa = \frac{1}{17}$ is chosen in such a way that the sum over $n \mid P(\kappa \log x)$ of the error term in (16) is of order $o(\pi(x))$ for $x \to \infty$. By corollary 11, the limit for $x \to \infty$ of the sum in (17) converges.

To finish the proof of theorem 14 in the inert case, we are left with proving that $M^-(x, \frac{1}{17}\log x, \infty) = o(\pi(x))$ for $x \to \infty$. As in Hooley's proof, we use the following trivial identity:

$$\begin{aligned} M^-(x, \frac{1}{17}\log x, \infty) = M^-(x, \frac{1}{17}\log x, \frac{\sqrt{x}}{\log^2 x}) \\ + M^-(x, \frac{\sqrt{x}}{\log^2 x}, \sqrt{x}\log x) \\ + M^-(x, \sqrt{x}\log x, \infty). \end{aligned} \tag{18}$$

For each term on the right we use a different method to prove that it is $o(\pi(x))$ for $x \to \infty$. For the last two, we can do this unconditionally; for the first we use GRH.

For the first term on the right in (18) we find the following trivial upper bound:

$$M^{-}(x, \frac{1}{17}\log x, \frac{\sqrt{x}}{\log^2 x}) \leq \sum{}' \pi^{-}(x, l). \tag{19}$$

Here $\sum'$ indicates summation over all primes l with

$$\frac{1}{17}\log x \leq l \leq \sqrt{x}/\log^2 x.$$

If we apply theorem 15 to bound $\pi^{-}(x, l)$, we are not able to prove that the right hand side of (19) is $o(\pi(x))$ for $x \to \infty$. This is caused by the presence of the cardinality of $C(l)$ in the error term of $\pi^{-}(x, l)$. Therefore we first apply proposition 6 and find the following.

$$\begin{aligned} \sum{}' \pi(x,l)^{-} \leq & \sum{}' \#\{p \leq x \text{ that split completely in } N_l^1/\mathbf{Q}\} \\ & + \sum{}' \#\{p \leq x \text{ that split completely in } N_l^2/\mathbf{Q}\} \end{aligned} \tag{20}$$

Now we use theorem 15 to bound the right hand side of (20). For example with $F = N_l^1$ and $C = \{\mathrm{id}_{N_l^1}\}$ we find that the first term on the right of (20) is bounded by

$$\sum{}' \frac{1}{[N_l^1 : \mathbf{Q}]} \cdot \mathrm{Li}(x) + O(\sum{}' \sqrt{x}\log(lx)). \tag{21}$$

By proposition 8b and the assumption that α and $\bar{\alpha}$ are multiplicatively independent, the first sum in (21) is part of the tail of a convergent sum and therefore tends to 0 for $x \to \infty$. The second term in (21) is $O(x/\log^2 x)$, by an easy application of the prime number theorem. The same estimates hold for the last term in (20) and we conclude that

$$M^{-}(x, \frac{1}{17}\log x, \frac{\sqrt{x}}{\log^2 x}) = O(\frac{x}{\log^2 x}) \quad \text{for } x \to \infty.$$

To bound the second term in (18), we use the following result of Brun-Titchmarsh. Fix a prime l and an integer a which is not divisible by l. For all $x > l$, the number of primes up to x that are congruent to a modulo l is at most $3x/(l-1)\log(x/l)$. If a prime p splits completely in N_l^1 or N_l^2 then $p \equiv \pm 1 \bmod l$, as $\mathbf{Q}(\zeta_l^+)$ is contained in both these fields. For the second term in (18) we find:

$$M^{-}(x, \frac{\sqrt{x}}{\log^2 x}, \sqrt{x}\log x) = O(\sum \frac{x}{(l-1)\log(x/l)}) = O(\frac{x\log\log x}{\log^2 x}),$$

where the summation is over those primes l with $\sqrt{x}/\log^2 x \leq l \leq \sqrt{x}\log x$.

For the last term in (18), we again use proposition 6 and find the following upper bound for $M^-(x, \sqrt{x}\log x, \infty)$:

$$(22)\quad {\sum}' \#\{p \le x \text{ inert in } K/\mathbf{Q} \text{ and that split completely in } N_l^1/\mathbf{Q}\} + \\ {\sum}' \#\{p \le x \text{ inert in } K/\mathbf{Q} \text{ and that split completely in } N_l^2/\mathbf{Q}\}$$

where $\sum'$ now means summing over all primes $l \ge \sqrt{x}\log x$. We prove that the last term in (22), M for short, is $o(\pi(x))$. A similar proof works for the other term and is left to the reader.

Let p be a generic prime that is inert in $K/\mathbf{Q}$ and that splits completely in $N_l^2/\mathbf{Q}$. In other words, the prime $p\mathcal{O}$ of K splits completely in $KN_l^2 = K(\zeta_l, \sqrt[l]{\alpha/\bar{\alpha}})$. Therefore, $\alpha/\bar{\alpha}$ is an l-th power modulo $p\mathcal{O}$. As $\alpha/\bar{\alpha}$ is in the kernel of the norm map $(\mathcal{O}/p\mathcal{O})^* \cong \mathbf{F}_{p^2}^* \to \mathbf{F}_p^*$, we find $(\alpha/\bar{\alpha})^{p+1} \equiv 1 \bmod p$. By definition of N_l^2, the intersection $N_l^2 \cap \mathbf{Q}(\zeta_l)$ equals $\mathbf{Q}(\zeta_l^+)$, the maximal real subfield of $\mathbf{Q}(\zeta_l)$. Therefore, l divides $p+1$ and we find that the fractional ideal generated by $(\alpha/\bar{\alpha})^{(p+1)/l} - 1$ has positive valuation at the prime $p\mathcal{O}$. To bound M, we note that, as $p \le x$ and $l \ge \sqrt{x}\log x$, we have the upper bound $(p+1)/l \le 2\sqrt{x}/\log x$. Choose integers β and γ of K such that $\alpha = \beta\gamma^{-1}$. We conclude that M is bounded above by the number of primes dividing the integral ideal generated by

$$\prod_{m \le \frac{2\sqrt{x}}{\log x}} ((\beta\bar{\gamma})^m - (\bar{\beta}\gamma)^m).$$

This is a non-zero integer of K, as $\langle \alpha, \bar{\alpha} \rangle$ has rank 2 by assumption. Taking the norm to $\mathbf{Q}$, and noting that the number of primes in a non-zero integer N is of order $O(\log|N|)$, we find that M is of order

$$O\Big(\sum_{m \le \frac{2\sqrt{x}}{\log x}} \log|\delta^{2m} + \bar{\delta}^{2m} - 2N_{K/\mathbf{Q}}(\delta)^m|\Big) = O\Big(\sum_{m \le \frac{2\sqrt{x}}{\log x}} m\Big) = O\Big(\frac{x}{\log^2 x}\Big),$$

with $\delta = \beta\bar{\gamma}$.

We conclude that $M^-(x, \frac{1}{17}\log x, \infty) = O(x \log\log x/\log^2 x)$, and combined with (14) and (17) we find

$$S^-(x) - \sum_{n=1}^{\infty} \frac{\mu(n)c(n)}{[L_n : \mathbf{Q}]} \cdot \mathrm{Li}(x) = O\Big(\frac{x \log\log x}{\log^2 x}\Big) \quad \text{for } x \to \infty.$$

As $\pi(x) \sim \mathrm{Li}(x) \sim x/\log x$ for $x \to \infty$, this concludes the proof of theorem 14 in the inert case.

Remark. The main obstruction to generalize the above proof to number fields of degree larger than 2 seems to be showing that $M^-(x, \sqrt{x}\log x, \infty)$ is of order $o(\pi(x))$.

5. Conclusion of the proofs of theorems 1 and 4

First we proof theorem 1 for the 'degenerate' cases. If α is a root of unity, the set S^+ has zero density by proposition 2a and theorem 1 is proved by defining $c_\alpha^+ = 0$. Similar, if we define $c_\alpha^- = 0$ in case α and $\bar{\alpha}$ are multiplicatively dependent, theorem 1 follows from proposition 2b.

In all other cases we can use theorem 14: if GRH holds then the sets S^+ and S^- have a density. To complete the proof of theorem 1, we have to show that the infinite sums in theorem 14 are equal to rational multiples of certain Euler products. Theorem 1 follows from the following more precise theorem.

Theorem 16. *Let f be defined as in proposition 10, let t be the order of the torsion subgroup of $K^*/\langle\alpha,\bar{\alpha}\rangle$ and let r be the rank of $\langle\alpha,\bar{\alpha}\rangle$. Assume GRH holds.*

a. *If α is not a root of unity, then*

$$(23)\qquad \delta(S^+) = \delta(S_{2f}^+) \prod_{\substack{l \text{ prime} \\ l\nmid 2f,\, l|t}} \left(1 - \frac{1}{[L_l:K]}\right) \prod_{\substack{l \text{ prime} \\ l\nmid 2ft}} \left(1 - \frac{1}{l^r(l-1)}\right).$$

b. *If α and $\bar{\alpha}$ are multiplicatively independent, then*

$$(24)\qquad \delta(S^-) = \delta(S_{2f}^-) \prod_{\substack{l \text{ prime} \\ l\nmid 2f,\, l|t}} \left(1 - \frac{c(l)}{[L_l:K]}\right) \prod_{\substack{l \text{ prime} \\ l\nmid 2ft}} \left(1 - \frac{2}{l(l-1)}\right),$$

with $c(l) = \#\{\sigma \in \mathrm{Gal}(L_l/\mathbf{Q}) : \sigma|_K \neq \mathrm{id}, \sigma^2 = \mathrm{id}\}$.

Proof. a. As α is not a root of unity, we can apply the first part of theorem 14 to find the following expression for the density of S^+:

$$\delta(S^+) = \frac{1}{2}\sum_{n=1}^{\infty} \frac{\mu(n)}{[L_n:K]} = \frac{1}{2}\sum_{d|2f} \sum_{\substack{k=1 \\ \gcd(k,2f)=1}}^{\infty} \frac{\mu(dk)}{[L_{dk}:K]}.$$

Here we used that μ vanishes on integers which are not squarefree. As the rank r is at least 1, the right hand side is absolutely convergent by corollary 11. To obtain an Euler product for this sum we proceed as follows. Let k and d be integers, with k prime to $2f$ and d a divisor of $2f$. By proposition 10e we have the equalities $[L_{dk} : K] = [L_d : K][L_k : K]$ and $[L_k : K] = \prod_{l|k}[L_l : K]$. Using these relations and equation (11) we find the following formula:

$$\begin{aligned}\delta(S^+) &= \frac{1}{2}\sum_{d|2f}\frac{\mu(d)}{[L_d:K]}\sum_{\substack{k=1\\ \gcd(k,2f)=1}}^{\infty}\frac{\mu(k)}{[L_k:K]}\\ &= \delta(S^+_{2f})\prod_{\substack{l\nmid 2f\\ \text{prime}}}(1-\frac{1}{[L_l:K]}).\end{aligned}$$

By proposition 8a, the degree of L_l/K equals $l^r(l-1)$ for all primes $l \nmid 2ft$. If we substituting this into the formula above, this completes the proof in the split case.

b. By the second part of theorem 14 we obtain

$$\delta(S^-) = \frac{1}{2}\sum_{d|2f}\sum_{\substack{k=1\\ \gcd(k,2f)=1}}^{\infty}\frac{\mu(dk)c(dk)}{[L_{dk}:K]}.$$

Recall that $c(n)$ denotes the cardinality of the set $\{\sigma \in \mathrm{Gal}(L_n/\mathbf{Q}) : \sigma|_K \neq \mathrm{id}, \sigma^2 = \mathrm{id}\}$. If L_n and L_m are linearly disjoint over K, we have the isomorphism

$$\mathrm{Gal}(L_{nm}/\mathbf{Q}) \cong \{(\sigma,\tau) \in \mathrm{Gal}(L_n/\mathbf{Q}) \times \mathrm{Gal}(L_m/\mathbf{Q}) : \sigma|_K = \tau|_K\},$$

and hence the equality $c(nm) = c(n)c(m)$. Arguing as in the split case and using equation (12), we find the following formula for the density of S^-

$$\delta(S^-) = \delta(S^-_{2f})\prod_{\substack{l\nmid 2f\\ \text{prime}}}(1-\frac{c(l)}{[L_l:K]}).$$

As by assumption α and $\bar{\alpha}$ are multiplicatively independent, proposition 8b implies $c(l)/[L_l : K] = 2/\big(l(l-1)\big)$ for all primes $l \nmid 2ft$ and we are done. □

The proof of theorem 4 is highly similar to the above proof. Let K be a quadratic field not contained in $\mathbf{Q}(\zeta_l)$ for all primes l. Denote the torsion subgroup of K^* by μ_K. Assume that α and $\bar{\alpha}$ are multiplicatively independent, that $K^*/\langle\mu_K, \alpha, \bar{\alpha}\rangle$ is torsion free and that 2 ramifies completely in $L_2/\mathbf{Q}$. This last assumption implies by proposition 10f that the fields $\{L_l\}_l$ are linearly disjoint over K. With theorem 14, we find that GRH implies the following:

$$\delta(S^+) = \frac{1}{2}\prod_{l\text{ prime}}(1-\frac{1}{[L_l:K]}),$$

$$\delta(S^-) = \frac{1}{2}\prod_{l\text{ prime}}(1-\frac{c(l)}{[L_l:K]}).$$

Using proposition 8 we find for all odd primes l the equalities $[L_l : K] = l^2(l-1)$ and $c(l)/[L_l : K] = 2/l(l-1)$. If $\sqrt{\alpha}$ and $\sqrt{\bar{\alpha}}$ generate the same quadratic extension of K, then $\alpha\bar{\alpha} = \beta^2$ for some $\beta \in K^*$. As α and $\bar{\alpha}$ are multiplicatively independent, the element β is a non-trivial 2-torsion element in $K^*/\langle\mu_K, \alpha, \bar{\alpha}\rangle$. Therefore $K(\sqrt{\alpha})/K$ and $K(\sqrt{\bar{\alpha}})/K$ are different quadratic extensions and L_2 is of degree 4 over K. If we substitute all field degrees in the first formula above, this proves the formula for $\delta(S^+)$ in theorem 4. To obtain the formula for $\delta(S^-)$ we still need the Euler factor at $l = 2$. As $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is not a square in K^*, proposition 6b yields $\delta(S_2^-) = \frac{1}{4}$. Using (10) we find

$$1 - \frac{c(2)}{[L_2 : K]} = 2\delta(S_2^-) = \frac{1}{2}.$$

An efficient method to approximate the Euler products in theorem 4 is explained in [6].

6. Proof of theorem 3

We can decide 'at a finite level' whether one of the sets S^+ or S^- has zero density.

Proposition 17. *Let f be defined as in proposition 10, and define the sets $S_{2f}^+ = \bigcap_{l|2f} S_l^+$ and $S_{2f}^- = \bigcap_{l|2f} S_l^-$. Assume GRH holds. If α is not a root of unity then:*

$$\delta(S_{2f}^+) = 0 \Longleftrightarrow \delta(S^+) = 0.$$

If α and $\bar{\alpha}$ are multiplicatively independent and α is not a cube in K^* then:

$$\delta(S_{2f}^-) = 0 \Longleftrightarrow \delta(S^-) = 0.$$

The implications from left to right are unconditionally true.

Proof. The implications from left to right are trivial as S_{2f}^+ contains S^+ and S_{2f}^- contains S^-. If GRH holds and α is not a root of unity, the density of S^+ is given by (23). The fact that α is not a root of unit implies that r is at least 1 and hence the infinite product in (23) is non-zero. Using proposition 8a and formula (9), we find that the product over the primes $\{l : l \nmid 2f, l \mid t\}$ in (23) is also non-zero. Here we use that if K is equal to $\mathbf{Q}(\zeta_3)$, then f is divisible by 3. Hence $\delta(S^+)$ is zero if and only if $\delta(S_{2f}^+)$ is zero.

The second equivalence in the proposition follows in a similar way by using the formula (24) and proposition 8b. □

The non-vanishing of the density of one of the sets S_{2f}^+ or S_{2f}^-, is equivalent with the existence of an element in $\mathrm{Gal}(L_{2f}/\mathbf{Q})$ with certain properties. To be more precise, the combination of proposition 5 and Chebotarev's density theorem yields the following proposition.

Proposition 18. *Let $n \geq 2$ be an integer.*

a. *The set S_n^+ has non-zero density if and only if there exists $\sigma \in \operatorname{Gal}(L_n/\mathbf{Q})$ with $\sigma|_K = \mathrm{id}$ and $\sigma|_{L_l} \neq \mathrm{id}$ for all primes l dividing n.*
b. *The set S_n^- has non-zero density if and only if there exists $\sigma \in \operatorname{Gal}(L_n/\mathbf{Q})$ with $\sigma|_K \neq \mathrm{id}$ and $\operatorname{ord}(\sigma|_{L_l}) > 2$ for all primes l dividing n.*

Proposition 5 and Chebotarev's density theorem also imply that if S_{2f}^+ has zero density then it is a finite set. Namely, suppose S_{2f}^+ is an infinite set and has density 0. Then there exists a prime $p \in S_{2f}^+$ that is unramified in $L_{2f}/\mathbf{Q}$. Let $\rho \in \operatorname{Gal}(L_{2f}/\mathbf{Q})$ be the Frobenius automorphism of a prime above p in L_{2f}. The set of rational primes whose Frobenius class is the conjugacy class of ρ, is a subset of S_{2f}^+ and has positive density, contradicting the assumption $\delta(S_{2f}^+) = 0$. A similar observation holds for the set S_{2f}^-.

Under some mild restrictions on α, we know by proposition 8 that both S_l^+ and S_l^- have positive density for all primes l. Hence, for all primes $l \mid 2f$ there exists $\sigma_l \in \operatorname{Gal}(L_l/\mathbf{Q})$ with the properties as stated in proposition 18. If we want to prove that S_{2f}^+ or S_{2f}^- has non-zero density, we have to glue the different elements $\sigma_l \in \operatorname{Gal}(L_l/\mathbf{Q})$ to one element in $\operatorname{Gal}(L_{2f}/\mathbf{Q})$. We use proposition 12 to decide whether this is possible.

Proof of theorem 3a. First we assume that K is not equal to $\mathbf{Q}(\zeta_3)$ and that α does not satisfy any of the properties in proposition 2a; α is not a root of unity nor a square in K^*. We will show that S^+ has zero density if and only if the second statement of theorem 3a holds. Denote by f the conductor of $L_2^{\mathrm{ab}}/\mathbf{Q}$. By propositions 17 and 18, the set S^+ has non-zero density if and only if there exists $\sigma \in \operatorname{Gal}(L_{2f}/K)$ such that $\sigma_{L_l} \neq \mathrm{id}$ for all primes l dividing $2f$. Let e be the exponent of $L_2^{\mathrm{ab}}/\mathbf{Q}$, and for each prime $l \mid 2f$ define M_l as the maximal subfield of L_l that is abelian over $\mathbf{Q}$ of exponent dividing e. If we apply proposition 12 with $n = 2f$ we find

$$\operatorname{Gal}(L_{2f}/\mathbf{Q}) \xrightarrow{\sim} \{(\sigma_l)_l \in \prod_{\substack{l|2f \\ \text{prime}}} \operatorname{Gal}(ML_l/\mathbf{Q}) : \sigma_l|_M \text{ independent of } l\},$$

with M the compositum of the fields $\{M_l\}_{l|2f}$. Therefore, the set S^+ has non-zero density if and only if there exists for each prime $l \mid 2f$ an element $\sigma_l \in \operatorname{Gal}(ML_l/K)$ that is non-trivial on L_l and such that all σ_l agree on M.

The primes $l \mid 2f$ for which L_l is not contained in M do not cause any trouble: for arbitrary $\tau \in \operatorname{Gal}(M/K)$, there exists a $\sigma_l \in \operatorname{Gal}(ML_l/K)$ such that $\sigma_l|_M = \tau$ and $\sigma_l|_{L_l} \neq \mathrm{id}$. Namely, if l is such a prime we can choose a non-trivial element $\rho_l \in \operatorname{Gal}(L_l/K)$ for which $\rho_l|_{L_l \cap M} = \tau|_{L_l \cap M}$. The unique $\sigma_l \in \operatorname{Gal}(ML_l/K)$ that extends both ρ_l and τ has the desired property.

Let T be the set of primes l for which $L_l \subset M$, that is, for which $L_l/\mathbf{Q}$ is abelian of exponent dividing e. If T is non-empty define the subfield E of M as the compositum of the fields $\{L_l\}_{l \in T}$; if T is empty let E be equal to K. By the discussion above, the set S^+ has non-zero density if and only if there exists $\tau \in \mathrm{Gal}(E/K)$ that is non-trivial on L_l for all $l \in T$.

The existence of such an element τ depends on the set T. As $\mathbf{Q}(\zeta_l)$ is contained in L_l and e divides 4, we find that T is a subset of $\{2, 3, 5\}$. More precisely, we have the following equivalences

$$\begin{aligned} &2 \in T \Longleftrightarrow L_2 = L_2^{\mathrm{ab}}; \\ (25) \qquad &3 \in T \Longleftrightarrow L_3 = K(\zeta_3); \\ &5 \in T \Longleftrightarrow e = 4 \text{ and } L_5 = K(\zeta_5). \end{aligned}$$

If T is empty there is nothing to prove. The assumptions that α is not a square in K^*, and that K is not of discriminant -3, imply that there exists a non-trivial element $\tau_l \in \mathrm{Gal}(L_l/K)$ for all l in T. If T has at most 2 elements, the existence of τ is guaranteed. Indeed, for $T = \{l\}$ we can take $\tau = \tau_l$ as above. In case $T = \{l_1, l_2\}$ has cardinality 2, the argument is as follows. If L_{l_1} and L_{l_2} are linearly disjoint over K, the elements τ_{l_1} and τ_{l_2} determine an element τ with the desired properties. If not, any extension τ of a non-trivial element in $\mathrm{Gal}((L_{l_1} \cap L_{l_2})/K)$ to $E = L_{l_1}L_{l_2}$ will do.

Now we assume that T has cardinality 3, so E is equal to L_{30}. Because of (25), the field L_2^{ab} is of exponent 4 and equals $L_2 = K(\sqrt{\alpha})$. Furthermore α is a cube in $K(\zeta_3)^*$ and a fifth power in $K(\zeta_5)^*$. As we showed in the proof of proposition 8a, this is equivalent with α being a fifteenth power in K^*. If there exist $l_1, l_2 \in T$ with $l_1 \neq l_2$ and $L_{l_1} = L_{l_2}$, an argument as in the case $\#T = 2$ above shows the existence of τ. Therefore, we assume in addition that L_2, L_3 and L_5 are pairwise different and all abelian over $\mathbf{Q}$ of exponent dividing 4. The extensions L_2/K and L_3/K are both quadratic, so there exists a unique element $\sigma \in \mathrm{Gal}(L_6/K)$ that is non-trivial on both L_2 and L_3. The group $\mathrm{Gal}(L_6/K)$ is isomorphic to Klein's four group, so apart from L_2 and L_3 there is a unique third quadratic extension of K inside L_6. If L_5 is not contained in L_6, the element σ can be extended to an automorphism τ of L_{30} which is non-trivial on L_5 and hence $\delta(S^+)$ is positive. On the other hand, if L_5 is contained in L_6, then L_5 is this third quadratic extension of K inside L_6 and $\sigma|_{L_5}$ is automatically trivial. In this case S^+ has zero density. The field $L_{30} = L_6$ is of degree 8 over $\mathbf{Q}$, exponent 2 over K and contains both ζ_3 and ζ_5. This yields the equalities $E = \mathbf{Q}(\zeta_{15})$ and $K = \mathbf{Q}(\sqrt{5})$ and forces $L_2 = K(\sqrt{\alpha})$ to be equal to the maximal real subfield of $\mathbf{Q}(\zeta_{15})$.

To complete the proof of theorem 3a, we have to deal with the case $K = \mathbf{Q}(\zeta_3)$. Assume that K is equal to $\mathbf{Q}(\zeta_3)$ and that α does not satisfy any of the properties in proposition 2a. We need to show that $\delta(S^+)$ is positive. Let T be the set of primes l for which $L_l/\mathbf{Q}$ is abelian of exponent dividing 6. As $\mathbf{Q}(\zeta_l)$ is a subfield of L_l, the set T is contained in $\{2,3,7\}$. Denote by E the compositum of the fields $\{L_l\}_{l\in T}$. We will show that there exists $\tau \in \mathrm{Gal}(E/K)$ that is non-trivial on L_l for all $l \in T$. Using similar arguments as in the case $K \neq \mathbf{Q}(\zeta_3)$, this implies that $\delta(S^+)$ is positive. We assume that T has cardinality 3, and leave the other cases to reader. Because 3 is in T, the field L_3 is abelian over $\mathbf{Q}$ and hence $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is a cube in K^*. As by assumption α is not a cube in K^*, the element $\alpha/\bar{\alpha}$ is not a cube in K^* and $L_3 = \mathbf{Q}(\zeta_3, \sqrt[3]{\alpha/\bar{\alpha}})$ is cyclic over $\mathbf{Q}$ of degree 6. Denote by F_3 the unique cubic subfield of L_3. Furthermore, let F_7 be the unique cubic subfield of $L_7 = \mathbf{Q}(\zeta_3, \zeta_7)$ and let $\sigma_1 \in \mathrm{Gal}(F_3F_7/\mathbf{Q})$ be non-trivial on both F_3 and F_7. As α is not a square in K^*, there is a non-trivial element $\sigma_2 \in \mathrm{Gal}(L_2/K)$. Because the fields L_2 and F_3F_7 as linearly disjoint over $\mathbf{Q}$, there exists a unique $\sigma \in \mathrm{Gal}(L_2F_3F_7/K)$ extending both σ_1 and σ_2. Any extension τ of σ to $E = L_2L_3L_7$ is non-trivial on L_2, L_3 and L_7. □

As we noted before the proof of theorem 3a, the set S^- has non-zero density if certain elements in $\mathrm{Gal}(L_l/\mathbf{Q})$, with l ranging over the prime divisors of $2f$, can be 'glued' to one element in $\mathrm{Gal}(L_{2f}/\mathbf{Q})$. To decide whether this is possible, we first make a more detailed analysis of the situation at a single prime l.

Proposition 19. *Assume K is not equal to $\mathbf{Q}(\zeta_3)$ and that α does not satisfy any of the conditions of proposition 2b. For each prime l, let M_l be the maximal subfield of L_l that is of exponent 2 over $\mathbf{Q}$, and let k_l be the quadratic field defined in the introduction. For each $\rho \in \mathrm{Gal}(M_l/\mathbf{Q})$ with $\rho|_K \neq id$ the following holds:*

$$\rho \text{ can be extended to an automorphism of } L_l \text{ of order larger than } 2$$
$$\Updownarrow$$
$$\rho|_{k_l} \neq \mathrm{id}.$$

Proof. For odd l the field M_l is of degree 2 or 4 over $\mathbf{Q}$, according to whether K is contained in $\mathbf{Q}(\zeta_l)$ or not. In both cases, $\mathrm{Gal}(K(\zeta_l)/M_l)$ is cyclic of order $(l-1)/2$. Therefore, if l is larger than 5 then any ρ can be extended to an automorphism of $K(\zeta_l)$ of order larger than 2. Namely, suppose $\hat{\rho}$ is an extension of ρ to $K(\zeta_l)$ of order 2. The product of $\hat{\rho}$ with a generator of $\mathrm{Gal}(K(\zeta_l)/M_l)$ yields an extension of ρ of order larger than 2.

Now assume $l = 5$ and denote by k the subfield of $M_5 = K(\sqrt{5})$ fixed by ρ. If k is not equal to $\mathbf{Q}(\sqrt{5})$, the group $\mathrm{Gal}(K(\zeta_5)/k)$ is cyclic of order 4 and a generator of this group extends ρ. Therefore, we suppose that k equals $\mathbf{Q}(\sqrt{5})$. As ρ is non-trivial on K, this implies in particular that K is not $\mathbf{Q}(\sqrt{5})$. In case α is a fifth power in K^*, the field L_5 coincides with $K(\zeta_5)$, which is of exponent 2 over $\mathbf{Q}(\sqrt{5})$ and any extension of ρ to L_5 will have order 2. We claim that if α is not a fifth power then there exists an extension of ρ to L_5 of order larger than 2. To prove the claim, choose a field $N_5 \in \{N_5^1, N_5^2\}$ such that $KN_5/K(\zeta_5)$ is non-trivial. This is possible because if both extensions are trivial then both $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ and $\alpha/\bar{\alpha}$ are fifth powers in K^* and so is α. In diagram 1 below, we have drawn all fields involved.

$$\begin{tikzcd}
 & KN_5 \arrow[dl, dash, "2"'] \arrow[dr, dash, "5"] & & & \\
N_5 \arrow[dr, dash, "5"'] & & K(\zeta_5) \arrow[dl, dash, "2"] \arrow[dr, dash, "2"] & & \\
 & N_5 \cap K(\zeta_5) \arrow[dr, dash, "2"'] & & M_5 \arrow[dl, dash, "2"] \arrow[dr, dash, "2"] & \\
 & & k = \mathbf{Q}(\sqrt{5}) \arrow[dr, dash, "2"'] & & K \arrow[dl, dash, "2"] \\
 & & & \mathbf{Q} &
\end{tikzcd}$$

diagram 1

$$\begin{tikzcd}
 & KN_{3,\rho} \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & & \\
N_{3,\rho} \arrow[dr, dash, "3"'] & & M_3 = K(\zeta_3) \arrow[dl, dash, "2"] \arrow[dr, dash, "2"] & \\
 & k \arrow[dr, dash, "2"'] & & K \arrow[dl, dash, "2"] \\
 & & \mathbf{Q} &
\end{tikzcd}$$

diagram 2

As N_5 is Galois over $\mathbf{Q}$, it is cyclic of degree 5 over $N_5 \cap K(\zeta_5)$. Therefore, the field KN_5 is cyclic of degree 10 over $N_5 \cap K(\zeta_5)$. Any extension of a generator of $\mathrm{Gal}(KN_5/(N_5 \cap K(\zeta_5))$ to L_5 has order larger than 2 and, as such an extension is trivial on $\mathbf{Q}(\sqrt{5})$ and non-trivial on K, extends ρ. This concludes the proof of the claim.

By assumption K is not equal to $\mathbf{Q}(\zeta_3)$, so $M_3 = K(\zeta_3)$ is of degree 4 over $\mathbf{Q}$. The fixed field k of ρ is equal to either $\mathbf{Q}(\zeta_3)$ or $\mathbf{Q}(\sqrt{-3D})$, where D denotes the discriminant of K. As in corollary 7, let $N_{3,\rho}$ be the unique field in $\{N_3^1, N_3^2\}$ that contains the fixed field k of ρ. In diagram 2 we have drawn the fields involved. If $N_{3,\rho}/k$ is non-trivial, and therefore cyclic of degree 3, the group $\mathrm{Gal}(KN_{3,\rho}/k)$ is cyclic of degree 6. An extension of a generator of this group to L_3 extends ρ and is of order larger than 2. On the other hand, if $N_{3,\rho}/k$ is trivial then all extensions of ρ to L_3 have order 2 by corollary 7. The extension $N_{3,\rho}/k$ is trivial if either k equals $\mathbf{Q}(\zeta_3)$ and $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is a cube in K^*, or k equals $\mathbf{Q}(\sqrt{-3D})$ and $\alpha/\bar{\alpha}$ is a cube in K^*.

For the prime $l = 2$ we can copy the proof of proposition 6b. If $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is a square in K^*, the extension $L_2/\mathbf{Q}$ is cyclic of degree 4, the field M_2 equals K and any extension of ρ has order 4. Otherwise, M_2 is equal to $K(\sqrt{\mathrm{N}_{K/\mathbf{Q}}(\alpha)})$ and, as both L_2/K and $L_2/\mathbf{Q}(\sqrt{\mathrm{N}_{K/\mathbf{Q}}(\alpha)})$ are of exponent 2, the element ρ can be extended to an element of order larger than 2 if and only if ρ is non-trivial on $\mathbf{Q}(\sqrt{\mathrm{N}_{K/\mathbf{Q}}(\alpha)})$. □

Proof of theorem 3b. First we assume that K is not equal to $\mathbf{Q}(\zeta_3)$ and that α does not satisfy any of the properties stated in proposition 2b; α and $\bar{\alpha}$ are multiplicatively independent, α is not a cube in K^* and $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$

is not a square in $\mathbf{Q}^*$. Let f denote the conductor of $L_2^{\mathrm{ab}}/\mathbf{Q}$. Because of proposition 17, it is sufficient to prove that the second condition in theorem 3b is equivalent with the property that $\delta(S_{2f}^-)$ is zero. Again using proposition 17, we find that the set S_{2f}^- has zero density if and only if the possibly smaller set S_{30f}^- has zero density.

For each prime l, let k_l be the quadratic field defined in the introduction. Let E denote the compositum of K, k_2, k_3 and k_5. First we prove the following equivalence,

$$(26) \qquad \delta(S_{30f}^-) \neq 0 \Longleftrightarrow \begin{array}{l}\text{there exists an automorphism } \tau \text{ of } E \\ \text{that is non-trivial on } K, k_2, k_3 \text{ and } k_5.\end{array}$$

By proposition 18, the left hand side of (26) is equivalent with the existence of $\sigma \in \mathrm{Gal}(L_{30f}/\mathbf{Q})$ such that $\sigma|_K \neq \mathrm{id}$ and $\mathrm{ord}(\sigma|_{L_l}) > 2$ for all primes l dividing $30f$. If such a σ exists, the element $\tau = \sigma|_E$ has the desired properties by proposition 19, and the implication from left to right is proved.

Now we assume that there exists a $\tau \in \mathrm{Gal}(E/\mathbf{Q})$ which is non-trivial on K, k_2, k_3 and k_5. We will lift τ to an element $\sigma \in \mathrm{Gal}(L_{30f}/\mathbf{Q})$ with the properties as in the last paragraph. The construction of σ depends on the field L_2. By assumption $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is not a square in $\mathbf{Q}^*$, hence $\mathrm{Gal}(L_2/\mathbf{Q})$ is either dihedral of order 8 or cyclic of order 4.

First we assume $\mathrm{Gal}(L_2/\mathbf{Q})$ is dihedral of order 8 and define M as the compositum of the fields $\{M_l\}_{l|30f}$, with M_l the maximal subfield of L_l that is of exponent 2 over $\mathbf{Q}$. Note that E is contained in M. By proposition 12 the fields $\{ML_l\}_{l|30f}$ are linearly disjoint over M. Lift τ to an automorphism of M, which we again denote by τ. By assumption $\tau|_{k_l}$ is not equal to the identity for all primes l dividing $30f$. We can lift $\tau|_{M_l}$ to an element $\tau_l \in \mathrm{Gal}(L_l/\mathbf{Q})$ of order larger than 2 by proposition 19. As the intersection $M \cap L_l$ equals M_l, the elements τ_l and τ have a common extension to ML_l. By the isomorphism (13) we find that the elements $(\tau_l)_{l|30f}$ determine an element $\sigma \in \mathrm{Gal}(L_{30f}/\mathbf{Q})$ with the prescribed properties.

If $L_2/\mathbf{Q}$ is cyclic of order 4 we define f_0 as the maximal odd divisor of $30f$ and let M be the compositum of the fields $\{M_l\}_{l|f_0}$, where again M_l denotes the maximal subfield of L_l that is of exponent 2 over $\mathbf{Q}$. By proposition 12 we find the fields $\{ML_l\}_{l|f_0}$ to be linearly disjoint over M. By the same argument as in the last paragraph, we find $\sigma_0 \in \mathrm{Gal}(L_{f_0}/\mathbf{Q})$ which $\sigma_0|_{L_l}$ or order larger than 2 for all primes $l \mid f_0$. Let σ be an extension of σ_0 to L_{30f}. Because σ is non-trivial on the unique quadratic subfield K of L_2, the restriction $\sigma|_{L_2}$ automatically has order 4. We conclude that σ has the desired properties, and this concludes the proof of (26).

To conclude the proof of theorem 3b in the case $K \neq \mathbf{Q}(\zeta_3)$, we show that there exists $\tau \in \mathrm{Gal}(E/\mathbf{Q})$ as on the right hand side of (26) if and only if the second statement in theorem 3b does *not* hold.

First assume there exists $\tau \in \mathrm{Gal}(E/\mathbf{Q})$ as in (26) and let $F \subset E$ be the compositum of three different quadratic fields among K, k_2, k_3 and k_5. If F is of degree 4, then $\mathrm{Gal}(F/\mathbf{Q})$ is isomorphic to Klein's four group and F has exactly three quadratic subfields. However, the element $\tau|_F \in \mathrm{Gal}(F/\mathbf{Q})$ is non-trivial on all of these subfields, which is clearly impossible.

Now we assume that the second statement in theorem 3b does not hold and we prove that there exists $\tau \in \mathrm{Gal}(E/\mathbf{Q})$ that is non-trivial on K, k_2, k_3 and k_5. Let X be the set of characters of these quadratic fields. The non-empty set X generates the character group of $\mathrm{Gal}(E/\mathbf{Q})$, and has cardinality at most 4. It is sufficient to show that there exists $\tau \in \mathrm{Gal}(E/\mathbf{Q})$ on which all characters in X are non-trivial. We view the character group of $\mathrm{Gal}(E/\mathbf{Q})$ as a $\mathbf{F}_2$-vector space and choose a maximal $\mathbf{F}_2$-independent subset $S \subset X$. As S is an $\mathbf{F}_2$-basis for the character group of $\mathrm{Gal}(E/\mathbf{Q})$, there exists a unique $\tau \in \mathrm{Gal}(E/\mathbf{Q})$ on which all characters in S are non-trivial. We claim that all characters in X are non-trivial on τ. If X equals S, there is nothing to prove. Otherwise, all characters in X can uniquely be written as a product of at most three characters in S. The number of characters in such a product is not 2, as this would imply that there are 3 distinct fields among k_2, k_3, k_5 and K, whose compositum is of degree 4. If a character in X is the product of one or three elements of S, then it is indeed non-trivial on τ. This proves the claim and the existence of τ with the required properties.

Finally we assume that K is equal to $\mathbf{Q}(\zeta_3)$ and that α does not satisfy any of the properties stated in proposition 2b. Let f be the conductor of L_6^{ab} and let n be the product of the primes in the set $\{2, 3, 5, 7, 13\} \cup \{q : q|f \text{ prime}\}$. We will prove the existence of an element $\sigma \in \mathrm{Gal}(L_n/\mathbf{Q})$ that is non-trivial on K and for which $\sigma|_{L_l}$ has order larger than 2 for all primes $l|n$. This implies by proposition 18 that S_n^- has positive density. Because S_n^- is contained in S_{2f}^-, proposition 17 implies that $\delta(S^-)$ is positive. As the second statement in theorem 3b does not hold, this completes the proof of theorem 3b.

For each prime l, let M_l be the maximal subfield of L_l that is abelian of exponent dividing 6 over $\mathbf{Q}$. In particular we have the equalities $M_2 = L_2^{\mathrm{ab}} = K(\sqrt{\mathrm{N}_{K/\mathbf{Q}}(\alpha)})$ and $M_3 = L_3^{\mathrm{ab}} = K(\sqrt[3]{\alpha/\bar{\alpha}})$. Denote by M the compositum of the fields $\{M_l\}_{l|n}$. To construct an element $\sigma \in \mathrm{Gal}(L_n/\mathbf{Q})$ with the above described properties, we first fix a specific automorphism τ of M, which we then extend to L_n.

If $l \equiv 1 \bmod 3$, the field M_l contains the unique cubic subfield F_l of $\mathbf{Q}(\zeta_l)$. As by assumption $\alpha/\bar{\alpha}$ is not a cube in K^*, the field M_3 also contains a unique cubic field F_3. Let F be the compositum of F_3, F_7 and F_{13}. We claim that there exists an automorphism τ_1 of F that is of order 3 on each of these cubic fields. To prove the claim we assume that F_3 is contained in the compositum F_7F_{13}, as otherwise the existence of τ_1 is trivial. As F_7 is disjoint from F_{13}, the group $\mathrm{Gal}(F/\mathbf{Q})$ is isomorphic to $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ and hence has four subgroups of order 3. It follows that there exists $\tau_1 \in \mathrm{Gal}(F/\mathbf{Q})$ outside the union of $\mathrm{Gal}(F/F_3)$, $\mathrm{Gal}(F/F_7)$ and $\mathrm{Gal}(F/F_{13})$, which proves the claim. Because there is no element in K of norm 5, the field $\mathbf{Q}(\sqrt{5})$ is different from the maximal real subfield $\mathbf{Q}(\sqrt{\mathrm{N}_{K/\mathbf{Q}}(\alpha)})$ of M_2 and hence M_2 and $\mathbf{Q}(\sqrt{5})$ are disjoint over $\mathbf{Q}$. Using that $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is not a square in $\mathbf{Q}^*$, it follows that there exists $\tau_2 \in \mathrm{Gal}(M_2(\sqrt{5})/\mathbf{Q})$ that is non-trivial on K, $\mathbf{Q}(\sqrt{\mathrm{N}_{K/\mathbf{Q}}(\alpha)})$ and $\mathbf{Q}(\sqrt{5})$.

As the subfields F and $M_2(\sqrt{5})$ of M are linearly disjoint, there exists $\tau \in \mathrm{Gal}(M/\mathbf{Q})$ extending both τ_1 and τ_2. Fix such an element τ. We claim that τ can be extended to $\sigma \in \mathrm{Gal}(L_n/\mathbf{Q})$ such that $\mathrm{ord}(\sigma|_{L_l}) > 2$ for all primes $l|n$. By proposition 12 it suffices to construct for all primes $l|n$ elements $\sigma_l \in \mathrm{Gal}(ML_l/\mathbf{Q})$ such that $\sigma_l|_M = \tau$ and $\mathrm{ord}(\sigma_l|_{L_l}) > 2$.

For primes $l \in \{2,3,5,7,13\}$ *any* extension $\sigma_l \in \mathrm{Gal}(ML_l/\mathbf{Q})$ of τ has the property $\mathrm{ord}(\sigma_l|_{L_l}) > 2$. For $l \in \{3,7,13\}$ this follows from $\mathrm{ord}(\tau|_{F_l}) = 3$. Because τ is non-trivial on $\mathbf{Q}(\sqrt{5})$, any extension of $\tau|_{\mathbf{Q}(\sqrt{5})}$ to $\mathbf{Q}(\zeta_5)$ will have order 4. As $\mathbf{Q}(\zeta_5)$ is contained in L_5, we find that any extension σ_5 of τ to ML_5 will have the property $\mathrm{ord}(\sigma_5|_{L_5}) > 2$. The corresponding property for $l = 2$ follows from the fact that $L_2/\mathbf{Q}$ is dihedral of order 8 and that τ is non-trivial on K and $\mathbf{Q}(\sqrt{\mathrm{N}_{K/\mathbf{Q}}(\alpha)})$.

Now let $l \notin \{2,3,5,7,13\}$ be a prime divisor of n. The extension L_l^{ab}/M_l is cyclic of degree $(l-1)/\gcd(l-1,6)$. This degree is larger than 2 by the assumptions on l. Therefore, the element $\tau|_{M_l}$ has an extension $\tau_l \in \mathrm{Gal}(L_l/\mathbf{Q})$ of order larger than 2. As ML_l is the disjoint compositum of M and L_l over M_l, there exists a unique $\sigma_l \in \mathrm{Gal}(ML_l/\mathbf{Q})$ extending both τ and τ_l. The element σ_l has the desired properties. □

7. Examples

In this section, we compute for four values of α the density of the sets S^+ and S^-. In the first 2 examples, these densities vanish. For the α's in the last 2 examples, we give explicit values of c_α^+ and c_α^-, by counting automorphisms with certain properties.

Example 1. For $\alpha = (\frac{15+3\sqrt{5}}{2})^{15}$, both S^+ and S^- have zero density.
This is just an easy corollary of theorem 3. The fact that α is a cube in $K = \mathbf{Q}(\sqrt{5})$ implies $\delta(S^-) = 0$. As $K(\sqrt{\alpha})$ is the maximal real subfield of $\mathbf{Q}(\zeta_{15})$, the second part of theorem 3a gives $\delta(S^+) = 0$.

Example 2. For $\alpha = -150 + 57\sqrt{7}$ the set S^- has zero density.
The field $K = \mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{7})$ has discriminant $D = 4 \cdot 7$. We can write $\alpha = \pi\bar{\pi}^4$, with $\pi = 2 + \sqrt{7}$ a generator of a prime above 3 in K, so α is not a cube in K^*. As the norm of α is not a square in K^*, the field $L_2 = K(\sqrt{\alpha}, \sqrt{\bar{\alpha}}) = K(\sqrt{\pi}, \sqrt{\bar{\pi}})$ is dihedral of order 8 over $\mathbf{Q}$ and the definition in the introduction gives $k_2 = \mathbf{Q}(\sqrt{\mathrm{N}_{K/\mathbf{Q}}(\alpha)}) = \mathbf{Q}(\sqrt{-3})$. Because of the equality $\frac{\alpha}{\bar{\alpha}} = (\frac{\bar{\pi}}{\pi})^3$, we have $k_3 = \mathbf{Q}(\sqrt{-3 \cdot 7})$. We find that K, k_2 and k_3 are the three quadratic fields in a V_4-extension of $\mathbf{Q}$, so $\delta(S^-) = 0$ by the second part of theorem 3b.

Example 3. Let $\beta = \frac{1+\sqrt{77}}{2}$ and $\alpha = (2-\beta)(1+\beta)^6(3-2\beta)^4(1+2\beta)^{-11} \in K = \mathbf{Q}(\sqrt{77})$. If GRH holds then

$$\delta(S^-) = \frac{10550659}{63836100} \cdot \prod_{\substack{l \text{ odd} \\ \text{prime}}} (1 - \frac{2}{l(l-1)}).$$

The elements $\pi_{17} = 2 - \beta$ and $\bar{\pi}_{17} = 1 + \beta$ generate the two primes above 17, and $\pi_{73} = 3 - 2\beta$ and $\bar{\pi}_{73} = 1 + 2\beta$ generate the two primes above 73. We have

$$\alpha = \pi_{17}\bar{\pi}_{17}^6\pi_{73}^4\bar{\pi}_{73}^{-11},$$

so α and $\bar{\alpha}$ are multiplicatively independent, and the following relations hold:

$$\text{(27)} \qquad \alpha\bar{\alpha} = \mathrm{N}_{K/\mathbf{Q}}(\alpha) = \left(\frac{17}{73}\right)^7; \quad \frac{\alpha}{\bar{\alpha}} = \left(\frac{\bar{\pi}_{17}\pi_{73}^3}{\pi_{17}\bar{\pi}_{73}^3}\right)^5.$$

Let t denote the order of the torsion subgroup of $K^*/\langle\alpha, \bar{\alpha}\rangle$, and let f be the conductor of L_2^{ab}/Q. If we assume GRH, theorem 16 gives the following formula for the density of S^-:

$$\text{(28)} \qquad \delta(S^-) = \delta(S_{2f}^-) \prod_{\substack{l \text{ prime} \\ l \nmid 2f, l \mid t}} (1 - \frac{c(l)}{[L_l : K]}) \prod_{\substack{l \text{ prime} \\ l \nmid 2ft}} (1 - \frac{2}{l(l-1)}).$$

First we compute the density of S_{2f}^-. As $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is not a square in K^*, the extension $L_2/\mathbf{Q}$ is dihedral of order 8 and $L_2^{\mathrm{ab}} = \mathbf{Q}(\sqrt{7 \cdot 11}, \sqrt{17 \cdot 73})$. We find the conductor $f = 7 \cdot 11 \cdot 17 \cdot 73$. Chebotarev's density theorem and proposition 5b give the equality

$$\text{(29)} \qquad \delta(S_{2f}^-) = \frac{\#G(2f)}{[L_{2f} : \mathbf{Q}]},$$

where

$$G(2f) = \{\sigma \in \mathrm{Gal}(L_{2f}/\mathbf{Q}) : \sigma|_K \neq \mathrm{id} \text{ and } \sigma|_{L_l}^2 \neq \mathrm{id} \text{ for all primes } l \mid 2f\}.$$

To compute $\#G(2f)$, we argue as in the proof of theorem 3b. For each prime l, let M_l be the maximal subfield of L_l of exponent 2 over $\mathbf{Q}$, and define M as the compositum of the fields $\{M_l\}_{l|2f}$ If l is an odd prime, we have $M_l = K(\sqrt{(\frac{-1}{l})l})$, a field of degree 4 over $\mathbf{Q}$. With $M_2 = L_2^{\mathrm{ab}}$ as above, this yields the equality

$$M = \mathbf{Q}(\sqrt{-7}, \sqrt{-11}, \sqrt{17}, \sqrt{73}),$$

a field of degree 16 over $\mathbf{Q}$. The fields $\{ML_l\}_{l|2f}$ are linearly disjoint over M by proposition 12. Therefore, the elements of $G(2f)$ correspond bijectively to the tuples $(\hat{\rho}_l)_{l|2f}$, where $\hat{\rho}_l \in \mathrm{Gal}(ML_l/\mathbf{Q})$ is an element of order larger than 2 that is non-trivial on K and for which $\hat{\rho}_l|_M$ is independent of l. To count for each prime $l \mid 2f$ the number of such $\hat{\rho}_l$, we fix $\rho \in \mathrm{Gal}(M/\mathbf{Q})$ with $\rho|_K \neq \mathrm{id}$. As M_l is the maximal exponent 2 extension in L_l, the fields L_l and M are disjoint over M_l. Therefore, an element $\hat{\rho}_l$ as above, is uniquely determined by ρ and an element $\rho_l \in \mathrm{Gal}(L_l/\mathbf{Q})$ of order larger than 2 with $\rho_l|_{M_l} = \rho|_{M_l}$. Trivially, the number of extensions of $\rho|_{M_l}$ to L_l is $[L_l : M_l]$. The above discussion leads to the following formula:

$$\#G(2f) = \sum_{\substack{\rho\in\mathrm{Gal}(M/\mathbf{Q}) \\ \rho|_K\neq\mathrm{id}}} \prod_{\substack{l|2f \\ \text{prime}}} \left([L_l : M_l] - e_l(\rho)\right), \tag{30}$$

with, for each prime $l \mid 2f$ and $\rho \in \mathrm{Gal}(M/\mathbf{Q})$ that is non-trivial on K,

$$e_l(\rho) = \#\{\rho_l \in \mathrm{Gal}(L_l/\mathbf{Q}) \text{ with } \rho_l|_{M_l} = \rho|_{M_l} \text{ and } \rho_l^2 = \mathrm{id}\}.$$

In other words, $e_l(\rho)$ counts the elements of the set C_l, defined in corollary 7, for which the action on M_l is given by ρ.

First we compute the degrees $[L_l : K]$. The field L_2 is of degree 4 over K. For odd primes l, we use proposition 8. To find l-torsion in $K^*/\langle\alpha, \bar{\alpha}\rangle$, we assume there are integers a and b, such that $\alpha^a\bar{\alpha}^b = \gamma^l$ for some $\gamma \in K^*$. If we take the norm to $\mathbf{Q}$ we find

$$\left(\frac{17}{73}\right)^{7(a+b)} = \mathrm{N}_{K/\mathbf{Q}}(\gamma)^l. \tag{31}$$

From (27), we know that $\mathrm{N}_{K/\mathbf{Q}}(\alpha) = \frac{17}{73}$ is a 7-torsion element in $K^*/\langle\alpha, \bar{\alpha}\rangle$. As $\frac{\alpha}{\bar{\alpha}}$ is not a 7-th power in K^*, we conclude that L_7 is of degree 7 over $K(\zeta_7)$. With the definition of N_7^1 and N_7^2 from proposition 6, we find

$$[L_7 : K] = 42, \quad [L_7 : KN_7^1] = 7, \quad [L_7 : KN_7^2] = 1.$$

If $l \neq 7$, the equality (31) implies $a \equiv -b \bmod l$, so that $\frac{\alpha}{\bar{\alpha}}$ is an l-th power in K^*. From (27) we see that l equals 5. As $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is not a 5-th power in K^*, we find $[L_5 : K(\zeta_5)] = 5$ and

$$[L_5 : K] = 20, \quad [L_5 : KN_5^1] = 1, \quad [L_5 : KN_5^2] = 5. \tag{32}$$

For odd primes $l \neq 5, 7$, the group $K^*/\langle\alpha, \bar{\alpha}\rangle$ has no l-torsion and proposition 8 yields

$$[L_l : K] = l^2(l-1), \quad [L_l : KN_l^1] = l, \quad [L_l : KN_l^2] = l.$$

As M_l/K is quadratic for all primes l, we can now compute the degree of L_{2f} with $f = 7 \cdot 11 \cdot 17 \cdot 73$ using the following formula:

$$[L_{2f} : \mathbf{Q}] = [M : \mathbf{Q}] \prod_{\substack{l \text{ prime} \\ l|2f}} [ML_l : M] = [M : \mathbf{Q}] \prod_{\substack{l \text{ prime} \\ l|2f}} [L_l : M_l]$$
$$= 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^2 \cdot 17^2 \cdot 73^2.$$

We use proposition 19 to limit the number of possible ρ's in (30): if for some $\rho \in \mathrm{Gal}(M/\mathbf{Q})$ there exists a prime $l \mid 2f$ for which $\rho|_{k_l}$ is trivial, then all extensions of ρ to L_l have order 2. For these ρ, we have $e_l(\rho) = [L_l : M_l]$, and the contribution to $G(2f)$ is 0. As 3 and 5 do not divide $2f$, the only fields involved are $k_2 = \mathbf{Q}(\sqrt{\mathrm{N}_{K/\mathbf{Q}}(\alpha)}) = \mathbf{Q}(\sqrt{17 \cdot 73})$ and K. In the table below we list the 4 elements of $\mathrm{Gal}(M/\mathbf{Q})$ that are non-trivial on both K and k_2. A plus sign indicates trivial action, a minus sign the non-trivial action.

ρ	$\sqrt{-7}$	$\sqrt{-11}$	$\sqrt{17}$	$\sqrt{73}$
$\rho_{(1)}$	$+$	$-$	$+$	$-$
$\rho_{(2)}$	$-$	$+$	$+$	$-$
$\rho_{(3)}$	$+$	$-$	$-$	$+$
$\rho_{(4)}$	$-$	$+$	$-$	$+$

We are left with computing the numbers $e_l(\rho)$ for $l \mid 2f$ and the 4 elements ρ in the table. As in the proof of proposition 6b, the fact that these ρ are non-trivial on both K and k_2, implies that all extensions of $\rho|_{M_2}$ to L_2 have order 4, thus $e_2(\rho) = 0$. For primes $l \equiv 3 \bmod 4$ we have $M_l \cap \mathbf{Q}(\zeta_l^+) = \mathbf{Q}$, so that $\rho|_{M_l}$ has an unique extension $\bar{\rho}_l$ to $M_l\mathbf{Q}(\zeta_l^+) = K(\zeta_l)$ of order 2. Let $N_{l,\rho}$ be the unique field in $\{N_l^1, N_l^2\}$ that contains the fixed field of $\bar{\rho}_l$. According to corollary 7 we have $e_l(\rho) = [L_l : KN_{l,\rho}]$. For primes $l \equiv 1 \bmod 4$ we have $M_l \cap \mathbf{Q}(\zeta_l^+) = \mathbf{Q}(\sqrt{l})$ and we distinguish two cases. If ρ is non-trivial on $\mathbf{Q}(\sqrt{l})$, there is no extension to $K(\zeta_l)$ of order 2, so that $e_l(\rho) = 0$. On the other hand, if ρ is trivial on $\mathbf{Q}(\sqrt{l})$, there are precisely 2 extensions to $K(\zeta_l)$ of order 2. Corollary 7 implies $e_l(\rho) = [L_l : KN_l^1] + [L_l : KN_l^2]$. If we substitute the degrees that we computed above, we find the following table.

ρ	$e_7(\rho)$	$e_{11}(\rho)$	$e_{17}(\rho)$	$e_{73}(\rho)$
$\rho_{(1)}$	7	11	34	0
$\rho_{(2)}$	1	11	34	0
$\rho_{(3)}$	7	11	0	146
$\rho_{(4)}$	1	11	0	146

Now we have all the information to compute (29). We find:

$$\delta(S_{2f}^-) = \frac{88661}{449680}.$$

As we saw above, the prime divisors of t, the order of the torsion subgroup of $K^*/\langle\alpha,\bar{\alpha}\rangle$, are 5 and 7. As 7 divides f, we only need $c(5)/[L_5 : K]$ in order to compute (28). Corollary 7 and (32) give $c(5)/[L_5 : K] = 3/10$. Substituting the values for $\delta(S_{2f}^-)$ and $c(5)/[L_5 : K]$ in (28) yields the result.

Example 4. Let $\alpha = (3 \cdot 23 \cdot (\frac{-13+3\sqrt{13}}{2}))^3 \in K = \mathbf{Q}(\sqrt{13})$. If GRH holds then

$$\delta(S^+) = \frac{23576564}{133666461} \cdot \prod_{l \text{ prime}} (1 - \frac{1}{l^2(l-1)}).$$

The element $\frac{-13+3\sqrt{13}}{2}$ is of norm 13. We find that $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ is a square in K^*, but not a square in $\mathbf{Q}^*$, so the extension $L_2/\mathbf{Q}$ is cyclic of degree 4. For each prime l, let M_l denote the maximal abelian subfield of L_l of exponent dividing 4. The extension $M_{13}/\mathbf{Q}$ is cyclic of degree 4, and $L_2 = M_2$ is the unique subfield of $M_{13}(\sqrt{3 \cdot 23})$ that is cyclic of degree 4 over $\mathbf{Q}$ and ramified above 3, 13 and 23. Therefore, the conductor f of $L_2/\mathbf{Q}$ is equal to $3 \cdot 13 \cdot 23$. To compute $\delta(S^+)$ we use formula (23). By Chebotarev's density theorem and proposition 5a we have

$$\delta(S_{2f}^+) = \frac{\#G(2f)}{[L_{2f} : \mathbf{Q}]},$$

where

$$G(2f) = \{\sigma \in \mathrm{Gal}(L_{2f}/K) : \sigma|_{L_l} \neq \mathrm{id} \text{ for all primes } l \mid 2f\}.$$

Let M be the compositum of the fields $\{M_l\}_{l|2f}$. Using the same arguments as in example 3, we find that the elements of $G(2f)$ correspond bijectively to the tuples $(\rho_l)_{l|2f}$, where $\rho_l \in \mathrm{Gal}(L_l/K)$ is non-trivial and such that $(\rho_l|_{M_l})_{l|2f}$ determine an unique $\rho \in \mathrm{Gal}(M/K)$. To compute $\#G(2f)$, we fix $\rho \in \mathrm{Gal}(M/K)$ and compute the number of tuples corresponding to ρ. First we note that M_2 equals L_2 and, as α is a cube in K^*, the field L_3 is equal to $M_3 = K(\zeta_3)$. Therefore, we may assume that the restrictions $\rho|_{M_2}$ and $\rho|_{M_3}$ are non-trivial. The field M is the disjoint compositum of the quadratic extensions M_3, M_{13} and M_{23} of K and M_2 is not contained in the compositum of any two of these fields. We conclude that we can restrict to two possible $\rho \in \mathrm{Gal}(M/K)$.

ρ	M_3	M_{13}	M_{23}
$\rho_{(1)}$	$-$	$+$	$+$
$\rho_{(2)}$	$-$	$-$	$-$

For each prime $l \mid 2f$ and $\rho \in \{\rho_{(1)}, \rho_{(2)}\}$, the number of extensions of $\rho|_{M_l}$ to a non-trivial element $\rho_l \in \mathrm{Gal}(L_l/K)$ is $[L_l : M_l] - 1$ or $[L_l : M_l]$, depending on whether $\rho|_{M_l}$ is trivial or not. Using that the quotient $\alpha/\bar{\alpha}$ is the sixth power of a fundamental unit in K, we find the elements α and $\bar{\alpha}$ to be multiplicatively independent. Moreover, the group $K^*/\langle\alpha,\bar{\alpha}\rangle$ has no l-torsion, for all primes $l \geq 5$. With proposition 8, we are now able to compute $\#G(2f)$ and $[L_{2f} : \mathbf{Q}]$:

$$\begin{aligned}\#G(2f) &= ([L_{13} : M_{13}] - 1)([L_{23} : M_{23}] - 1) + [L_{13} : M_{13}][L_{23} : M_{23}] \\ &= 11 \cdot 23 \cdot 23297\end{aligned}$$

$$[L_{2f} : \mathbf{Q}] = [M : \mathbf{Q}][L_{13} : M_{13}][L_{23} : M_{23}] = 2^4 \cdot 3 \cdot 11 \cdot 13^2 \cdot 23^2$$

Substituting this into (23) yields the result.

References

[1] E. ARTIN, *The collected papers of Emil Artin,* (eds S. Lang, J. Tate). Addison-Wesley, 1965.

[2] H. BILHARZ, *Primdivisoren mit vorgegebener Primitivwurzel.* Math. Ann. **114** (1937), 476–492.

[3] G. COOKE, P. J. WEINBERGER, *On the construction of division chains in algebraic number fields, with applications to SL_2.* Commun. Algebra **3** (1975), 481–524.

[4] H. W. LENSTRA, JR, *On Artin's conjecture and Euclid's algorithm in global fields.* Inv. Math. **42** (1977), 201–224.

[5] C. HOOLEY, *On Artin's conjecture.* J. Reine Angew. Math. **225** (1967), 209–220.

[6] P. MOREE, *Approximation of singular series and automata.* Manuscripta Math. **101** (2000), 385–399.

[7] M. RAM MURTY, *On Artin's Conjecture.* J. Number Theory **16** (1983), 147–168.

[8] H. ROSKAM, *A quadratic analogue of Artin's conjecture on primitive roots.* J. Number Theory **81** (2000), 93–109. Errata in J. Number Theory **85** (2000), 108.

[9] H. ROSKAM *Prime divisors of linear recurrences and Artin's primitive root conjecture for number fields.* J. Théor. Nombres Bordeaux **13** (2001), 303–314.

[10] J.-P. SERRE, *Quelques applications du théorème de densité de Chebotarev.* Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401.

[11] J.-P. SERRE, *Local Fields* (2nd corrected printing). Springer-Verlag, New York, 1995.

[12] P. J. WEINBERGER, *On euclidean rings of algebraic integers.* Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), 321–332. Amer. Math. Soc., Providence, R. I., 1973.

Hans ROSKAM
Mathematisch Instituut
Universiteit Leiden, P.O. Box 951
2300 RA Leiden, The Netherlands
E-mail : roskam@math.leidenuniv.nl