M-SECTABLE ANGLES AND THE DENSITY OF POLYNOMIAL IMAGES

PETER J. KAHN

Department of Mathematics
Cornell University
Ithaca, New York 14853

April 4, 2013
Revised April 26, 2013

Abstract. Let K be an algebraic number field with integer ring $\mathcal{O}_K$ and f a polynomial of degree > 1 in $\mathcal{O}_K[x]$. We use a *height function* on K [Lan] to define what we call the *density of* $f(K)$ *in* K . Using a counting theorem of Schanuel [Sch], we show that this quantity exists and is 0. Now assume further that K is a subfield of $\mathbb{R}$, and let m be a positive integer whose odd part is a product of one or more distinct Fermat primes. Let $\mathbf{m} - \mathbf{Sect}$ consist of all $\cos(\alpha)$ for angles α that are straightedge-and-compass m-sectable (e.g., trisectable when $m = 3$). We apply the result above to show that $\mathbf{m} - \mathbf{Sect} \cap K$ has density 0 in the set $[-1, 1] \cap K$.

1. Introduction

Let K be an algebraic number field with ring of integers $\mathcal{O}_K$, and choose a polynomial $f \in \mathcal{O}_K[x]$. For any element $a \in K$, set $p(x, a) = f(x) - a$. We are interested in the density in K of the set $Z_K(f)$ of all $a \in K$ such that $p(x, a)$ has a zero in K. An alternative description of $Z_K(f)$, of course, is that it is the set $f(K)$. But we prefer the first formulation for reasons that will become clear below.

To define density, we make use of the *height* function H_K (cf [Lan], Ch. 3), a non-negative, real-valued function on K with the following important property: For any real, non-negative B, the set $V_K(B)$ of all $a \in K$ such that $H_K(a) \leq B$ is finite. We describe H_K further in § 2. The *finite density* $\delta_K(Z_K(f); B)$ is defined to be the following ratio of cardinalities

$$\delta_K(Z_K(f); B) = \frac{|Z_K(f) \cap V_K(B)|}{|V_K(B)|}. \tag{1}$$

If $\lim_{B\to\infty} \delta_K(Z_K(f); B)$ exists, we denote it by $\delta_K(Z_K(f))$ and call it the *density* of $Z_K(f)$ in K.

Our main result about the density of such sets is the following:

Theorem 1.1. *(see Corollary 3.6): Let $f \in \mathcal{O}_K[x]$ be a degree d polynomial, $d > 1$. Then, there exist positive real numbers L_0 and B_0 such that, for $B \geq B_0$,*

$$\delta_K(Z_K(f); B) \leq L_0 B^{(2/d)-2}. \tag{2}$$

Therefore, the density $\delta_K(Z_K(f))$ exists and equals zero.

The constant L_0 is given explicitly in Corollary 3.6. However, B_0 has no such easy description. This theorem is proved in §3.

The motivation for this analysis of the sets $Z_K(f)$ does not lie strictly within the realm of algebra but rather with a particular application we have in mind. We first explain the motivation and then describe the application, which is our main interest.

The classical Greek angle trisection problem was solved in the negative in 1837 by the French mathematician P.-L. Wantzel [Wan]. Specifically, Wantzel established the following result:

Wantzel's Theorem: *Let α be an arbitrary angle and set $a = cos(\alpha)$. Let*

$$q(x, a) = 4x^3 - 3x - a.$$

Then α admits a trisection using only an unmarked straightedge and compass if and only if the polynomial $q(x, a)$ has a zero in the field $\mathbb{Q}(a)$.

There are many values of $a = \cos(\alpha)$ for which $q(x, a)$ has no such zero. (For example, choose $a = 3 \cdot 2^{-n}$, for $n \geq 2$, and apply Eisenstein's Theorem; also, cf. Lemma 5.1 e) and f), together with Lemma 5.2 a)). Thus, Wantzel's Theorem establishes the existence of non-trisectable angles.

This result and its proof are accessible to mid-level undergraduates (cf.,[Cou]), and, indeed, they formed a topic in an undergraduate course taught by the author for several years. Class discussions led to questions about the set of trisectable angles α or, essentially equivalently, the set of corresponding values $a = \cos(\alpha)$: for example, how large is this set?

Wantzel's Theorem implies a "quick and dirty" answer to this question via the observation that when α is trisectable, the value $\cos(\alpha)$ must be an algebraic number. (See Theorem 1.2 (b) below.) Thus, the set of trisectable angles is at most countable, hence very sparse in the set of all angles.

The algebraicity of cosines of trisectable angles suggests that we restrict attention to the field $\mathbb{A}$ of algebraic numbers—more exactly, to those algebraic numbers in the real interval $[-1, 1]$— and determine how densely such cosines populate $\mathbb{A} \cap [-1, 1]$. A finite-dimensional approximation to this seems more amenable, so in this paper we replace $\mathbb{A}$ by a finite-degree subfield, i.e., by an algebraic number field. Wantzel's criterion for trisectability then allows us to transform this question into one concerning polynomials, thus motivating Theorem 1.1. Given a real number field K, the set of all cosines in K corresponding to trisectable angles is clearly contained in the set $Z_K(4x^3 - 3x)$, thus explaining our original description of the sets $Z_K(f)$ and our interest in them.

The density we seek is, in fact, zero (Corollary 1.4). But before stating this result more precisely, we observe that the number three (underlying the notion of *tri*section) ought not to be uniquely privileged. We could, after all, seek a straightedge-and-compass-constructible equipartition of angles into m parts—which we call m-section—for any positive integer m. And, when m is a power of two, we have such a construction for every angle: simply bisect as often as needed. However, for any other integer m, the situation is different, as Theorem 1.2 below shows. To state this theorem, we introduce some notation and terminology that will be in force throughout the paper.

For every positive integer m, we let $T_m(x)$ denote the m^{th} *Chebyshev polynomial of the first kind* (see §5), and we set $P_m(x, a) = T_m(x) - a$, for any $a \in \mathbb{R}$. We note that $P_3(x, a)$ is precisely the polynomial $q(x, a)$ in Wantzel's Theorem.

Next, we find it convenient to identify angles with points on the unit circle in the complex numbers $\mathbb{C}$. This leads to our using non-standard notation of the form $e^{i\theta}$ for angles. For example, instead of 90° or $\pi/2$, we shall denote that angle by $e^{\pi i/2}$. Further, standard angle sums will appear here as products of unit complex numbers, and angle multiples will appear as powers of unit complex numbers.

Finally, we introduce the notion of a *Gauss number*. For any positive integer m, let m_{odd} denote its odd part, that is, its maximum, positive odd divisor. We say that m is a Gauss number, if $m_{odd} = 1$ or if m_{odd} is a product of one or more distinct Fermat primes, that is, primes of the form $2^{2^k} + 1$. The values $k = 0, 1, 2, 3, 4$ produce primes 3, 5, 17, 257, 65537, respectively. The author is unaware of any other Fermat primes. The terminology *Gauss number* is motivated by the following celebrated result:

Gauss's Theorem: The positive integer m is a Gauss number if and only if the angle $e^{2\pi i/m}$ is constructible. □

The following theorem will be proved in §5.

Theorem 1.2. *Let m be any positive integer.*

(a) $m_{odd} = 1$ *if and only if every angle is m-sectable .*

(b) *Suppose $m_{odd} \neq 1$ and α is an m-sectable angle. Then $a = \cos(\alpha)$ is an algebraic number.*

(c) *Suppose that m is a Gauss number. Then an angle α is m-sectable if and only if the polynomial $P_{m_{odd}}(x, \cos(\alpha))$ has a zero in $\mathbb{Q}(\cos(\alpha))$.*

Remarks: (1) The interesting part of statement (a) is that the m-sectability of all angles implies that $m_{odd} = 1$.

(2) Statement (b) of the theorem implies that when $m_{odd} \neq 1$, there are at most countably many m-sectable angles and that we should look for their cosines among the algebraic numbers (in $[-1, 1]$), just as in the special case of $m = 3$. Thus, we are led to ask how densely such cosines populate $K \cap [-1, 1]$, for K a real number field.

(3) We can get an estimate for this density for certain m via the criterion given in statement (c) of the theorem, together with Corollary 3.6 (or Theorem 1.1).

(4) *Statement (c) of the theorem generalizes Wantzel's criterion for trisectability.*

> Here is an example showing that statement (c) would be *false* if we used $P_m(x, \cos(\alpha))$ rather than $P_{m_{odd}}(x, \cos(\alpha))$ in the statement. Let $m = 6$, and choose $\alpha = e^{\pi i/2}$. Of course $\cos(\alpha) = 0$, so $P_6(x, \cos(\alpha)) = T_6(x) = 32x^6 - 48x^4 + 18x^2 - 1$ (see §5). Since $e^{\pi i/6}$, which trisects α, is constructible and can then be bisected, α is $6 - \textit{sectable}$. However, $T_6(x)$ has the following factorization into *irreducibles* over $\mathbb{Q}$: $(2x^2-1)(16x^4-16x^2+1)$. Hence, $P_6(x, \cos(\alpha))$ has no zero in $\mathbb{Q}(\cos(\alpha))$. But $m = 6$ is a Gauss number, so statement (c) does apply: $6_{odd} = 3$, and $P_3(x, \cos(\alpha)) = T_3(x) = 4x^3 - 3x$ which does have a zero in $\mathbb{Q}(\cos(\alpha)) = \mathbb{Q}$.

We can now state our main results. Theorem 1.1 and statement (c) of Theorem 1.2 allow us to bound the number of cosines of m-sectable angles in terms of their height (Theorem 1.3). As a corollary to this theorem, we get the desired density result (Corollary 1.4).

Theorem 1.3. *Let $K \subset \mathbb{R}$, be an algebraic number field of degree $[K : \mathbb{Q}] = n$, and let m be a positive integer. We denote by m_g the largest odd Gauss number dividing m. Finally, we let* $\mathbf{m} - \mathbf{Sect}$ *consist of all $a = \cos(\alpha) \in K$ for which α is m-sectable. Then, for any λ such that $1/2 < \lambda < 1$, there exist constants $B_0 > 0$, $\mathfrak{S} > 0$ and $\|T_{m_g}\|$ such that, when $B \geq B_0$,*

$$|\mathbf{m} - \mathbf{Sect} \cap V_K(B)| \leq \lambda \mathfrak{S} \cdot (2\|T_{m_g}\|)^{2n} B^{2/m_g}.$$

Here the quantity $\mathfrak{S}$ is Schanuel's constant (cf. Schanuel's Theorem in §2.3 below), whereas $\|T_{m_g}\|$ is the sum of the absolute values of the coefficients of the Chebyshev polynomial $T_{m_g}(x)$. We leave the verification of the following formula to the reader: Let k be a positive, odd integer. Then,

$$\|T_k\| = \frac{1}{2}\left((\sqrt{2}+1)^k - (\sqrt{2}-1)^k\right) = \sinh(k\ln(\sqrt{2}+1)).$$

.

The proofs of Theorem 1.3 and Corollary 1.4 are given in §6.

Corollary 1.4. *Assume that m is a positive integer and that m_g is the largest odd Gauss number dividing m. There exists a positive B_1 such that if $B \geq B_1$, then*

$$\delta_K(\mathbf{m}-\mathbf{Sect}; B) \leq (2\|T_{m_g}\|)^{2n} B^{(2/m_g)-2}.$$

Therefore, when $m_g \neq 1$, $\delta_K(\mathbf{m}-\mathbf{Sect})$ exists and equals 0.

We note that the results of this paper always occur in the context of a fixed algebraic number field K. This is not completely satisfactory, because our overarching interest concerns the density of $\mathbf{m}-\mathbf{Sect}$ in $\mathbb{A}$ (or more precisely, in $\mathbb{A}\cap[-1,1]$). Therefore, we are interested in what happens to the estimates as the field K varies. It is for this reason that a specific constant appears as a coefficient in our estimates above; for a fixed field K we could content ourselves with the fact that the estimates hold for *some* unspecified or or even uncomputable constant. The conclusion about density existing and equalling 0 would still follow. The case of a variable K and the density of $\mathbf{m}-\mathbf{Sect}$ in $\mathbb{A}\cap[-1,1]$ will be addressed in a subsequent paper.

2. Preliminaries

2.1. Let K be an algebraic number field of degree $n = [K:\mathbb{Q}] = s+2t$, where s is the number of real embeddings of K into the field $\mathbb{C}$ of complex numbers and t is the number of conjugate pairs of complex embeddings. Let $\sigma_i, i = 1,\ldots,s$, denote the real embeddings, and let $\sigma_j, j = s+1,\ldots,s+t$ denote complex embeddings, choosing one of these for each conjugate pair. Each σ_h induces an absolute value $|\ |_h$ on K via the rule $|x|_h = |\sigma_h(x)|$, where the unadorned $|\ |$ denotes the standard absolute value on $\mathbb{C}$.

For each $\alpha \in K$, one can define the *height* $H_K(\alpha)$ by the following rule: Write the fractional ideal generated by α as a quotient of ideals $\mathfrak{b},\mathfrak{c}$ in the ring of integers $\mathcal{O}_K$, $\mathfrak{c}$ non-zero: $<\alpha>=\mathfrak{b}\mathfrak{c}^{-1}$. It will be convenient not to insist here that $\mathfrak{b}$ and $\mathfrak{c}$ are coprime. Let $\mathfrak{g}$ denote the ideal which is their greatest common divisor $gcd(\mathfrak{b},\mathfrak{c})$. Then,

$$H_K(\alpha) = \mathbf{N}(\mathfrak{g}^{-1}\mathfrak{c})\prod_{h=1}^{s+t} sup(1, |\alpha|_h^{N_h}), \tag{3}$$

where $N_h = 1$ for $h \leq s$, $N_h = 2$ for $h > s$, and $\mathbf{N}(\mathfrak{g}^{-1}\mathfrak{c})$ is the absolute norm, i.e., the cardinality $|\mathcal{O}_K/\mathfrak{g}^{-1}\mathfrak{c}|$. See [Lan], Chapter 3 for further details.

We shall make important use of three properties of the function H_K. The first is the already-mentioned finiteness of the sets $V_K(B) = \{x \in K : H_K(x) \leq B\}$, for each non-negative, real B. The other properties of H_K are as follows.

(a) It is invariant under inversion:

$$H_K(x) = H_K(x^{-1}), \tag{4}$$

valid for every non-zero $x \in K$;

(b) It respects exponentiation:

$$H_K(x^e) = H_K(x)^e, \tag{5}$$

valid for every non-negative integer e.

2.2. Suppose we are given: (1) a pair of sets S, T such that $S \subseteq T \subseteq \mathbb{C}$ and $0 \in T$; (2) an algebraic number field K embedded in $\mathbb{C}$; (3) a positive, real B. We then define the *finite density* $\delta_K(S, T; B)$ by

$$\delta_K(S, T; B) = \frac{|V_K(B) \cap S|}{|V_K(B) \cap T|}. \tag{6}$$

If S (resp. T) contains K, we may omit reference to S (resp. T).

If $\lim_{B\to\infty} \delta_K(S, T; B)$ exists, we denote it by $\delta_K(S, T)$ and call it the *density* of $K \cap S$ in $K \cap T$.

2.3. The following is a special case of a theorem of S. Schanuel [Sch]. It will be used for our estimate of finite densities.

Theorem 2.1 (Schanuel's Theorem). *Let K be an algebraic number field of degree $[K : \mathbb{Q}] = n$, and let B be a real number > 1. Then, there exists a constant $\mathfrak{S}$ depending only on K, such that*

$$|V_K(B)| = \mathfrak{S} \cdot B^2 + \mathbf{O}(C(n, B)),$$

where

$$C(n, B) = \begin{cases} B \log B & : \quad n = 1 \\ B^{1/n} & : \quad n \geq 2 \end{cases}.$$

Remarks: a) Schanuel computes $\mathfrak{S}$ explicitly in terms of standard numerical invariants of the field K (see [Lan] or [Sch]). For example, when $n = 1$, $\mathfrak{S}$ reduces to $6/\pi^2$. The precise value of $\mathfrak{S}$ is not needed in this paper.

b) The term "$\mathbf{O}(C(n, B))$" follows the standard "big oh" convention.

2.4. We continue with the terminology of the previous sections. We are interested in the set

$$V_K(B)\cap Z_K(f) = \{a \in K : p(x,a) \text{ has a zero in } K \text{ and } H_K(a) \leq B\} = V_K(B)\cap f(K).$$

In particular, we are interested in the cardinality $|V_K(B)\cap Z_K(f)|$, for large B, and in the finite density

$$\delta_K(Z_K(f);B) = \frac{|V_K(B)\cap Z_K(f)|}{|V_K(B)|}.$$

Our procedure will be to show that $|V_K(B)\cap Z_K(f)|$ is dominated by $|V_K(cB^t)|$, for some real constants c and t independent of B, and then to apply Schanuel's Theorem to this last.

3. Computing $|V_K(B)\cap Z_K(f)|$

We write $f(x) = a_d x^d + \dots a_1 x + a_0$, where each $a_i \in \mathcal{O}_K$, and we continue with this notation throughout the paper.

As noted above,

$$V_K(B)\cap Z_K(f) = V_K(B)\cap f(K).$$

Therefore, to compare $|V_K(B)\cap Z_K(f)|$ with $|V_K(B)|$, we proceed by estimating $H_K(f(\alpha))$ in terms of $H_K(\alpha)$, for any non-zero $\alpha \in K$.

Write $\alpha = \beta/\gamma$, for some $\beta,\gamma \in \mathcal{O}_K$, and denote the principal ideals $<\beta>, <\gamma>$ by $\mathfrak{b},\mathfrak{c}$, respectively. Let $\mathfrak{g} = \gcd(\mathfrak{b},\mathfrak{c})$. Then, by (3),

$$H_K(\alpha) = \mathbf{N}(\mathfrak{g}^{-1}\mathfrak{c})\prod_{h=1}^{s+t}\sup(1,|\alpha|_h^{N_h}). \tag{7}$$

Note that $\gamma^d f(\alpha) \in \mathcal{O}_K$, so we may write $f(\alpha)$ as a quotient $\gamma^d f(\alpha)/\gamma^d$ of two K-integers. Let $\mathfrak{d} =< \gamma^d f(\alpha) >$. Then $< f(\alpha) >= \mathfrak{d}(\mathfrak{c}^d)^{-1}$. If $\mathfrak{G}$ denotes $\gcd(\mathfrak{d},\mathfrak{c}^d)$, then

$$H_K(f(\alpha)) = \mathbf{N}(\mathfrak{G}^{-1}\mathfrak{c}^d)\prod_{h=1}^{s+t}\sup(1,|f(\alpha)|_h^{N_h}). \tag{8}$$

Therefore, to compare $H_K(\alpha)$ with $H_K(f(\alpha))$, we must compare $\mathfrak{g}$ with $\mathfrak{G}$ and $|\alpha|_h^{N_h}$ with $|f(\alpha)|_h^{N_h}$, for each $h = 1,\dots,s+t$.

3.1. Comparing $\mathfrak{g}$ with $\mathfrak{G}$. We have $\gamma^d f(\alpha) = a_d\beta^d + a_{d-1}\gamma\beta^{d-1} + \dots a_1\gamma^{d-1}\beta + a_0\gamma^d$ so that

$$a_d^{d-1}\gamma^d f(\alpha) = (a_d\beta)^d + a_{d-1}\gamma(a_d\beta)^{d-1} + \dots + a_d^{d-i-1}a_i\gamma^{d-i}(a_d\beta)^i + \dots + a_d^{d-1}a_0\gamma^d. \tag{9}$$

Recall that $\mathfrak{b} =< \beta >$, $\mathfrak{c} =< \gamma >$, and $\mathfrak{d} =< \gamma^d f(\alpha) >$. We use (9) to prove

Lemma 3.1. *$gcd(a_d^{d-1}\mathfrak{d},\mathfrak{c}^d) = gcd(a_d\mathfrak{b},\mathfrak{c})^d$.*

Proof. First we show that both ideals have the same prime divisors. Let $\mathfrak{p}$ be a prime ideal dividing the right-hand side (RHS) in the statement of the lemma. Then $\mathfrak{p}|a_d\mathfrak{b}$ and $\mathfrak{p}|\mathfrak{c}$. With the aid of (9), it is easy to see that $\mathfrak{p}$ divides the LHS. Next suppose that a prime, again called $\mathfrak{p}$, divides the LHS. Then, $\mathfrak{p}|\mathfrak{c}$ and $\mathfrak{p}|a_d^{d-1}\mathfrak{d}$, and, using (9) again, we see that $\mathfrak{p}|(a_d\mathfrak{b})^d$, hence $\mathfrak{p}|$ RHS.

Next let $\mathfrak{p}$ be a prime factor occurring with exponent e in the prime factorization of the RHS. We shall show that it occurs with the same exponent on the LHS. Since the RHS is a d^{th} power, e has the form cd, for some $c \geq 1$. But then $\mathfrak{p}^c|gcd(a_d\mathfrak{b}, \mathfrak{c})$, by unique factorization of ideals, so $\mathfrak{p}^c|a_d\mathfrak{b}$ and $\mathfrak{p}^c|\mathfrak{c}$. It follows that $\mathfrak{p}^e|\mathfrak{c}^d$ and,

$$\mathfrak{p}^e|(a_d\mathfrak{b})^d \quad \text{and} \quad \mathfrak{p}^e| < a_d^{d-i-1}a_i\gamma^{d-i}(a_d\beta)^i >,$$

for each $i = d-1, d-2, \ldots, 0$, i.e., each principal ideal generated by the terms on the right-hand side of (9). So, using (9) again, we can conclude that $\mathfrak{p}^e|a_d^{d-1}\mathfrak{d}$. Therefore, $\mathfrak{p}^e$ divides the LHS. Since this holds for all prime divisors of the RHS, we may conclude that the RHS divides the LHS.

Finally, suppose that $\mathfrak{p}, c, d, e$ are as in the previous paragraph and that $\mathfrak{p}^{e+1}|$ LHS, so that $\mathfrak{p}^{e+1}|\mathfrak{c}^d$. But the prime factors of $\mathfrak{c}^d$ must have exponents that are multiples of d. Since $e+1 = cd+1$, it follows that $\mathfrak{p}^{(c+1)d}|\mathfrak{c}^d$, hence that $\mathfrak{p}^{c+1}|\mathfrak{c}$. Therefore, each term of the form $a_d^{d-i-1}a_i\gamma^{d-i}(a_d\beta)^i, i = d-1, d-2, \ldots, 0$, on the right-hand side of (9), belongs to the ideal $\mathfrak{p}^{(d-i)(c+1)} \cdot \mathfrak{p}^{ci} = \mathfrak{p}^{cd+d-i}$, hence to the ideal $\mathfrak{p}^{cd+1}$, so that (again via (9)) $\mathfrak{p}^{cd+1}|(a_d\mathfrak{b})^d$. As just argued, this implies that $\mathfrak{p}^{(c+1)d}|(a_d\mathfrak{b})^d$, hence that $\mathfrak{p}^{c+1}|a_d\mathfrak{b}$. Combining this with the already-proved relation $\mathfrak{p}^{c+1}|\mathfrak{c}$, we conclude that $\mathfrak{p}^{(c+1)d}$ divides the RHS in the statement of the lemma, contradicting the fact that $\mathfrak{p}$ has exponent $e = cd$ on the RHS.

It follows that $\mathfrak{p}$ must also occur with exponent e in the prime factorization of the LHS, completing the proof of the lemma.

□

Corollary 3.1. *(a)* $\mathfrak{g}^d$ *divides* $a_d^{d-1}\mathfrak{G}$. *(b)* $\mathfrak{G}$ *divides* $a_d^d\mathfrak{g}^d$.

Proof. (a) $\mathfrak{g}^d$ divides $\gcd(a_d\mathfrak{b}, \mathfrak{c})^d$, which, by the lemma, equals $\gcd(a_d^{d-1}\mathfrak{d}, \mathfrak{c}^d)$. This last clearly divides $a_d^{d-1}\mathfrak{G}$.

(b) $\mathfrak{G} = \gcd(\mathfrak{d}, \mathfrak{c}^d)$, which divides $\gcd(a_d^{d-1}\mathfrak{d}, \mathfrak{c}^d) = \gcd(a_d\mathfrak{b}, \mathfrak{c})^d$, and this last clearly divides $a_d^d\mathfrak{g}^d$. □

We apply this corollary to obtain

Corollary 3.2. *Set* $\mathbf{N}(< a_d >) = \kappa$. *Then*

$$\kappa^{-d}\mathbf{N}(\mathfrak{g}^{-d}) \leq \mathbf{N}(\mathfrak{G}^{-1}) \leq \kappa^{d-1}\mathbf{N}(\mathfrak{g}^{-d}). \quad \square$$

3.2. Comparing $|\alpha|_h^{N_h}$ with $|f(\alpha)|_h^{N_h}$. Note that $|\alpha|_h^{N_h}$ and $|f(\alpha)|_h^{N_h}$ are equal to $|\sigma_h(\alpha)|^{N_h}$ and $|f(\sigma_h(\alpha))|^{N_h}$, respectively, where $\sigma_h : K \to \mathbb{C}$ is an embedding of K, and $N_h = 1$ or 2 according as $h = 1, \ldots, s$ or $h = s+1, \ldots, s+t$, respectively. Therefore, we must compare $\sup(1, |x|)^e$ and $\sup(1, |f(x)|)^e$, for x ranging over $\mathbb{C}$ and

$e = 1, 2$. More precisely, we shall obtain upper and lower bounds for the quotient of the latter function by $\sup(1, |x^d|)^e$. For $e = 1, 2$, define

$$\begin{aligned}
Q_e(x) &= \frac{\sup(1, |f(x)|^e)}{\sup(1, |x^d|^e)} && (10)\\
\|f\| &= |a_d| + \ldots + |a_0| && (11)\\
U &= \sup(1, \|f\|) && (12)\\
L &= \inf\left(\left|\frac{a_d}{2}\right|, \left|\frac{a_d}{2\|f\|}\right|^d\right). && (13)
\end{aligned}$$

Lemma 3.2. *For all $x \in \mathbb{C}$,*

$$L^e \leq Q_e(x) \leq U^e.$$

Proof. It is not hard to see from general observations that the function Q_e has positive upper and lower bounds. The point of the lemma is that it produces explicit ones that are easily calculated.

We begin by noting that

$$Q_e(x) = \begin{cases} \sup(1, |f(x)|^e) & : \quad |x| \leq 1, \\ \sup(1, |f(x)|^e)|x^d|^{-e} & : \quad |x| \geq 1 \end{cases}.$$

Now we calculate the upper bound. When $|x| \leq 1$, the usual triangle inequality shows immediately that $\sup(1, |f(x)|^e) \leq \sup(1, \|f\|)^e$. When $|x| \geq 1$, we note that

$$(|f(x)|^e)|x^d|^{-e} = |a_d + a_{d-1}(1/x) + \ldots + a_1(1/x^{d-1}) + a_0(1/x^d)|^e,$$

and the triangle inequality again implies that $\sup(1, \|f\|)^e$ is an upper bound.

Next, we deal with the lower bound. It follows directly from the definition that $L \leq 1/2^d$. When $|x| \leq 1$, then clearly $Q_e(x) \geq 1$, implying that L^e is a lower bound in this case.

When $|x| \geq 1$ the calculation is more complicated. We set

$$R = \frac{2\|f\|}{|a_d|}.$$

(Note that $R \geq 2$.) There are two cases:

Case 1: $|x| \geq R$. We compute $Q_e(x) =$

$$\begin{aligned}
|f(x)|^e|x^d|^{-e} &= |a_d + a_{d-1}(1/x) \ldots + a_1(1/x)^{d-1} + a_0(1/x)^d|^{\,e} \\
&\geq ||a_d| - |a_{d-1}(1/x) + \ldots + a_1(1/x)^{d-1} + a_0(1/x)^d||^{\,e}.
\end{aligned}$$

The subtrahend $|a_{d-1}(1/x) + \ldots + a_0(1/x)^d|$ on the right-hand side of the inequality is dominated by $(|a_{d-1}| + \ldots + |a_0|)/R = |a_d|(|a_{d-1}| + \ldots + |a_0|)/2\|f\| < |a_d|/2$, the inequality at the end coming from the fact that $\|f\| > |a_{d-1}| + \ldots + |a_0|$. Therefore, we get $Q_e(x) > |a_d/2|^e$ in this case.

Case 2: $1 \leq |x| \leq R$. In this case, $1 \leq |x^d| \leq (2\|f\|/|a_d|)^d$. Therefore, $Q_e(x) = \sup(|x^d|^{-e}, |f(x)||x^d|^{-e}) \geq |x^d|^{-e} \geq (|a_d|/2\|f\|)^{de}$.

We can then combine the two cases to obtain

$$Q_e(x) \geq \inf\left(\left|\frac{a_d}{2}\right|, \left|\frac{a_d}{2\|f\|}\right|^d\right)^e = L^e$$

as desired.

□

3.3. Comparing $H_K(f(\alpha))$ with $H_K(\alpha^d)$.

Lemma 3.3. *Let κ, U, and L be as defined in the preceding two subsections, and recall that $n = [K : \mathbb{Q}]$. Then*

$$\kappa^{-d} L^n \leq \frac{H_K(f(\alpha))}{H_K(\alpha^d)} \leq \kappa^{d-1} U^n$$

Proof. We first verify that

$$\frac{H_K(f(\alpha))}{H_K(\alpha^d)} = \frac{\mathbf{N}(\mathfrak{G}^{-1})}{\mathbf{N}(\mathfrak{g}^{-d})} \cdot \prod_{h=1}^{s+t} \frac{\sup(1, |f(\sigma_h(\alpha))|^{N_h})}{\sup(1, |\sigma_h(\alpha)^{dN_h}|)},$$

and then that the right-hand side, in turn, equals

$$\frac{\mathbf{N}(\mathfrak{G}^{-1})}{\mathbf{N}(\mathfrak{g}^{-d})} \cdot \prod_{h=1}^{s+t} Q_{N_h}(\sigma_h(\alpha)).$$

We then apply Corollary 3.2 and Lemma 3.2 to this last expression, observing that

$$\sum_{h=1}^{s+t} N_h = n.$$

□

3.4. Evaluating $|V_K(B) \cap Z_K(f)|$.

Recall that $Z_K(f)$ is identical with the range $f(K)$. When we combine this with Lemma 3.3, we obtain the following:

Corollary 3.3.

$$f(V_K((\kappa^{1-d}U^{-n}B)^{1/d})) \subseteq V_K(B) \cap Z_K(f) \subseteq f(V_K((\kappa(L^{-n}B)^{1/d})). \tag{14}$$

Proof. The verifications of the two inclusions are almost the same. We prove the right-hand inclusion and leave the other to the reader. Suppose $\beta \in V_K(B) \cap f(K)$, i.e. $\beta = f(\alpha)$, for some $\alpha \in K$, and $H_K(f(\alpha)) \leq B$. By Lemma 3.3, $\kappa^{-d}L^n H_K(\alpha^d) \leq B$. Therefore, $H_K(\alpha)^d \leq \kappa^d L^{-n} B$, and hence $H_K(\alpha) \leq \kappa(L^{-n}B)^{1/d}$, i.e., $\alpha \in V_K(\kappa(L^{-n}B)^{1/d})$. Apply f to this last relation. □

Corollary 3.4.

$$|V_K((\kappa^{1-d}U^{-n}B)^{1/d})|/d \leq |V_K(B) \cap Z_K(f)| \leq |V_K((\kappa(L^{-n}B)^{1/d})|.$$

Proof. Since f is a degree d polynomial defined on K, for every subset S of K,we have the following comparison of cardinalities: $|S|/d \leq |f(S)| \leq |S|$. Apply this to the sets in the preceding corollary. □

We now apply Schanuel's Theorem to Corollary 3.4.

Corollary 3.5.

$$\begin{aligned}(\frac{1}{d}\mathfrak{S}\cdot(\kappa^{1-d}U^{-n})^{2/d}B^{2/d} + \mathbf{O}(C(n,(\kappa^{1-d}U^{-n}B)^{1/d})) \leq \\ |V_K(B)\cap Z_K(f)| \quad &\leq \quad \mathfrak{S}\cdot(\kappa L^{-n})^{2/d}B^{2/d} + \mathbf{O}(C(n,(\kappa L^{-n}B)^{1/d})).\end{aligned}$$

Before stating the next corollary (which gives Theorem 1.1), we remind the reader that

$$\kappa = \mathbf{N}(< a_d >),$$

where $\mathbf{N}$ is the absolute norm on $\mathcal{O}_K$, and a_d is the leading coefficient of f. Also

$$L = \inf\left(\left|\frac{a_d}{2}\right|, \left|\frac{a_d}{2\|f\|}\right|^d\right).$$

Corollary 3.6 (cf. Theorem 1.1). *Let K be an algebraic number field of degree n, and let f be any degree d polynomial in $\mathcal{O}_K[x]$, with $d > 1$. For any ϵ strictly between 0 and 1, there exists a positive B_0, such that, for $B \geq B_0$, the finite density $\delta_K(Z_K(f);B)$ satisfies*

$$\delta_K(Z_K(f);B) \leq (1+\epsilon)\kappa^{2/d}L^{-2n/d}B^{(2/d)-2}.$$

Therefore, $\delta_K(Z_K(f) := \lim_{B\to\infty}\delta_K(Z_K(f);B)$ exists and equals zero.

For Theorem 1.1 in the Introduction, we can take ϵ equal to, say, 1/2 and the constant L_0, then, to equal $(3/2)\kappa^{2/d}L^{-2n/d}$.

It is worth noting that Schanuel's constant $\mathfrak{S}$ disappears in the estimate for δ_K.

Proof. By Schanuel's Theorem (see 2.1), $|V_K(B)| = \mathfrak{S}\cdot B^2 + \mathbf{O}(C(n,B))$. Divide this into the last expression in Corollary 3.5. The result is

$$\delta_K(Z_K(f);B) \leq \frac{\mathfrak{S}\cdot(\kappa L^{-n})^{2/d}B^{2/d} + \mathbf{O}(C(n,(\kappa L^{-n}B)^{1/d})}{\mathfrak{S}\cdot B^2 + \mathbf{O}(C(n,B))}. \tag{15}$$

Assume now that $n \geq 2$, so that $C(n,B) = B^{1/n}$. The quantity B^2 grows much faster than $B^{1/n}$ as B goes to infinity. Therefore, for any ϵ strictly between 0 and 1, there exists a B_1 such that, for $B \geq B_1$, $(1-(\epsilon/2))\mathfrak{S}\cdot B^2 \leq \mathfrak{S}\cdot B^2 + \mathbf{O}(B^{1/n})$.

Applying this to (15) and simplifying, we get

$$\delta_K(Z_K(f);B) \leq \frac{(\mathfrak{S}\cdot(\kappa L^{-n})^{2/d})B^{2/d}+\mathbf{O}(B^{1/nd})}{(1-(\epsilon/2))\mathfrak{S}\cdot B^2} \tag{16}$$

$$\leq \left(\frac{1}{1-(\epsilon/2)}\right)(\kappa L^{-n})^{2/d}B^{(2/d)-2}+\mathbf{O}(B^{(1/nd)-2}). \tag{17}$$

Finally, we observe that $B^{(2/d)-2}$ decreases more slowly than $B^{(1/nd)-2}$ as B gets large, and also that $(1-(\epsilon/2))^{-1}$ is strictly smaller than $1+\epsilon$ when ϵ is strictly between 0 and 1. Therefore, there exists a $B_0 \geq B_1$ such that, for $B \geq B_0$,

$$\delta_K(Z_K(f);B) \leq (1+\epsilon)(\kappa L^{-n})^{2/d}B^{(2/d)-2}, \tag{18}$$

which is the desired estimate.

The case $n = 1$ is proved similarly and is left to the reader. □

4. Intersecting with $[-1,1]$.

Our main application of the foregoing results involves angle cosines, which are real numbers lying in the interval $[-1,1]$. Therefore, we should be estimating the size of the sets $V_K(B)\cap[-1,1]$, as well as densities relative to these. This section shows how to obtain these estimates quite easily in terms of those for the sets $V_K(B)$. Since we are dealing with real numbers in $V_K(B)$, we shall assume in this section that K is a subfield of $\mathbb{R}$. Let $K^* = K \setminus \{0\}$.

Let $I : K^* \to K^*$ denote the inversion $\alpha \mapsto \alpha^{-1}$. It gives a bijection

$$K^* \cap [-1,1] \to K^* \setminus (-1,1),$$

where here $(-1,1)$ denotes the interior of the interval $[-1,1]$. As noted earlier in equation (4), $H_K(\alpha) = H_K(I(\alpha))$, for all non-zero $\alpha \in K$, so I induces a bijection of finite sets $V_K(B)\cap K^*\cap[-1,1] \to V_K(B)\cap(K^*\setminus(-1,1))$. When $B \geq 1$, these sets intersect in $\{-1,1\}$, and their union is $V_K(B)\cap K^* = V_K(B)\setminus\{0\}$. It follows that

$$2|V_K(B)\cap K^*\cap[-1,1]| - 2 = |V_K(B)| - 1. \tag{19}$$

But $V_K(B)\cap[-1,1] = (V_K(B)\cap K^*\cap[-1,1])\cup\{0\}$, so $|V_K(B)\cap[-1,1]| - 1 = |V_K(B)\cap K^*\cap[-1,1]|$. Combining this with equation (19), we get the following:

Lemma 4.1. *For any real $B \geq 1$,*

$$|V_K(B)\cap[-1,1]| = \frac{1}{2}(|V_K(B)|+3).$$

5. m-sectability of angles and Chebyshev polynomials

We begin here by establishing our notation and conventions and by reminding the reader of some basic facts about constructibility. (For an elementary treatment of constructibility, the reader may consult [Cou].) We identify the Cartesian plane with the complex numbers and the X-axis with the real numbers in the usual way. As described earlier, for us an *angle* will mean a complex number of unit length, and angle sums will be products of such numbers and angle multiples will be powers. Given a set S of complex numbers that includes the numbers 0 and 1, we say that a number α is *constructible over* S if there exists a straightedge and compass construction starting with the numbers in S and resulting in α. *When* $S = \{0, 1\}$, *we say simply that* α *is constructible.*

Let $RI(S)$ denote the set of real and imaginary parts of the numbers in S. Clearly a complex number α is constructible over S if and only if it is constructible over $RI(S)$, and this is true if and only if both the real and imaginary parts of α are constructible over S (equivalently, over $RI(S)$, or equivalently, over the field $\mathbb{Q}(RI(S))$). When α is an angle, the constructibility of either $a = \cos(\alpha)$ or $b = \sin(\alpha)$ implies the constructibility of the other, hence of α. Thus, for example the angle β is constructible over $\{0, 1, \alpha\}$ if and only if $\cos(\beta)$ is constructible over the field $\mathbb{Q}(\cos(\alpha))$.

The *fundamental theorem of constructible numbers* asserts that a real number r is constructible over a subfield $F \subseteq \mathbb{R}$ if and only if there is a finite tower $F = F_0 \subset F_1 \subset \ldots \subset F_k$ such that (i) $r \in F_k \subset \mathbb{R}$; (ii) each extension $F_i \subset F_{i+1}$ is quadratic.

Given a positive integer m, we say that *an angle* α *is* m-sectable if there exists an angle β satisfying $\beta^m = \alpha$ such that $\cos(\beta)$ is constructible over $\mathbb{Q}(\cos(\alpha))$. Note that our conventions allow β to be in quadrants other than the first even when α is an acute angle.

Next we introduce the Chebyshev polynomials. Let u and v be indeterminates, and consider the ring $\mathbb{C}[u, v]$. Then, there exist unique real polynomials $A_m(u, v)$ and $B_m(u, v)$ such that

$$(u + iv)^m = A_m(u, v^2) + ivB_m(u, v^2) \tag{20}$$

in $\mathbb{C}[u, v]$. Let x and y be any complex numbers, and substitute x for u and y for v in (20), obtaining

$$(x + iy)^m = A_m(x, y^2) + iyB_m(x, y^2). \tag{21}$$

The m^{th} *Chebyshev polynomial of the first kind* is now defined as follows. For any complex number x, choose y so that $y^2 = 1 - x^2$. Then,

$$T_m(x) = A_m(x, 1 - x^2). \tag{22}$$

(The Chebyshev polynomials of the second kind may be defined analogously using the polynomials B_m; we shall not use these.)

An explicit formula for $T_m(x)$ can be derived from the above:

$$T_m(x) = \sum_{0 \le 2k \le m} \sum_{l=0}^{k} (-1)^{k+l} \binom{m}{2k} \binom{k}{\ell} x^{m-2k+2\ell}. \tag{23}$$

Here are some examples of $T_m(x)$ for small values of m: $T_0(x) = 1$, $T_1(x) = x$, $T_2(x) = 2x^2 - 1$, $T_3(x) = 4x^3 - 3x$, $T_4(x) = 8x^4 - 8x^2 + 1$, $T_5(x) = 16x^5 - 20x^3 + 5x$, $T_6(x) = 32x^6 - 48x^4 + 18x^2 - 1$.

When α and β are angles satisfying $\beta^m = \alpha$, we have the well-known trigonometric identity $T_m(\cos(\beta)) = \cos(\alpha)$, which is one of the hallmark properties of the Chebyshev polynomials. Further properties of the $T_m(x)$ that are useful for us will be given in Lemma 5.1 below.

The polynomials $P_m(x, a)$ are now related to the Chebyshev polynomials as in the introduction: namely, for any complex number a,

$$P_m(x, a) = T_m(x) - a.$$

The above trigonometric identity, then, may be written as $P_m(\cos(\beta), \cos(\alpha)) = 0$. As noted in the introduction, $P_3(x, a)$ is precisely the polynomial $q(x, a)$ appearing in Wantzel's Theorem.

The proof of Theorem 1.2 will be given in this section via several subsidiary results.

First we give a lemma presenting some useful properties of the polynomials $T_m(x)$ and $P_m(x, a)$.

Lemma 5.1. (a) *The leading term of $P_m(x, a)$ (resp., $T_m(x)$) is $2^{m-1}x^m$.*

(b) *If m is odd, $T_m(x)$ is an odd function of x, so that $T_m(0) = 0$. Moreover, $T_m(\pm 1) = \pm 1$. When m is even, $T_m(x)$ is an even function of x. Also then $T_m(0) = (-1)^{m/2}$ and $T_m(\pm 1) = 1$.*

(c) *For any positive integers r and s, $T_{rs}(x) = T_r(T_s(x))$.*

(d) *If m is an odd prime, then except for the leading coefficient and possibly the constant term a, every coefficient in $P_m(x, a)$ is divisible by m.*

(e) *If m is prime, then there exist infinitely many values of $a \in \mathbb{Q}$ such that $P_m(x, a)$ is irreducible over $\mathbb{Q}$.*

(f) *If m is prime and a is a transcendental number, then $P_m(x, a)$ is irreducible over $\mathbb{Q}(a)$.*

(g) *Let m be a positive integer, and let x denote a real variable. Then $|x| \leq 1$ if and only if $|T_m(x)| \leq 1$.*

Proof. Statements (a)- (c) give well-known properties of Chebyshev polynomials of the first kind; they follow easily from the definition. Statement (d) may not be as widely known, but it is immediate once one notes that each term in the formula for $T_m(x)$ has a factor of the form $\binom{m}{2k}$ and that this factor is divisible by the prime m except when $k = 0$.

We prove statement (e) in two parts. First, when $m = 2$, then $P_m(x, a) = 2x^2 - 1 - a$, which is clearly irreducible for all $a \in \mathbb{Q}$ such that $(1 + a)/2$ is not a perfect square in $\mathbb{Q}$. Secondly, suppose that m is an odd prime. Choose any rational value $a = r/s$ such that r and s are coprime and r is divisible by m but not by m^2. Then, using statement (d), we may apply Eisenstein's Criterion together with the Gauss Lemma to conclude that $P_m(x,a)$ is irreducible over $\mathbb{Q}$.

We now show that statement(f) follows from statement (e) via a somewhat standard argument. Let t be an indeterminate, and consider the polynomial $P_m(x,t)$ as a polynomial in $\mathbb{Q}[t][x]$. Suppose that it factors in $\mathbb{Q}[t][x]$, say $P_m(x,t) = FG$, where both F and G are polynomials of positive degree in x, with coefficients c_i and d_j, respectively, that are polynomials in $\mathbb{Q}[t]$. Statement (e) implies that we may choose a rational number a such that $P_m(x,a)$ is irreducible over $\mathbb{Q}$ and such that a is not a zero of any non-zero c_i or d_j. Now define a $\mathbb{Q}$-algebra homomorphism $\mathbb{Q}[t] \to \mathbb{Q}$ by sending t to a. This induces a homomorphism $\mathbb{Q}[t][x] \to \mathbb{Q}[x]$ which sends $P_m(x,t)$ to $P_m(x,a)$. It also sends F and G to positive-degree polynomials in $\mathbb{Q}[x]$ whose product is $P_m(x,a)$, a contradiction. Therefore, $P_m(x,t)$ is irreducible over $\mathbb{Q}[t]$, hence over $\mathbb{Q}(t)$. Now suppose that a is a transcendental number. The rule $t \mapsto a$ defines a $\mathbb{Q}$-algebra isomorphism $\mathbb{Q}[t] \to \mathbb{Q}[a]$, hence an isomorphism $\mathbb{Q}(t)[x] \to \mathbb{Q}(a)[x]$. Obviously $P_m(x,t) \mapsto P_m(x,a)$, so the latter is irreducible over $\mathbb{Q}(a)$.

Finally, we prove statement (g). The "conjugate" of identity (20) is

$$(u - iv)^m = A_m(u, v^2) - ivB_m(u, v^2).$$

Multiplying it by (20) yields the identity

$$(u^2 + v^2)^m = A_m(u, v^2)^2 + v^2 B_m(u, v^2)^2.$$

Now let I be the ideal in $\mathbb{C}[u,v]$ generated by $u^2 + v^2 - 1$. The quotient $\mathbb{C}[u,v]/I$ is a ring R generated by the images s of u and t of v, which satisfy $s^2 + t^2 = 1$. The displayed identity above becomes

$$1 = A_m(s, 1 - s^2)^2 + (1 - s^2)B_m(s, 1 - s^2)^2$$

in R. Choose any real number x and then any complex number y such that $x^2+y^2 = 1$. There is then a unique homomorphism of R to $\mathbb{C}$ sending s to x and t to y, under which the last identity above gets mapped to,

$$1 = T_m(x)^2 + (1 - x^2)B_m(x, 1 - x^2)^2.$$

The polynomials T_m and B_m are real polynomials in the real variable x, so it is immediate that $|x| \leq 1$ if and only if $|T_m(x)| \leq 1$. □

Remark: (1) Statement (g) is a technical fact about $T_m(x)$ that will be helpful when the sets we are estimating are contained in $[-1,1]$. We can reformulate this fact in a possibly more useful form as follows:

$$T_m([-1,1]) \subseteq [-1,1] \quad \text{and} \quad T_m(\mathbb{R} \setminus [-1,1]) \subseteq \mathbb{R} \setminus [-1,1].$$

The following lemma gives statements (a) and (b) of Theorem 1.2.

Lemma 5.2. (a) *Let $m_{odd} \neq 1$. If the angle α is m-sectable, then $P_m(x, \cos(\alpha))$ is reducible over the field $\mathbb{Q}(\cos(\alpha))$.*

(b) *Let m be as in (a), and suppose that α is m-sectable. Then $\cos(\alpha)$ is an algebraic number.*

(c) *If every angle is m-sectable, then $m_{odd} = 1$ and conversely.*

Remark: In Remark (4) below Theorem 1.2 in the Introduction, we give an example showing that the conclusion of statement (a) of this lemma cannot be replaced by the statement "$P_m(x, \cos(\alpha))$ has a zero in $\mathbb{Q}(\cos(\alpha))$."

Proof. (a) By hypothesis, there is an angle β that is constructible over the set $\{0, 1, \alpha\}$ such that $\beta^m = \alpha$. As we comment above, $\cos(\beta)$ is constructible over the field $\mathbb{Q}(\cos(\alpha))$. Let $g(x)$ be the minimal polynomial of $\cos(\beta)$ over $\mathbb{Q}(\cos(\alpha))$. From the fundamental theorem of constructible numbers, we know that the degree of $g(x)$ is a power of 2. Since $\cos(\beta)$ is a zero of $P_m(x, \cos(\alpha))$, $g(x)$ must divide $P_m(x, \cos(\alpha))$. Moreover, it is a proper divisor because m is not a power of 2. This proves statement (a).

(b) If $m_{odd} \neq 1$, then m has an odd prime divisor, say p. Let α be an m-sectable angle. Then α is also p-sectable, since powers (or multiples) of constructible angles are constructible. Further $p_{odd} = p \neq 1$, so the hypotheses of statement (a) are satisfied for p and α, whence $P_p(x, \cos(\alpha))$ is reducible over $\mathbb{Q}(\cos(\alpha))$. Therefore, by statement (f) in Lemma 5.1, $\cos(\alpha)$ must be algebraic.

(c) If every angle is m-sectable, there are m-sectable angles α for which $\cos(\alpha)$ is transcendental. For this not to contradict statement (b), it must be the case that $m_{odd} = 1$. Conversely, when $m_{odd} = 1$, it is the case that every angle is m-sectable: just use the well-known angle bisection construction as often as needed.

□

The following proposition gives statement (c) of Theorem 1.2.

Proposition 5.1. *Suppose that m is a Gauss number. Then an angle α is m-sectable if and only if $P_{m_{odd}}(x, \cos(\alpha))$ has a zero in $\mathbb{Q}(\cos(\alpha))$.*

Proof. In preparation for the main body of the proof, we begin with some trivial cases. Suppose $m_{odd} = 1$. In this case, every angle α is m-sectable—just use repeated bisection when necessary— and $P_{m_{odd}}(x, \cos(\alpha)) = x - \cos(\alpha)$, which obviously has a zero in $\mathbb{Q}(\cos(\alpha))$ for each α. So the proposition is true in this case.

Next, suppose $\alpha = e^{0 \cdot i} = 1$ or $\alpha = e^{\pi i} = -1$, so that $\cos(\alpha) = 1$ or $\cos(\alpha) = -1$, respectively. We note then that we have $P_m(1, 1) = P_m(-1, -1) = 0$, for any odd m, so the proposition is satisfied for these values of α and m.

Third, we observe that an angle α is m-sectable if and only if it is m_{odd}-sectable, again using repeated bisection when needed.

Collecting these three observations, we see that *it suffices to prove the result for m an odd Gauss number and > 1, and for $\alpha \neq \pm 1$. We assume these conditions from now on in this proof.*

One final preparatory argument, which uses one of the foregoing conditions: Suppose that β is an angle satisfying $\beta^m = \alpha$, and let $\zeta = e^{2\pi i/m}$. Clearly the angles $\beta\zeta^i$, $i = 0, 1, \dots m-1$ are the distinct zeros of $z^m - \alpha$, and, therefore, the quantities $\cos(\beta\zeta^i)$ are zeros of $P_m(x, \cos(\alpha))$. *We claim that all the zeros* $\cos(\beta\zeta^i)$ *of* $P_m(x, \cos(\alpha))$ *are distinct*: For suppose $\cos(\beta\zeta^i) = \cos(\beta\zeta^j)$, where $0 \leq j < i \leq m-1$. Then we must have $\beta\zeta^i = (\beta\zeta^j)^{-1}$, which implies that $\beta^2 = \zeta^{-(i+j)}$. But then $\alpha^2 = \beta^{2m} = 1$, implying that $\alpha = \pm 1$, which we have ruled out. This verifies the claim. (This argument holds for any positive value of m, but we do not need this.)

It follows that the quantities $\cos(\beta\zeta^i)$, $i = 0, 1, \dots, m-1$ exhaust the zeros of $P_m(x, \cos(\alpha))$.

We are now ready to prove one implication of the proposition. Suppose some zero r of $P_m(x, \cos(\alpha))$ belongs to $\mathbb{Q}(\cos(\alpha))$, and let β be any angle satisfying $\beta^m = \alpha$. *A fortiori*, r is constructible over $\mathbb{Q}(\cos(\alpha))$. By what was just shown above, r has the form $\cos(\beta\zeta^{i_0})$, for some i_0. Hence $\beta\zeta^{i_0}$ is constructible over $\{0, 1, \alpha\}$. Since $(\beta\zeta^{i_0})^m = \alpha$, it follows that α is m-sectable. This completes the proof of the implication.

We now prove the converse. Suppose α is m-sectable, so that there is an angle β satisfying $\beta^m = \alpha$ with β constructible over $\{0, 1, \alpha\}$. The angle ζ defined above is constructible (over $\{0, 1\}$), by Gauss's Theorem, as are then the powers ζ^i, $i = 1, 2 \dots, m-1$. It follows that the angles $\beta\zeta^i$ are all constructible over $\{0, 1, \alpha\}$, $i = 0, 1, \dots, m-1$. Therefore, the corresponding zeros $\cos(\beta\zeta^i)$ of $P_m(x, \cos(\alpha))$ are constructible over $\mathbb{Q}(\cos(\alpha))$, and, by the argument above, they comprise all of the zeros of $P_m(x, \cos(\alpha))$.

Let $g_i(x)$ denote the minimal polynomial of $\cos(\beta\zeta^i)$ over $\mathbb{Q}(\cos(\alpha))$, $i = 0, 1, \dots, m-1$. Each $g_i(x)$ is irreducible over $\mathbb{Q}(\cos(\alpha))$, is a divisor of $P_m(x, \cos(\alpha))$, and has degree a power of 2, as in the proof of Lemma 5.2 (a). Since m is not a power of 2, each $g_i(x)$ is a proper divisor of $P_m(x, \cos(\alpha))$. Let $h_1(x), h_2(x), \dots, h_s(x)$ denote the distinct polynomials among the $g_i(x)$. Then $P_m(x, \cos(\alpha)) = 2^{m-1}h_1(x) \cdot \ldots \cdot h_s(x)$, since both sides of the equation are polynomials with the same leading coefficients and zeros. Therefore, the odd number m is a sum of powers of 2, and so one of these powers must be 2^0, say $\deg(g_{i_1}(x)) = 2^0$. This means the zero $\cos(\beta\zeta^{i_1})$ of $P_m(x, \cos(\alpha))$ belongs to $\mathbb{Q}(\cos(\alpha))$, completing the proof of the proposition and, hence, the proof of Theorem 1.2.

□

6. Counting m-sectable angles.

We saw in the preceding section that for any integer m not a power of 2, the m-sectable angles have cosines that are algebraic numbers. That is, the set $\mathbf{m} - \mathbf{Sect}$

of such cosines is contained in $\mathbb{A} \cap [-1, 1]$. We replace the field of algebraic numbers with a number field K embedded in $\mathbb{R}$ and apply the results of §§3 and 4 to compute the finite density $\delta_K(\mathbf{m - Sect}; B)$, for large, positive real B.

Lemma 6.1. *Let m be a Gauss number. Let $T_{m_{odd}}(x)$ denote the m_{odd}^{th} Chebyshev polynomial of the first kind (cf. (23)), and set $P_{m_{odd}}(x, a) = T_{m_{odd}}(x) - a$. Then, for any number field $K \subset \mathbb{R}$,*

$$\mathbf{m - Sect} \cap K \subseteq Z_K(T_{m_{odd}}) \cap [-1, 1].$$

Proof. Recall that $\mathbf{m - Sect} = \mathbf{m_{odd} - Sect}$ for every m (cf. the proof of Proposition 5.1). Choose any $a \in \mathbf{m - Sect} \cap K$. Then there exists an m_{odd}-sectable angle α such that $a = \cos(\alpha)$. Therefore, $a \in [-1, 1]$. Furthermore, by Theorem 1.2, $P_{m_{odd}}(x, a)$ has a zero in $\mathbb{Q}(a) \subseteq K$. Therefore, $a \in Z_K(T_{m_{odd}})$. □

Proposition 6.1 (Theorem 1.3). *Let m be any positive integer, and let m_g denote the largest odd Gauss number dividing m. For any λ satisfying $1/2 < \lambda < 1$, there exists a B_0 such that $B \geq B_0$ implies*

$$|\mathbf{m - Sect} \cap V_K(B)| \leq \lambda \mathfrak{S} \cdot (2\|T_{m_g}\|)^{2n} B^{2/m_g},$$

where we recall that $n = [K : \mathbb{Q}]$ and $\mathfrak{S}$ is Schanuel's constant.

Proof. Notice that when $m_g = 1$, we have $\|T_{m_g}\| = \|x\| = 1$, and the inequality above is a trivial consequence of Schanuel's Theorem. We now turn to the proof for the case $m_g \neq 1$.

Let k denote the maximal Gauss number dividing m. Then, $k_{odd} = k_g = m_g \neq 1$. Moreover, $\mathbf{m - Sect} \subseteq \mathbf{k - Sect}$. So, it suffices to prove the result for k instead of for m. Use Lemma 6.1 to obtain the inequality

$$|(\mathbf{k - Sect}) \cap V_K(B)| \leq |Z_K(T_{k_{odd}}) \cap [-1, 1] \cap V_K(B)|. \tag{24}$$

Now Corollary 3.3 and and Lemma 5.1 (g) imply that

$$|Z_K(T_{k_{odd}}) \cap [-1, 1] \cap V_K(B)| \leq |T_{k_{odd}}\big(V_K(\kappa(L^{-n}B)^{1/k_{odd}}) \cap [-1, 1]\big)|,$$

and the right hand side clearly is dominated by $|V_K(\kappa(L^{-n}B)^{1/k_{odd}}) \cap [-1, 1]|$. We then apply Lemma 4.1 to this last to obtain

$$\frac{1}{2}(|V_K(\kappa(L^{-n}B)^{1/k_{odd}})| + 3).$$

Applying Schanuel's Theorem to this (see § 2), and making use of properties of "big oh," we get

$$|\mathbf{k - Sect} \cap V_K(B)| \leq \frac{1}{2}\mathfrak{S} \cdot (\kappa(L^{-n}B)^{1/m_{odd}})^2 + \mathbf{O}(C(n, \kappa(L^{-n}B)^{1/k_{odd}})).$$

Choose λ as stated above. Then, for sufficiently large B, the right-hand side above is dominated by $\lambda\mathfrak{S} \cdot (\kappa(L^{-n}B)^{1/k_{odd}})^2$. It remains to evaluate κ and L in this context.

Directly from the definitions, we have $\kappa = 2^{n(k_{odd}-1)}$ and $L = (2^{(k_{odd}-2)k_{odd}})\|T_{k_{odd}}\|^{-k_{odd}}$. Substituting these expressions into our formula, we get

$$|\mathbf{k} - \mathbf{Sect} \cap V_K(B)| \leq \lambda\mathfrak{S} \cdot (2\|T_{k_{odd}}\|)^{2n} B^{2/k_{odd}},$$

as claimed.

□

We are now finally ready to prove the result that was our goal for this paper:

Corollary 6.1 (Corollary 1.4)**.** *Assume that m is a positive integer and that m_g is the largest odd Gauss number dividing m. There exists a positive B_1 such that if $B \geq B_1$, then*

$$\delta_K(\mathbf{m} - \mathbf{Sect}; B) \leq (2\|T_{m_g}\|)^{2n} B^{(2/m_g)-2}.$$

Therefore, when $m_g \neq 1$, $\delta_K(\mathbf{m} - \mathbf{Sect})$ exists and equals 0.

Proof. In Schanuel's Theorem choose B so large that $|V_K(B)| \geq \lambda\mathfrak{S} \cdot B^2$, and choose B_1 larger than this and so that the bound for $|\mathbf{m} - \mathbf{Sect} \cap V_K(B)|$ in Proposition 6.1 holds for all $B \geq B_1$. Then, for such B, the quotient

$$\delta_K(\mathbf{m} - \mathbf{Sect}; B) = \frac{|\mathbf{m} - \mathbf{Sect} \cap V_K(B)|}{|V_K(B)|}$$

is clearly less than or equal to the quotient

$$\frac{\lambda\mathfrak{S} \cdot (2\|T_{m_g}\|)^{2n} B^{2/m_g}}{\lambda\mathfrak{S} \cdot B^2} = (2\|T_{m_g}\|)^{2n} B^{(2/m_g)-2},$$

as desired.

When $m_g \neq 1$, the exponent of B is negative, so the finite densities go to 0 as B goes to infinity.

□

References

[Cou] Richard Courant and Herbert Robbins. "What is Mathematics?" Thirteenth Printing. Oxford University Press. New York, London, Toronto (1967).

[Lan] Serge Lang. "Fundamentals of Diophantine Geometry." Springer-Verlag, New York (1983).

[Sch] Stephen Schanuel. *Heights in number fields*, Bull. Soc. Math. France **107** (1979) 433-449

[Wan] Pierre-Laurent Wantzel. *Recherches sur les moyens de reconnâitre si un Problème de Géometrie peut se résoudre avec la règle et le compas.* Journal de Mathématiques Pures et Appliquées **1 (2)** (1837) 366-372.