MINIMAL POLYNOMIALS OF ALGEBRAIC NUMBERS WITH RATIONAL PARAMETERS

KARL DILCHER, ROB NOBLE, AND CHRIS SMYTH

1. Introduction

It is unusual for an irreducible polynomial to have a root with rational real part or with rational imaginary part. Of course, such polynomials exist: one can simply take the minimal polynomial of, say, $1+i\sqrt{2}$ or $\sqrt{2}+i$. The same applies to polynomials having a root of rational modulus. But it turns out to be of interest to characterize these three kinds of polynomials. We therefore define our first family of polynomials, $\mathcal{C}_1$, to consist of the minimal polynomials of some algebraic number having rational *real* part. Our second family, $\mathcal{C}_2$, consists of the minimal polynomials of some algebraic number having rational *imaginary* part, while our third family, $\mathcal{C}_3$, consists of the minimal polynomials of some algebraic number having rational *modulus*.

We describe the polynomials of each family in Sections 3, 4 and 5. Then in Sections 6, 7 and 8 we classify the polynomials belonging to two of the three families, while in Section 9 we do the same for the polynomials belonging to all three families. Section 2 contains preliminary results needed for the proofs.

For a rational linear polynomial, its root has rational real part, imaginary part and modulus. An irreducible quadratic polynomial z^2+pz+q with rational coefficients and with discriminant $\Delta = p^2-4q$ belongs to $\mathcal{C}_1$ if and only if $\Delta<0$, to $\mathcal{C}_2$ if and only if $-\Delta$ is a square (in which case it belongs to $\mathcal{C}_1\cap\mathcal{C}_2$) or $\Delta>0$, and to $\mathcal{C}_3$ if and only if $\Delta<0$ and q is a square (in which case it belongs to $\mathcal{C}_1\cap\mathcal{C}_3$). Hence it belongs to $\mathcal{C}_2\cap\mathcal{C}_3$ if and only if $-\Delta$ and q are both squares (in which case it belongs to $\mathcal{C}_1\cap\mathcal{C}_2\cap\mathcal{C}_3$). For $-\Delta=a^2$ and $q=b^2$ this latter condition is $4b^2-a^2=p^2$. This is essentially the Pythagoras equation, with solution $p=u^2-v^2$, $a=2uv$ and $2b=u^2+v^2$ for some rationals u and v. For the rest of the paper, therefore, we can restrict our attention to polynomials of degree at least 3.

2010 *Mathematics Subject Classification.* Primary 11R06; Secondary 12E10.

Key words and phrases. Minimal polynomials, roots, rational parameters, irreducibility.

Research supported in part by the Natural Sciences and Engineering Research Council of Canada and by the Killam Trusts.

2. Preliminaries

There are two different techniques for studying minimal polynomials, depending on whether one works with the polynomials themselves, or with their roots, which are algebraic numbers. Recall that for any such root, the monic irreducible polynomial it satisfies is its *minimal polynomial*, and, for a given root of such a polynomial, the collection of all roots constitutes its set of *conjugates*. In this paper, we employ both approaches. For the second, the following lemma and corollary are needed. They contain the main application of Galois Theory required for our proofs.

Lemma 1. *Let $H(z_1, \ldots, z_k) \in \mathbb{Q}[z_1, \ldots, z_k]$ be such that $H(\alpha_1, \alpha_2, \ldots, \alpha_k) = 0$ for certain algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_k$. Then for each conjugate α_1' of α_1 there are conjugates $\alpha_2', \ldots, \alpha_k'$ of $\alpha_2, \ldots, \alpha_k$, respectively, such that $H(\alpha_1', \alpha_2', \ldots, \alpha_k') = 0$.*

Proof. Take F to be a Galois extension of $\mathbb{Q}$ containing $\alpha_1, \alpha_2, \ldots, \alpha_k$. Then we know from Galois Theory that for any $\alpha \in F$ the set S_α of its conjugates is stable under the action of the Galois group $G = \mathrm{Gal}(F/\mathbb{Q})$, and that, furthermore, this action is transitive on S_α. Thus we can apply to $H(\alpha_1, \alpha_2, \ldots, \alpha_k) = 0$ an automorphism $\sigma \in G$ with $\sigma(\alpha_1) = \alpha_1'$ to get $0 = \sigma H(\alpha_1, \alpha_2, \ldots, \alpha_k) = H(\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_k))$. Then, for $j \geq 2$ put $\alpha_j' = \sigma(\alpha_j)$, a conjugate of α_j. □

Corollary 1. *Let $H(z_1, z_2, z_3) \in \mathbb{Q}[z_1, z_2, z_3]$ be such that $H(\alpha_1, \alpha_2, \pm i) = 0$ for some choice of sign $\pm$ and algebraic numbers α_1, α_2, where α_1 has a real conjugate. Then, for each conjugate α_1' of α_1, there exist conjugates α_2' and α_2'' of α_2 such that $H(\alpha_1', \alpha_2', i) = H(\alpha_1', \alpha_2'', -i) = 0$.*

Proof. Assume the hypotheses, and let α_1^* be a real conjugate of α_1. By Lemma 1, there exists a conjugate α_2^* of α_2 such that, for some choice of $\varepsilon = \pm 1$, we have

$$H(\alpha_1^*, \alpha_2^*, \varepsilon i) = 0. \tag{1}$$

We then also have

$$H(\alpha_1^*, \overline{\alpha_2^*}, -\varepsilon i) = 0. \tag{2}$$

Now let α_1' be a conjugate of α_1. Then α_1' is also a conjugate of α_1^* so that, for some $\mathbb{Q}$-embedding σ, we have $\sigma(\alpha_1^*) = \alpha_1'$. Applying σ to (1) and (2) yields

$$H(\alpha_1', \sigma(\alpha_2^*), \varepsilon\sigma(i)) = H(\alpha_1', \sigma(\overline{\alpha_2^*}), -\varepsilon\sigma(i)) = 0.$$

Since one of $\varepsilon\sigma(i), -\varepsilon\sigma(i)$ is equal to i while the other is equal to $-i$, the result follows by defining α_2' and α_2'' appropriately such that $\{\alpha_2', \alpha_2''\} = \{\sigma(\alpha_2^*), \sigma(\overline{\alpha_2^*})\}$. □

The following simple well-known lemma is basic to our analysis of the minimal polynomials of algebraic numbers with rational real part.

Lemma 2. *If the minimal polynomial $P(z) \in \mathbb{Q}[z]$ of an irrational algebraic number α also has $-\alpha$ as a root, then $P(z) = Q(z^2)$ for some monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$.*

Proof. We know that $P(z)$ is monic, irreducible and of degree at least two. Suppose that $\alpha \in \mathbb{C}$ is such that $P(\alpha) = P(-\alpha) = 0$. Then $P(z)$ and $P(-z)$ share the root α. Since P is the minimal polynomial of α, we must have $P(-z) = \pm P(z)$ so that P is either odd or even. Now, P cannot be odd since it is not divisible by z. We conclude that P is even and consequently a polynomial in z^2. Finally, if $P(z) = Q(z^2)$, then the fact that P is monic and irreducible forces Q to be monic and irreducible as well. □

Thus the lemma says that an irreducible polynomial of degree at least two with rational coefficients, having two roots summing to 0, must be a polynomial in z^2. However, we mention in passing that it is not the case that an irreducible polynomial with rational coefficients having three roots summing to 0 must be a polynomial in z^3. (In fact, its degree need not even be divisible by 3.) See [2], where the counterexample $P(z) = z^{20} + 4 \cdot 5^9 z^{10} + 16 \cdot 5^{15}$ is shown to have three roots that sum to 0.

The following lemma is needed in Section 6.

Lemma 3. *Let $Q(z) \in \mathbb{Q}[z]$ be an irreducible polynomial having both a positive real root and a negative real root. Then $Q(z^2)$ is irreducible and, for every nonzero $r \in \mathbb{Q}$, the polynomial $Q((z+ir)^2)Q((z-ir)^2) \in \mathbb{Q}[z]$ is also irreducible.*

Proof. Let $\beta > 0$ and $\beta' < 0$ be roots of Q. Then, as $\sqrt{\beta'}$ is imaginary, it does not belong to $\mathbb{Q}(\beta')$, so

$$[\mathbb{Q}(\sqrt{\beta'}) : \mathbb{Q}] = 2[\mathbb{Q}(\beta') : \mathbb{Q}] = \deg Q(z^2).$$

Hence $Q(z^2)$ is irreducible.

Now put $Q_2(z) = Q(z^2)$, so that Q_2 is irreducible. Then $Q((z+ir)^2)Q((z - ir)^2) = Q_2(z + ir)Q_2(z - ir)$ has a root, α say, with $\alpha + ir = \sqrt{\beta}$. Since $\mathbb{Q}(\sqrt{\beta})$ is a real field, it cannot contain α, and hence

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2[\mathbb{Q}(\sqrt{\beta}) : \mathbb{Q}] = 2 \deg Q_2 = \deg \left(Q((z + ir)^2)Q((z - ir)^2) \right).$$

Hence $Q((z+ir)^2)Q((z-ir)^2)$ is irreducible. □

The following result is needed for the proofs of Theorems 6 and 7. It is, in principle, well-known (see, e.g., [8, p. 179]), but it is convenient for us to state and prove the precise special case we require.

Denote by G the group of Möbius transformations $\frac{az+b}{cz+d}$ with $a, b, c, d \in \mathbb{Q}$, $ad - bc = \pm 1$, under functional composition. Furthermore, for nonnegative rational numbers t, let H_t denote the subgroup of G generated by $g_t = t - z$ and $g_* = 1/z$.

Lemma 4. *The subgroup H_t of G is infinite in all cases except*

$$H_0 = \left\{ z, \frac{1}{z}, -z, -\frac{1}{z} \right\}, \quad H_1 = \left\{ z, \frac{1}{z}, 1-z, \frac{1}{1-z}, \frac{z}{z-1}, \frac{z-1}{z} \right\}.$$

Furthermore

$$\frac{1}{2}\sum_{h \in H_0} h^2 = z^2 + \frac{1}{z^2} \quad \textit{and} \quad \frac{1}{2}\sum_{h \in H_1} h^2 = \ell(z)^2 + \frac{21}{4},$$

where

$$\ell(z) = \frac{(z-2)(z-\frac{1}{2})(z+1)}{z(z-1)}. \tag{3}$$

This latter sum is related to the classical j-invariant $j(\lambda)$ of the general elliptic curve in Legendre form $Y^2 = X(X-1)(X-\lambda)$. Indeed,

$$j(\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2} = 256\ell(\lambda)^2 + 1728;$$

see, for instance, [12, p. 68]. We need to work with the sums $\sum h^2$ that appear in the lemma because $\sum_{h \in H_0} h = 0$ and $\sum_{h \in H_1} h = 3$ are of no use to us, being independent of z.

Proof of Lemma 4. The group G is well-known to be isomorphic, via $\frac{az+b}{cz+d} \mapsto \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, to the group of rational matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ of determinant ± 1, factored by the subgroup $\pm I$, where I is the 2×2 identity matrix. Under this isomorphism, $g' = g_* \circ g_t = 1/(t-z)$ corresponds to the matrix $A' = \left(\begin{smallmatrix} 0 & 1 \\ -1 & t \end{smallmatrix}\right)$. If H_t is finite, then g' must have finite order, and so the eigenvalues of A' must be roots of unity. Now the characteristic equation of A' is $\lambda^2 - t\lambda + 1 = 0$, and, for its roots to be roots of unity, the sum of its roots, namely t, must be an algebraic integer between -2 and 2. But t is nonnegative and rational, so $t \in \{0, 1, 2\}$. However, for $t = 2$ we have $A'^n = \left(\begin{smallmatrix} 1-n & n \\ -n & 1+n \end{smallmatrix}\right)$, so that A' is of infinite order. So for H_t finite, t can only be 0 or 1. For these two cases we use g_t and g_* to generate H_t as claimed, and to check that these sets are stable under the action of g_t and g_*. Finally, the values of the sums of squares can be verified by direct computation. □

The next result is needed for the proof of Theorem 14. Define the Möbius transformation F by

$$F(z) = \frac{\frac{i}{2}z + \frac{3}{4}}{z + \frac{i}{2}}. \tag{4}$$

Lemma 5. *The group H of Möbius transformations generated by $g_1 = 1 - z$ and F, defined by (4), is given by*

$$H = \left\{ z, \frac{2iz-3}{-4z+2i}, \frac{(-4+2i)z+1}{-4z+4+2i}, \frac{(-2+4i)z-i}{4iz-2-4i}, \frac{-2z+3i}{4iz-2}, \right.$$
$$\frac{-2iz-3+2i}{4z-4+2i}, \frac{(4-2i)z-3+2i}{4z+2i}, \frac{(-2+2i)z-1-3i}{(-4+4i)z+2-2i},$$
$$\left. \frac{(2+2i)z+1-3i}{(4+4i)z-2-2i}, \frac{-2iz+3+2i}{-4z+4+2i}, \frac{(-4-2i)z+3+2i}{-4z+2i}, 1-z \right\}.$$

Also,

$$\frac{1}{2}\sum_{h\in H} h^2 = \frac{v^3+3v^2+36v+12}{2v^2+8}, \tag{5}$$

where $v = w - 1/w$ with $w = \frac{1}{2}(2z-1)^2$.

As in the previous lemma, $\sum_{h\in H} h = 6$, independent of z.

Proof. The result can be verified, e.g., using the computer algebra system Maple [6], by showing that repeated applications of $z \mapsto 1 - z$ and F to z give H, which is then stable under both maps. Maple can also be used to verify the value of the sum in (5). □

As we shall see, for an irreducible polynomial P of degree at least 3 having a root with rational real part r, all roots of P having rational real part have the *same* real part r, denoted by $c_1(P)$. Similarly, for an irreducible polynomial P of degree at least 3 having a root with nonnegative rational imaginary part r', all roots of P having nonnegative rational imaginary part have the same imaginary part r', denoted by $c_2(P)$. Again, for an irreducible polynomial P of degree at least 3 having a root with rational modulus R, all roots of P having rational modulus have the same modulus R, denoted by $c_3(P)$. Thus, before stating the first of our 14 theorems, and corresponding examples, covering the different cases discussed in Section 1, we introduce a system of labelling for these theorems and examples, where appropriate: the label $[r, r', R]$ $(= [c_1(P), c_2(P), c_3(P)])$ indicates that the theorem in question deals with polynomials that have roots with rational real part r, roots with nonnegative rational imaginary part r', and roots with rational modulus R. A dash "–" indicates that one or two of the categories are irrelevant.

3. Polynomials in $\mathcal{C}_1$

In this section we study the family $\mathcal{C}_1$ of minimal polynomials of algebraic numbers with rational real part. Our first example is the minimal polynomial of four different algebraic numbers, all with rational real part.

Example 1 ($[1,-,-]$)**.** *Let $P(z) = z^4 - 4z^3 + 9z^2 - 10z + 5$. Consideration of possible factors shows that this polynomial is irreducible, and its roots are $1 \pm \frac{1}{2}(1-\sqrt{5})i$, $1 \pm \frac{1}{2}(1+\sqrt{5})i$, all four roots having rational real part. So $P \in \mathcal{C}_1$.*

More generally, if r is rational and w is a totally real algebraic number then the minimal polynomial of $r + iw$ has all roots $r \pm iw'$, for conjugates w' of w, with rational real part. We notice that all these rational real parts are the same. Corollary 2 below shows that this is typical.

However, our next example shows that not all the roots of a polynomial in $\mathcal{C}_1$ need have rational real part.

Example 2 ($[0,-,-]$)**.** *Consider $P(z) = z^4 - 2$; it is irreducible over $\mathbb{Q}$, and among its roots $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$, two have real part 0. So $P \in \mathcal{C}_1$.*

Theorem 1 ($[r,-,-]$)**.** *Let P be a polynomial of degree at least 3. Then $P \in \mathcal{C}_1$ if and only if $P(z) = Q((z-r)^2)$ for some $r \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ having a negative real root. In this case, P has a root with rational real part r.*

Proof. Suppose first that $P(z) = Q((z-r)^2)$ for some $r \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ that has a negative real root t. Write $t = -s^2$ where $s \in \mathbb{R}$ is nonzero. Then, with $\alpha = r + is$, we have

$$P(\alpha) = Q((is)^2) = Q(-s^2) = Q(t) = 0$$

so that α is a root of P with rational real part r. Since P is monic, in order to show that $P \in \mathcal{C}_1$, we are reduced to proving that P is irreducible over $\mathbb{Q}$. To accomplish this, we show that $\deg_{\mathbb{Q}}(\alpha) = \deg P$. Since $\alpha = r + \sqrt{t}$, and $\sqrt{t} \notin \mathbb{Q}(t)$ (because $\mathbb{Q}(t)$ is a real field, while $\sqrt{t}$ is purely imaginary), we conclude that $[\mathbb{Q}(\alpha) : \mathbb{Q}(t)] = 2$. It follows from the multiplicativity of degrees in field extensions that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(t)][\mathbb{Q}(t) : \mathbb{Q}] = 2[\mathbb{Q}(t) : \mathbb{Q}] = 2\deg Q = \deg P$ as required.

For the other direction, suppose that $P \in \mathcal{C}_1$ has degree at least 3. Then P is monic, irreducible and has a root $\alpha = r + is$ with rational real part r and imaginary part $s \neq 0$. Therefore $P(z + r)$ is monic, irreducible, of degree at least two and has $\pm is$ as roots. It follows from Lemma 2 that

$P(z+r) = Q(z^2)$ for some monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$. Since $P(z) = Q((z-r)^2)$, and Q has the negative real root $-s^2$, the result follows. □

The following consequence of Theorem 1 is perhaps the most interesting property of the polynomials in $\mathcal{C}_1$.

Corollary 2. *All roots of a polynomial $P \in \mathcal{C}_1$ of degree at least 3 that have rational real part have the same real part r given by the arithmetic mean of the roots of P, namely $r = \operatorname{tr} P/\deg P$. Further, we have $P(r-z) = P(r+z)$.*

Proof. If $d = \deg P$, then Theorem 1 gives

$$P(z) = ((z-r)^2)^{d/2} + [\text{lower terms in } (z-r)^2] = z^d - rdz^{d-1} + \dots,$$

which shows that $rd = \operatorname{tr} P$ and, in particular, that r is unique. Finally, $P(r-z) = P(r+z)$ follows directly from the classification in Theorem 1. □

It will be convenient to adopt the following notation. By Corollary 2, we know that all roots of a polynomial $P \in \mathcal{C}_1$ of degree at least 3 that have rational real part have the same real part. We call this quantity *the rational real part of the roots of P*, denoted by $c_1(P)$.

Both Theorem 1 and Corollary 2 are illustrated by Example 1, where $Q(z) = z^2 + 3z + 1$ and $r = 1$. The roots of Q are $(-3 \pm \sqrt{5})/2$, and if we rewrite the four roots in Example 1 as

$$1 \pm \sqrt{-\tfrac{3\pm\sqrt{5}}{2}},$$

this will serve as an illustration of the product expansion $P(z) = \prod_{j=1}^{d'}((z-r)^2 - \beta_j)$, where the β_j $(j = 1, \dots, d')$ are the roots of Q, which follows immediately from Theorem 1.

Theorem 1 and Corollary 2 also provide a simple algorithm for testing whether or not a given polynomial P has a root with rational real part. Define $r := \operatorname{tr} P/\deg P$ and then expand $P(z+r)$ to see whether it is $Q(z^2)$ for some polynomial $Q(z) \in \mathbb{Q}[z]$. Finally test whether Q is irreducible and has a negative real root.

In the following corollary we provide two further simple criteria.

Corollary 3. (*a*) *Let $P \in \mathcal{C}_1$ be of degree at least 3. Then $P'(c_1(P)) = 0$.*

(*b*) *Let r be rational and $w_1, w_2 \in \mathbb{R}$. Two algebraic numbers $r + iw_1$ and $r + iw_2$ have the same minimal polynomial if and only if w_1^2 and w_2^2 have the same minimal polynomial.*

Proof. (a) From Theorem 1, $P'(z) = 2(z-r)Q'((z-r)^2)$, giving the result with $r = c_1(P)$.

(b) We note that, by Theorem 1, if $r+iw$ is one root of P having real part r, then Q is the minimal polynomial of $-w^2$; this implies the statement. $\square$

We see that the polynomials in Examples 1 and 2 satisfy Part (a). Indeed, if P is as in Example 1, then $P'(z) = 2(z-1)(2z^2-4z+5)$, while if P is as in Example 2, then $P'(z) = 4z^3$.

However, note that the converse of Part (a) is not true; that is, if the derivative of a polynomial has a rational root, this does not imply that the given polynomial has roots with rational real part. For instance, if P is as in Example 1, then the polynomial $P(z)+2$ has the same derivative, with $r=1$ as a root. However, the roots of $P(z)+2$ turn out to be $1 \pm \frac{1}{2}\sqrt{2\sqrt{3}-3} \pm \frac{i}{2}\sqrt{2\sqrt{3}+3}$, where the two instances of "$\pm$" are independent. The polynomial therefore has no roots with rational real part, while it is still irreducible.

We remark in passing that if the roots of a polynomial of degree d all have the same real part r then this real part must be rational, as is seen by looking at the polynomial's trace, $rd \in \mathbb{Q}$. (This was pointed out by Henri Cohen some years ago. See also [11, Corollary 1] for an alternative, longer, proof of this.)

4. Polynomials in $\mathcal{C}_2$

Having dealt with minimal polynomials of algebraic numbers having rational *real* part, it is natural to consider minimal polynomials of algebraic numbers having rational *imaginary* part, i.e., polynomials $P \in \mathcal{C}_2$. By replacing a root α of such a polynomial by $\bar{\alpha}$, if necessary, we can confine our attention to those α having nonnegative imaginary part. It is perhaps not surprising that we will obtain results similar in nature to those in the previous section.

Example 3 ($[-,1,-]$)**.** *Let $P(z) = z^4+2z^3+z^2+5$. It is not difficult to verify that this polynomial is irreducible, and its roots are*

$$\tfrac{-1-\sqrt{5}}{2} \pm i, \quad \tfrac{-1+\sqrt{5}}{2} \pm i.$$

Thus it is the minimal polynomial of two different algebraic numbers with positive rational imaginary parts. So $P \in \mathcal{C}_2$.

More generally, if r is rational and v is a totally real algebraic number then the minimal polynomial of $v+ir$ has all roots $v' \pm ir$, for conjugates v' of v, with rational imaginary part. We notice that these rational imaginary parts have the same absolute value. Corollary 4 below shows that this is typical.

Example 2 in the previous section shows that not all roots of a polynomial in $\mathcal{C}_2$ need have rational imaginary part. Since all polynomials of odd degree have a real root, $\mathcal{C}_2$ contains all irreducible polynomials of odd degree. Because there are standard procedures, Sturm sequences for instance, for determining whether a polynomial has a real root, we can restrict our description of polynomials in $\mathcal{C}_2$ to those having a root with *positive* imaginary part.

Theorem 2 ($[-, r, -]$)**.** *Let P be a polynomial of degree at least 3. Then $P \in \mathcal{C}_2$ and has a root with positive rational imaginary part if and only if $P(z) = Q(z + ir)Q(z - ir)$ for some positive $r \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ having a real root. In this case, P has a root with positive rational imaginary part r.*

Proof. Suppose first that $P(z) = Q(z+ir)Q(z-ir)$ for some nonzero $r \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ that has a real root t. Define $\alpha = t + ir$. Then α is a root of P having nonzero rational imaginary part r. Since P is monic, and lies in $\mathbb{Q}[z]$, in order to complete the proof, we need only establish that P is irreducible. We do this by showing that $\deg_{\mathbb{Q}}(\alpha) = \deg P$. It is sufficient to show that α has at least $\deg P = 2 \deg Q$ conjugates over $\mathbb{Q}$. But this follows from the fact that $r \neq 0$ so that each of the $\deg P$ numbers $t' \pm ir$ are conjugates of α where t' runs over the $\deg Q$ conjugates of t.

Conversely, suppose that $P \in \mathcal{C}_2$ and has a root $\alpha = t + ir$ with nonzero rational imaginary part r. Define Q to be the minimal polynomial of t. Then Q is monic, irreducible and has a real root t. Finally, $P(z) = Q(z+ir)Q(z-ir)$ since α is a root of the polynomial $Q(z + ir)Q(z - ir) \in \mathbb{Q}[z]$ and each of the $2 \deg Q$ numbers $t' \pm ir$, as t' runs over the conjugates of t, are roots of P so that $\deg P = 2 \deg Q$. □

As we did in the previous section, we now derive a number of consequences from this classification theorem.

Corollary 4. *All roots of a polynomial $P \in \mathcal{C}_2$ of degree at least 3 that have positive rational imaginary part have the same positive imaginary part. Further, if r is such an imaginary part, then $P(z)$ divides $P(z + 2ir)P(z - 2ir)$.*

Proof. Let $\alpha = s+ir$ be a root of P having rational imaginary part r. Define $\gamma = i\alpha = -r + is$. Then γ has rational real part $-r$ so that its minimal polynomial lies in $\mathcal{C}_1$. By Corollary 2, we conclude that every conjugate of

γ that has rational real part must have rational real part equal to $-r$. Since $\alpha = -i\gamma$, we see that the conjugates of α are among the numbers $\pm i\gamma'$ where γ' runs over the conjugates of γ. Since $\Im(i\gamma') = -\Re\gamma'$, we conclude that each conjugate of α having rational imaginary part has imaginary part equal to $\pm r$. For the second part, we use Theorem 2 to write $P(z) = Q(z+ir)Q(z-ir)$ for a polynomial $Q(z) \in \mathbb{Q}[z]$ so that

$$\begin{aligned} P(z+2ir)P(z-2ir) &= Q(z+3ir)Q(z+ir)Q(z-ir)Q(z-3ir) \\ &= P(z)Q(z+3ir)Q(z-3ir). \end{aligned}$$

The result now follows from the observation that the polynomials $P(z+2ir)P(z-2ir)$ and $Q(z+3ir)Q(z-3ir)$ both have rational coefficients. $\square$

In analogy to the notation introduced following Corollary 2, it will be convenient to adopt the following notation. By Corollary 4, we know that all roots of a polynomial $P \in \mathcal{C}_2$ of degree at least 3 that have nonnegative rational imaginary part have the same imaginary part. We call this quantity *the nonnegative rational imaginary part of the roots of* P, denoted by $c_2(P)$. Of course $c_2(P) \geq 0$.

The case $r = 0$ of Corollary 4 provides us with the following consequence.

Corollary 5. *No real algebraic number of degree at least 3 has a conjugate with nonzero rational imaginary part.*

It might seem that it should be easy to deduce results about algebraic numbers with rational imaginary part from results about those with rational real part, using the fact that α has rational imaginary part if and only if $i\alpha$ has rational real part. This can indeed be done, and this approach has been used to some extent in our proofs. However, the results for the minimal polynomial of $i\alpha$ are not always so straightforward. In fact, the degree of $i\alpha$ can be twice that of α (e.g., $\alpha = 1$), equal to that of α (e.g., $\alpha = 1+i$), or half that of α (e.g., $\alpha = i$); here we have chosen examples with degrees at most 2, for the sake of simplicity.

Berry [1] showed that all algebraic numbers with all conjugates having imaginary part $\pm s$ were of the form $u + is$, where u is totally real, and s^2 is rational. See the survey article of McKee [7], where Berry's results are discussed and proved.

5. Polynomials in $\mathcal{C}_3$

In this section we consider polynomials $P \in \mathcal{C}_3$. By looking at cyclotomic polynomials it is clear that polynomials with rational coefficients can have

some, or in fact all, roots with rational moduli. Thus $\mathcal{C}_3$ is nonempty. Furthermore, we will see in Corollary 6 below that, in analogy to Corollaries 2 and 4, there can only be one rational modulus realized by roots of a given polynomial in $\mathcal{C}_3$.

Our next result describes the polynomials in $\mathcal{C}_3$.

Theorem 3 ([−, −, R])**.** *Let P be a polynomial of degree at least 3. Then $P \in \mathcal{C}_3$ if and only if $P(z) = (Rz)^n Q(z/R + R/z)$ for some positive $R \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n having a real root in the interval $(-2, 2)$. In this case, P has a root with rational modulus R.*

Proof. Suppose first that $P(z) = (Rz)^n Q(z/R + R/z)$ for some positive $R \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has a real root $t \in (-2, 2)$. Then, $z/R + R/z = t$ has two nonreal complex conjugate roots of modulus R. These roots are roots of P, and so P has a root with rational modulus. Finally, since these roots are quadratic over $\mathbb{Q}(t)$, we see that P has the correct degree to be their minimal polynomial. We conclude that $P \in \mathcal{C}_3$ as required.

Conversely, suppose that $P \in \mathcal{C}_3$. Then P is monic, irreducible and has a root α with rational modulus R. It follows that $R^{-\deg P} P(Rz) \in \mathcal{C}_3$ and has a root α/R of modulus 1. We are therefore reduced to the case $R = 1$ and α having modulus 1. In this case, we need to show that

$$P(z) = z^n Q(z + 1/z) \tag{6}$$

for some monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has a root α in $(-2, 2)$. To this end, define $Q(z) \in \mathbb{Q}[z]$ to be the minimal polynomial of $\alpha + 1/\alpha$. Then Q is monic irreducible and has the real root $\alpha + 1/\alpha = \alpha + \overline{\alpha} = 2\Re\alpha \in (-2, 2)$. All that is left is to show that P is given by (6). Since α is a root of the right-hand side of (6), we need only show that the degree of α over $\mathbb{Q}$ is at least $2n$. Since $\alpha = 1/\overline{\alpha}$, and any conjugate of $\overline{\alpha}$ is a conjugate of α, we see that for every conjugate α' of α, $1/\alpha'$ is also a conjugate of α. Since the quantity $2\Re\alpha = \alpha + \overline{\alpha} = \alpha + 1/\alpha$ takes on the same value at the conjugate α' as it does at the conjugate $1/\alpha'$, we see that it has at most $\frac{1}{2} \deg P$ conjugates. Therefore $\deg_{\mathbb{Q}}(\alpha) \geq 2n$, as required. □

Recall that a polynomial $P(z)$ is called *reciprocal* if $z^{\deg P} P(1/z) = P(z)$.

Corollary 6. *All roots of a polynomial $P \in \mathcal{C}_3$ of degree at least 3 that have rational modulus have the same modulus. Further, if R is this modulus, then $P(Rz)$ is a reciprocal polynomial.*

Proof. Let R be the largest rational modulus represented by the roots of P. Say $|\alpha| = R$ for a root α of P. Suppose that some root α_2 of P has rational modulus R_2. Then,

$$\alpha\overline{\alpha} = R^2, \qquad \alpha_2\overline{\alpha_2} = R_2^2.$$

Applying an embedding over $\mathbb{Q}$ that maps α to α_2 to the first equation yields $\alpha_2\alpha_3 = R^2$ for some conjugate α_3 of α. We therefore have

$$R^4 = \alpha_2\alpha_3\overline{\alpha_2\alpha_3} = \alpha_2\overline{\alpha_2}\alpha_3\overline{\alpha_3} = R_2^2|\alpha_3|^2.$$

It follows from the maximality of R that $R^2 \geq |\alpha_3|^2 = R^4/R_2^2 \geq R^2$. We therefore have equality so that, in particular, $R = R_2$. For the second part, we use Theorem 3 to write

$$P(z) = (Rz)^n Q(z/R + R/z)$$

for a suitable polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n. We then compute

$$\begin{aligned} z^{\deg P}P(R/z) &= z^{2n}(R^2/z)^n Q(1/z + z) \\ &= (R^2 z)^n Q(z + 1/z) = P(Rz), \end{aligned}$$

which was to be shown. □

In a similar way to the previous two sections it will be convenient to adopt the following notation. By Corollary 6, we know that all roots of a polynomial $P \in \mathcal{C}_3$ of degree at least 3 that have rational modulus have the same modulus. We call this quantity *the rational modulus of the roots of* P, denoted by $c_3(P)$. Clearly $c_3(P) > 0$.

Example 4. $(a)([-,-,1])$ *Let* $Q(z) = z^2 - 4z + 1$, *with roots* $2 \pm \sqrt{3}$, *one of which lies in* $(-2, 2)$. *Then Theorem 3 with* $R = 1$ *gives* $P(z) = z^2Q(z + 1/z) = z^4 - 4z^3 + 3z^2 - 4z + 1$, *which has two roots of modulus* 1, *namely* $1 - \frac{1}{2}\sqrt{3} \pm \frac{i}{2}\sqrt{-3 + 4\sqrt{3}}$.

$(b)([-,-,3])$ *If we choose* $Q(z) = z^2 - 2z + 1/4$, *then both roots* $1 \pm \frac{1}{2}\sqrt{3}$ *lie in* $(-2, 2)$, *and with* $R = 3$ *(for example) we get* $P(z) = (3z)^2Q(z/3 + 3/z) = z^4 - 6z^3 + (81/4)z^2 - 54z + 81$, *which has four roots of modulus* 3, *namely* $\frac{3}{4}(2 + \sqrt{3} \pm i\sqrt{9 - 4\sqrt{3}})$ *and* $\frac{3}{4}(2 - \sqrt{3} \pm i\sqrt{9 + 4\sqrt{3}})$.

R. M. Robinson [9] found a general construction for irreducible polynomials whose roots all lie on a circle with rational centre. Our construction of P is a variant of that of Robinson, who used $Q(z + R^2/z)$ instead of the more symmetric $Q(z/R + R/z)$. (On the other hand, Robinson's notation made it clear that his construction also worked when only R^2, rather than R, was rational.) Another difference is that Robinson required all roots of Q to lie in $(-2R, 2R)$, corresponding to our interval $(-2, 2)$, so that all

roots of P would have modulus R. Part (b) of the above example illustrates his construction, in our modified normalization. Robinson also conjectured that any irreducible polynomial having all its roots on a circle with rational centre c must be of the form $P(z-c)$, with P constructed in this way. This conjecture was disproved by Ennola [3]. See also [4, 5].

An immediate consequence of Corollaries 2, 4 and 6 is the following easy reducibility criterion.

Corollary 7. *If a polynomial of degree at least 3 with rational coefficients has roots with either*

– *different rational real parts, or*

– *rational imaginary parts of different absolute value, or*

– *different rational moduli,*

then it is reducible over $\mathbb{Q}$.

6. Polynomials in $\mathcal{C}_1 \cap \mathcal{C}_2$

In this and the following two sections we classify the polynomials that lie in the intersections of two of the classes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$.

Theorem 4 ($[r', r, -]$)**.** *Let P be a polynomial of degree at least 3. Then $P \in \mathcal{C}_1 \cap \mathcal{C}_2$ if and only if*

$$P(z) = \begin{cases} Q((z-r'+ir)^2)Q((z-r'-ir)^2) & \text{if } r \neq 0; \\ Q((z-r')^2) & \text{if } r = 0, \end{cases} \tag{7}$$

for some $r, r' \in \mathbb{Q}$ and some monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ having both a positive and a negative real root. In this case, P has a root with rational real part r' and a root with rational imaginary part r.

Proof. Since for any $r' \in \mathbb{Q}$ we clearly have that $P(z) \in \mathcal{C}_1 \cap \mathcal{C}_2$ if and only if $P(z-r') \in \mathcal{C}_1 \cap \mathcal{C}_2$, we can assume in our proof that P has a root having real part 0, (i.e., an imaginary root), so that $c_1(P) = 0$.

So suppose first that $P(z) \in \mathcal{C}_1 \cap \mathcal{C}_2$ has a root α with imaginary part r and a root α' with real part 0. Then, defining $\gamma = \alpha - ir$ and applying Lemma 1 to this equation, we get $\gamma' = \alpha' \pm ir$ for some choice of $\pm$ and some conjugate γ' of γ. Then γ is real and γ' is imaginary so that, on putting $\beta = \gamma^2$, $\beta' = \gamma'^2$ and defining Q to be the minimal polynomial of β, we see that Q has a positive real root β and a negative real root β'. Hence, by Lemma 3, the polynomial

$$\begin{cases} Q(z^2) & \text{if } r = 0; \\ Q((z-ir)^2)Q((z+ir)^2) & \text{if } r \neq 0 \end{cases} \tag{8}$$

is irreducible. But α is a root of this polynomial, and hence it is the minimal polynomial of α.

Conversely, given a monic irreducible polynomial Q having a positive real root, β say, and a negative real root, β' say, and a rational number r, and defining $\alpha = \sqrt{\beta} + ir$, we see that α is a root of the polynomial given by (8). Again, because this polynomial is irreducible, by Lemma 3, it is the minimal polynomial of α. Since α has imaginary part r and an imaginary conjugate $\alpha' = \pm\sqrt{\beta'} \pm ir$, we see that the polynomial $P(z)$ given by (8) belongs to $\mathcal{C}_1 \cap \mathcal{C}_2$. □

Example 5 ([1, 1, −]). *Let* $P(z) = z^8-8z^7+28z^6-56z^5+74z^4-72z^3+84z^2-88z+41$, *the minimal polynomial of* $1+i+\sqrt{1+\sqrt{2}}$. *Then* $Q(z) = z^2-2z-1$, *and* P *has four roots with real part* 1, *namely* $1 \pm i \pm \sqrt{1-\sqrt{2}}$, *and two roots with imaginary part* 1, *namely* $1 \pm \sqrt{1+\sqrt{2}} + i$. *So* $P \in \mathcal{C}_1 \cap \mathcal{C}_2$.

7. Polynomials in $\mathcal{C}_1 \cap \mathcal{C}_3$

In order to classify the polynomials that lie in both $\mathcal{C}_1$ and $\mathcal{C}_3$, we begin with a general characterization.

Theorem 5. *Let* $P \in \mathcal{C}_1 \cap \mathcal{C}_3$ *have degree at least* 3. *Then either* $c_1(P) = 0$ *or* $c_1(P) = \pm\frac{1}{2}c_3(P)$.

Proof. Suppose that $P \in \mathcal{C}_1 \cap \mathcal{C}_3$ is of degree at least 3, has a root β with rational real part r' and a root with rational modulus R. We need to prove that $r' = 0$ or $|r'| = R/2$. Now $P(\pm Rz)$ has $\pm\beta/R$ as a root with rational real part $\pm r'/R$ and also has a root of modulus 1. Define Q to be the polynomial corresponding to the choice of sign that gives rise to a root α with nonnegative real part $r := |r'|/R$. We complete the proof by showing that $r = 0$ or $r = \frac{1}{2}$.

We have $\alpha + \overline{\alpha} = 2r$ and $\alpha_1\overline{\alpha_1} = 1$. It follows from Lemma 1 that for every conjugate α' of α, both $2r - \alpha'$ and $1/\alpha'$ are conjugates of α. Consequently, the set S_α of all $\mathbb{Q}$-conjugates of α is stable under the Möbius transformations $z \mapsto 2r - z$ and $z \mapsto 1/z$. Since $r \geq 0$, these Möbius transformations generate the subgroup H_{2r} of G defined above. Now, if H_{2r} were infinite, then, as the H_{2r}-orbit of α is finite, α would have to be a fixed point of some $h \in H_{2r}$. But this implies that α and consequently Q has degree at most 2 over $\mathbb{Q}$, which is a contradiction. We conclude that H_{2r} is finite so that, by Lemma 4, $2r = 0$ or $2r = 1$, as required. □

By Theorem 5 we see that the polynomials of degree at least 3 in $\mathcal{C}_1 \cap \mathcal{C}_3$ are split into two categories. There are those that have a purely imaginary

root ($c_1(P) = 0$), and then there are those having roots with rational real part equal to plus or minus one half of the rational modulus of their roots ($c_1(P) = \pm\frac{1}{2}c_3(P)$). The next result characterizes the polynomials of the first variety.

Theorem 6 ([0, −, R])**.** *Let P be a polynomial of degree at least 3. Then $P \in \mathcal{C}_1 \cap \mathcal{C}_3$ and has a purely imaginary root if and only if $P(z) = (Rz)^{2n}Q((z/R + R/z)^2)$ for some positive $R \in \mathbb{Q}$ and monic irreducible $Q(z) \in \mathbb{Q}[z]$ of degree n having a real root in the interval $(0, 4)$ as well as a negative real root. In this case, P has a root with rational modulus R.*

Proof. First let $P \in \mathcal{C}_1 \cap \mathcal{C}_3$ be of degree at least 3 and have a purely imaginary root. As in the proof of Theorem 5, we may suppose that P has a purely imaginary root α, as well as a root α_1 with modulus 1. We then need to prove that

$$P(z) = z^{2n}Q((z + 1/z)^2)$$

for some polynomial Q as in the statement of the theorem. Define

$$s_0(z) = 2 + \frac{1}{2}\sum_{h\in H_0} h^2 = \left(z + \frac{1}{z}\right)^2$$

(see Lemma 4), $\beta = s_0(\alpha)$ and let Q be the minimal polynomial of β. Since α satisfies the polynomial

$$z^4 + (2 - \beta)z^2 + 1 \in \mathbb{Q}(\beta)[z], \tag{9}$$

we see that $[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] \leq 4$. Thus

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] \leq 4n, \tag{10}$$

where n is the degree of Q, so that α has at most $4n$ conjugates over $\mathbb{Q}$. But, since $s_0(\alpha)$ is H_0-invariant, we see that β is realized as $s_0(z)$ for all four of $z = \alpha, -\alpha, 1/\alpha$ and $-1/\alpha$. Thus each conjugate of β corresponds to at least 4 conjugates of α. It follows that α has at least $4n$ conjugates over $\mathbb{Q}$ so that, in fact, we have equality in (10). Since α is a root of the polynomial $z^{2n}Q((z + 1/z)^2)$, we can conclude by degree consideration that

$$P(z) = z^{2n}Q((z + 1/z)^2).$$

Now, Q is monic and irreducible. Further, as α is purely imaginary, we see that it has β as a real negative root. Finally, as $|\alpha_1| = 1$, we see that it has $(\alpha_1 + 1/\alpha_1)^2 = 4\Re(\alpha_1)^2$ as a real positive root lying in the interval $(0, 4)$.

Conversely, we may suppose that $R = 1$ so that we are reduced to proving that for a monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n having a real negative root β, as well as a real positive root β' lying in the interval

$(0,4)$, the polynomial $P(z) = z^{2n}Q((z+1/z)^2)$ lies in $\mathcal{C}_1 \cap \mathcal{C}_3$ and has a purely imaginary root. Since $\beta < 0$, the equation $(z+1/z)^2 = \beta$ has purely imaginary roots. Similarly, since $\beta' \in (0,4)$, the equation $(z+1/z)^2 = \beta'$ has nonreal roots of modulus 1. As these are roots of P and P is monic, the proof will be complete as soon as we verify that P is irreducible. To this end, let $(\alpha+1/\alpha)^2 = \beta$ and $(\alpha_1+1/\alpha_1)^2 = \beta'$ so that α is a purely imaginary root of P and α_1 is a nonreal root of P of modulus 1. It is enough to verify that $\deg_{\mathbb{Q}}(\alpha) = 4n$. Since $\sqrt{\beta} \notin \mathbb{R}$ and $\mathbb{Q}(\beta)$ is a real field, $[\mathbb{Q}(\sqrt{\beta}) : \mathbb{Q}(\beta)] = 2$. Also, if α were to lie in $\mathbb{Q}(\sqrt{\beta})$, we would be able to apply a suitable $\mathbb{Q}$-embedding that maps β to β' to obtain $\alpha_1 \in \mathbb{Q}(\sqrt{\beta'}) \subseteq \mathbb{R}$. This would contradict the fact that α_1 is nonreal. As α is of degree at most 2 over $\mathbb{Q}(\sqrt{\beta})$, we can conclude that $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{\beta})] = 2$. We therefore have

$$\begin{aligned}\deg_{\mathbb{Q}}(\alpha) &= [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{\beta})][\mathbb{Q}(\sqrt{\beta}) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] \\ &= 2 \cdot 2 \cdot n = 4n,\end{aligned}$$

as required. □

We illustrate Theorem 6 with the following example.

Example 6 ($[0,-,2]$)**.** *Let $Q(z) = z^2 - 2z - 1$, with roots $1 \pm \sqrt{2}$, one of which is negative, while the other one lies in $(0,4)$. Then $P(z) = (2z)^4 Q((\frac{z}{2} + \frac{2}{z})^2) = z^8 + 8z^6 + 16z^4 + 128z^2 + 256$ is irreducible, has four purely imaginary roots (and so of rational real part), namely $i(\pm\sqrt{-1+\sqrt{2}} \pm \sqrt{3+\sqrt{2}})$, and four roots of modulus 2, namely $\pm\sqrt{1+\sqrt{2}} \pm i\sqrt{3-\sqrt{2}}$. So $P \in \mathcal{C}_1 \cap \mathcal{C}_3$.*

When we try to classify the second type of polynomials in $\mathcal{C}_1 \cap \mathcal{C}_3$, we cannot guarantee the irreducibility of the characterizing polynomials. Indeed, Example 8 below shows that reducibility can occur. (In general, reducibility of polynomials is a difficult subject, as Schinzel's comprehensive treatise [10] shows.)

Theorem 7 ($[\pm\frac{R}{2}, -, R]$)**.** *Let P be a polynomial of degree at least 3. Then $P \in \mathcal{C}_1 \cap \mathcal{C}_3$ and $c_1(P) = \pm\frac{1}{2}c_3(P)$ if and only if P is irreducible and $P(z)$ or $P(-z)$ is given by*

$$(Rz)^{2n}(z-R)^{2n}Q(\ell(z/R)^2) \tag{11}$$

for some positive $R \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has a negative real root, where ℓ is given by (3)*. In this case, P has a root with rational modulus R.*

Proof. First, let $P \in \mathcal{C}_1 \cap \mathcal{C}_3$ be of degree at least 3 and such that $c_1(P) = \pm\frac{1}{2}c_3(P)$. As in the proofs of Theorems 5 and 6, we may suppose that P

has a root α with rational real part $\frac{1}{2}$, as well as a root α_1 of modulus 1. It is sufficient to prove that

$$P(z) = z^{2n}(z-1)^{2n}Q(\ell(z)^2)$$

for some monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has a negative real root. Define

$$s_1(z) = -\tfrac{21}{4} + \tfrac{1}{2}\sum_{h\in H_1} h^2 = \ell(z)^2$$

(see Lemma 4), $\beta = s_1(\alpha)$ and Q to be the minimal polynomial of β. Since the image under s_1 of the line $\Re(z) = \frac{1}{2}$ is the interval $(-\infty, 0)$, we see that Q has β as a negative real root. Since Q is both monic and irreducible, we are reduced to proving that

$$P(z) = z^{2n}(z-1)^{2n}Q(\ell(z)^2).$$

As usual, we will prove the equality by degree considerations. In this case, we have to show that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6n$. Since the equation $\ell(\alpha)^2 = \beta$ provides a degree 6 polynomial over $\mathbb{Q}(\beta)$ satisfied by α, we see that the index in question is at most $6[\mathbb{Q}(\beta) : \mathbb{Q}] = 6n$. On the other hand, since $s_1(\alpha)$ is H_1-invariant, we see that β is realized as $s_1(z)$ for each of the six values $h(\alpha)$ as h runs through H_1. It follows that to each conjugate of β, we can associate 6 conjugates of α so that α has at least $6n$ conjugates. It follows that we have equality so that, as remarked above, the proof of this direction is complete.

Conversely, using the same substitutions as above, we are reduced to proving that for a monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n having a real negative root, the polynomial $P(z) = z^{2n}(z-1)^{2n}Q(\ell(z)^2)$ lies in $\mathcal{C}_1 \cap \mathcal{C}_3$ and has a root with real part $\frac{1}{2}$, as well as a root with modulus 1, provided it is irreducible. Since we are assuming irreducibility, and P is monic, we are reduced to proving that it has a root with real part $\frac{1}{2}$ as well as a root with modulus 1. But if β is a negative real root of Q, then $\ell(z)^2 = \beta$ has a root α with real part equal to $\frac{1}{2}$, and, in fact, all roots are given by $h(\alpha)$ for $h \in H_1$. Since two of the $h(\alpha)$ lie on the unit circle, we also have a root of $\ell(z)^2 = \beta$ on the unit circle. It follows that P has roots of the desired form. □

The following example illustrates Theorem 7.

Example 7 ($[\pm\frac{1}{2}, -, 1]$)**.** *Let* $Q(z) = z+23/4$*, and* $P(z) = z^2(z-1)^2Q(\ell(z)^2)$ $= z^6 - 3z^5 + 5z^4 - 5z^3 + 5z^2 - 3z + 1$*. Then* P *is irreducible and has two roots with real part* $\frac{1}{2}$ *and two roots of modulus* 1*. If we replace* z *by* $-z$*, we*

get an example with zeros having real part $-\frac{1}{2}$. Hence in both cases we have again $P \in \mathcal{C}_1 \cap \mathcal{C}_3$.

We now discuss the possible reducibility of the polynomial P given by (11). As above, we can restrict our attention to the case $R = 1$ and P having a root α with real part $\frac{1}{2}$. Then

$$P(z) = z^{2n}(z-1)^{2n}Q(\ell(z)^2),$$

where $Q(z) \in \mathbb{Q}[z]$ is a monic irreducible polynomial of degree n having a negative real root $\beta = \ell(\alpha)^2 = s_1(\alpha)$. Now, all six roots of $s_1(z) = \beta$ define the same extension field $\mathbb{Q}(\alpha)$ of $\mathbb{Q}(\beta)$. This is because for any other root α', we have $\alpha' = h(\alpha)$ for some $h \in H_1$. We examine the various possibilities for the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)]$. We first note that the index must be a positive divisor of 6 since each of the $h(\alpha)$ must have the same degree over $\mathbb{Q}(\beta)$ and they satisfy a polynomial of degree 6. Since α has rational real part but is itself irrational, α must be nonreal. Since $\mathbb{Q}(\beta)$ is a real field, we see that $\alpha \notin \mathbb{Q}(\beta)$ so that the index in question cannot equal 1. It cannot be equal to 3 either, as we now show. If the index in question were equal to 3, then the minimal polynomial of α over $\mathbb{Q}(\beta)$ would have degree 3 and consequently a real root. This root must be equal to one of the $h(\alpha)$ as h runs through H_1. However, these values consist of the two points $\alpha, 1-\alpha$ on the line $\Re(z) = \frac{1}{2}$, the two points $1/\alpha$ and $1/(1-\alpha)$ on the circle $|z-1| = 1$ and the two points $\alpha/(\alpha-1)$ and $(\alpha-1)/\alpha$ on the circle $|z| = 1$. The real root would then have to be one of the real points on these curves, which are -1, 0, $\frac{1}{2}$, 1 or 2. Since all of these values are rational, this is impossible. We conclude that $[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] = 2$ or 6. We have irreducibility in case the index is 6 and so the reducible case corresponds to $[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] = 2$.

The following is an example of the occurrence of reducibility.

Example 8. *Let $\alpha = \frac{1}{2} + i\sqrt[4]{t}$ for $t \in \mathbb{N}$ square-free. Then we have*

$$\beta = s_1(\alpha) = \ell(\alpha)^2 = -\frac{\sqrt{t}(9+4\sqrt{t})^2}{(1+4\sqrt{t})^2} \in \mathbb{Q}(\sqrt{t}).$$

As $[\mathbb{Q}(\sqrt{t}) : \mathbb{Q}] = 2$, and β is irrational, we see that $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$ so that $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{t})$. Now, since α is a root of the polynomial $(z-\frac{1}{2})^2 + \sqrt{t} \in \mathbb{Q}(\sqrt{t})[z]$, we see that $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{t})] \le 2$. In fact $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{t})] = 2$, as α is nonreal. Therefore, α has degree 2 over $\mathbb{Q}(\beta)$ so that, taking $Q(z) \in \mathbb{Q}[z]$ of degree n to be the minimal polynomial of β, the polynomial P given by

$$P(z) = z^{2n}(z-1)^{2n}Q(\ell(z)^2)$$

is reducible. In fact, calculation shows that

$$Q(z) = z^2 + \frac{128t(16t-9)}{(16t-1)^2}z - \frac{t(16t-81)^2}{(16t-1)^2},$$

and

$$P(z) = z^4(z-1)^4Q(\ell(z)^2) = \frac{1}{16(16t-1)^2}P_1(z)P_2(z)P_3(z),$$

where

$$P_1(z) = (16t-1)z^4 + 8z^3 - 24z^2 + 32z - 16;$$
$$P_2(z) = (16t-1)z^4 - (64t+4)z^3 + (96t-6)z^2 - (64t+4)z + 16t - 1;$$
$$P_3(z) = 16z^4 - 32z^3 + 24z^2 - 8z - 16t + 1.$$

The minimal polymomial of α *is* $\frac{1}{16}P_3$.

8. Polynomials in $\mathcal{C}_2 \cap \mathcal{C}_3$

In a similar way to Section 7 we begin the classification of the polynomials in $\mathcal{C}_2 \cap \mathcal{C}_3$ with a general result.

Theorem 8. *Let* $P \in \mathcal{C}_2 \cap \mathcal{C}_3$ *have degree at least* 3. *Then either* $c_2(P) = 0$ *or* $c_2(P) = \frac{1}{2}c_3(P)$.

Proof. Assume the hypotheses, let α be a root of P with rational imaginary part r' and α_1 be a root of P with rational modulus R. Then the minimal polynomial P_1 of $i\alpha$ has a root $i\alpha$ with rational real part $-r'$ and the root $i\alpha_1$ with rational modulus R. It follows that P_1 lies in $\mathcal{C}_1 \cap \mathcal{C}_3$ so that, by Theorem 5, we have either $-r' = 0$ or $-r' = \pm R/2$. The result follows. □

By Theorem 8 we see that the polynomials of degree at least 3 in $\mathcal{C}_2 \cap \mathcal{C}_3$ are split into two families. There are those that have a real root ($c_2(P) = 0$), and then there are those having roots with nonnegative rational imaginary part equal to one half of the rational modulus of their roots ($c_2(P) = \frac{1}{2}c_3(P)$). The next result characterizes the polynomials of the first family.

Theorem 9 ([−, 0, R])**.** *Let* P *be a polynomial of degree at least* 3. *Then* $P \in \mathcal{C}_2 \cap \mathcal{C}_3$ *and has a real root if and only if* $P(z) = (Rz)^n Q(z/R + R/z)$ *for some positive* $R \in \mathbb{Q}$ *and monic irreducible polynomial* $Q(z) \in \mathbb{Q}[z]$ *of degree* n *having a real root* inside *the interval* $(-2, 2)$, *as well as a real root* outside *the interval* $(-2, 2)$. *In this case,* P *has a root with rational modulus* R.

Proof. First, let $P \in \mathcal{C}_2 \cap \mathcal{C}_3$ be of degree at least 3 and have a real root. Suppose that P has a real root α and a root α_1 of modulus R. By Theorem 3, we know that P can be written in the desired form, and that the resulting polynomial Q will have a root lying *inside* the interval $(-2, 2)$. In fact, from the proof of Theorem 3, we can take Q to be the minimal polynomial of $\frac{\alpha_1}{R} + \frac{R}{\alpha_1} \in (-2, 2)$. Since Q is then also the minimal polynomial of $\frac{\alpha}{R} + \frac{R}{\alpha}$, which lies *outside* the interval $(-2, 2)$, Q also has a root lying outside this interval.

Conversely, we may suppose, as above, that $R = 1$. We are therefore reduced to proving that for a monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n having a root inside the interval $(-2, 2)$ as well as a root outside this interval, the polynomial P given by

$$P(z) = z^n Q(z + 1/z)$$

lies in $\mathcal{C}_2 \cap \mathcal{C}_3$ and has a real root. Suppose then that $\beta \notin (-2, 2)$ and $\beta' \in (-2, 2)$ are real roots of Q. The equation $z + 1/z = \beta$ has a real root α which must then be a root of P. Also, the equation $z + 1/z = \beta'$ has a complex root α' of modulus 1 which must be a root of P. The result will then follow once we establish irreducibility. We will accomplish this by showing that the degree of α' over $\mathbb{Q}$ is equal to $2n$ so that P has the correct degree to be the minimal polynomial of α' and therefore be irreducible. Since α' is nonreal and $\mathbb{Q}(\beta')$ is a real field, we see that $\alpha' \notin \mathbb{Q}(\beta')$. Consequently, $[\mathbb{Q}(\alpha') : \mathbb{Q}(\beta')] \geq 2$. On the other hand, α' satisfies the polynomial $z^2 - \beta' z + 1 \in \mathbb{Q}(\beta')[z]$ so that $[\mathbb{Q}(\alpha') : \mathbb{Q}(\beta')] \leq 2$. We therefore have equality, so that

$$[\mathbb{Q}(\alpha') : \mathbb{Q}] = [\mathbb{Q}(\alpha') : \mathbb{Q}(\beta')][\mathbb{Q}(\beta') : \mathbb{Q}] = 2[\mathbb{Q}(\beta') : \mathbb{Q}] = 2n,$$

as required. □

Theorem 9 is illustrated by the following example.

Example 9 ([−, 0, 2])**.** *Let* $Q(z) = z^2 - 2z - 1$*, with roots* $1 \pm \sqrt{2}$*, one of which lies in* $(-2, 2)$*, while the other one does not. Then* $P(z) = (2z)^2 Q(\frac{z}{2} + \frac{2}{z}) = z^4 - 4z^3 + 4z^2 - 16z + 16$ *is irreducible, has two real roots (and so of rational imaginary part), namely* $1 + \sqrt{2} \pm \sqrt{-1 + 2\sqrt{2}}$*, and two roots of modulus 2, namely* $1 - \sqrt{2} \pm i\sqrt{1 + 2\sqrt{2}}$*. Hence* $P \in \mathcal{C}_2 \cap \mathcal{C}_3$*.*

When we try to classify the second type of polynomials in $\mathcal{C}_2 \cap \mathcal{C}_3$, as in the previous section we cannot guarantee the irreducibility of the characterizing polynomials, as Example 11 below shows.

Theorem 10 ($[-, \frac{R}{2}, R]$)**.** *Let P be a polynomial of degree at least 3. Then $P \in \mathcal{C}_2 \cap \mathcal{C}_3$ and $c_2(P) = \frac{1}{2}c_3(P)$ if and only if P is irreducible and has the form*

$$P(z) = (Rz)^{2n}(z^2 + R^2)^n Q(-i\ell(iz/R))Q(i\ell(-iz/R)) \tag{12}$$

for some positive $R \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has a nonzero real root, where ℓ is given by (3)*. In this case, P has a root with rational modulus R.*

Proof. First, let $P \in \mathcal{C}_2 \cap \mathcal{C}_3$ be of degree at least 3 and such that $c_2(P) = \frac{1}{2}c_3(P)$. As above it is sufficient to assume that $R = c_3(P) = 1$. We then need to prove

$$P_1(z) = z^{2n}(z^2 + 1)^n Q(-i\ell(iz))Q(i\ell(-iz)) \tag{13}$$

for some monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has a nonzero real root. In order to prove (13), we proceed as follows.

Write $\alpha = \gamma + i/2$, where γ is real and algebraic. Then $\alpha^* = \gamma^* + \varepsilon i/2$ for some conjugate γ^* of γ and $\varepsilon = \pm 1$. Define $H(z_1, z_2, z_3) = (z_1 + \varepsilon z_3/2)(z_2 - \varepsilon z_3/2) - 1$. Then $H(\gamma^*, \overline{\gamma^*}, i) = 0$. By Corollary 1, we see that to each conjugate γ' of γ, we can associate conjugates γ'' and γ''' of γ such that

$$(\gamma' + i/2)(\gamma'' - i/2) = 1;$$
$$(\gamma' - i/2)(\gamma''' + i/2) = 1.$$

Solving these equations for γ'' and γ''' yields $\gamma'' = F(\gamma')$ and $\gamma''' = \overline{F}(\gamma')$, where F is given by (4) and $\overline{F}$ is its conjugate given by

$$\overline{F}(z) = \frac{-\frac{i}{2}z + \frac{3}{4}}{z - \frac{i}{2}}.$$

Therefore, both F and $\overline{F}$ preserve the set of conjugates of γ. Now put

$$f(w) = w + F(w) + \overline{F}(w) = \frac{w(w^2 + \frac{9}{4})}{w^2 + \frac{1}{4}},$$

and define $\beta = f(\gamma)$ and $Q(z) \in \mathbb{Q}[z]$ to be the minimal polynomial of β. A calculation shows that $F \circ F = \overline{F}$ and $\overline{F} \circ F$ is the identity map. Thus $f(F(z)) = f(z)$. It can also be verified that $f(z \pm i/2) = \mp i\ell(\pm iz)$ so that α satisfies the numerator of $Q(f(z + i/2))Q(f(z - i/2))$ which is the monic polynomial in $\mathbb{Q}[z]$ given by

$$z^{2n}(z^2 + 1)^n Q(-i\ell(iz))Q(i\ell(-iz)),$$

where n is the degree of Q. Since Q has β as a nonzero real root, we are reduced to proving that α has degree $6n$ over $\mathbb{Q}$. Since $\alpha = \gamma + i/2$ and γ is real, we have $\deg_{\mathbb{Q}}(\alpha) = 2\deg_{\mathbb{Q}}(\gamma) = 2[\mathbb{Q}(\gamma) : \mathbb{Q}(\beta)]n$. We therefore need

to prove that γ has degree three over $\mathbb{Q}(\beta)$. Since γ satisfies the polynomial $z^3-\beta z^2+\frac{9}{4}z-\frac{1}{4}\beta \in \mathbb{Q}(\beta)[z]$, we see that the index in question is at most 3. Conversely, β is realized as $f(z)$ for each of $z=\gamma$, $z=F(\gamma)$ and $z=\overline{F}(\gamma)$. It follows that each conjugate β' of β corresponds to at least 3 conjugates of γ. Therefore, $[\mathbb{Q}(\gamma):\mathbb{Q}(\beta)] \geq 3$. We therefore have equality so that the proof of this direction is complete.

Conversely, we can suppose that $R=1$ so that P is given by

$$P(z) = z^{2n}(z^2+1)^n Q(-i\ell(iz))Q(i\ell(-iz))$$

for some monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has a nonzero real root β. Since P is monic, and we are assuming irreducibility, it suffices to show that P has a root α^* of modulus 1 and a root α with imaginary part $\frac{1}{2}$. We do this by verifying that $i\ell(-iz)=\beta$ has roots of the desired form. If we square both sides, we obtain the equation $\ell(-iz)^2=-\beta^2$. Since the right-hand side is negative, we know from the proof of Theorem 7 that this equation has six solutions for $-iz$ given by $h(\gamma)$ as h runs through H_1 and γ has real part equal to $\frac{1}{2}$. Multiplying by i gives us six solutions for z, two of which have imaginary part equal to $\frac{1}{2}$ and two of which lie on the unit circle. □

The following example illustrates Theorem 10.

Example 10 ($[-,\frac{1}{2},1]$)**.** *Let $Q(z)=z-1$, and, for ℓ as defined in Theorem 10,*

$$\begin{aligned} P(z) &= z^2(z^2+1)Q(-i\ell(iz))Q(i\ell(-iz)) \\ &= z^2(z^2+1)(-i\ell(iz)-1)(i\ell(-iz)-1) \\ &= z^6-2z^5+(25/4)z^4-6z^3+(25/4)z^2-2z+1. \end{aligned}$$

Then P is irreducible and has one root with imaginary part $\frac{1}{2}$, and two roots of modulus 1. Again $P \in \mathcal{C}_2 \cap \mathcal{C}_3$.

The next example shows that reducibility can occur in this situation as well. In fact, remarks similar to those immediately following Example 7 apply here too.

Example 11. *Let $\alpha = \sqrt[4]{t}+i/2$ for a square-free integer $t>1$. Then we have*

$$\beta = s(\sqrt[4]{t}) = i\ell(-i\alpha) = \frac{\sqrt[4]{t}(9+4\sqrt{t})}{1+4\sqrt{t}},$$

and β satisfies the polynomial

$$Q(z) = z^4 - \frac{128t(16t-9)}{(16t-1)^2}z^2 - \frac{t(16t-81)^2}{(16t-1)^2} \in \mathbb{Q}[z].$$

The discriminant of Q (as a quadratic in z^2) is $4t(256t^2+736t+81)^2$, which for a square-free integer $t>1$ cannot be a perfect square. Hence Q is irreducible as a polynomial in z^2 and thus in z, and is therefore the minimal polynomial of β. Note that $\gamma=\sqrt[4]{t}$ has the same degree over $\mathbb{Q}$ as β, so that $[\mathbb{Q}(\gamma):\mathbb{Q}(\beta)]=1$. The fact that this index is not equal to 3 implies that we do in fact obtain a reducible polynomial P. Calculation using Maple shows that, in fact,

$$P(z)=z^8(z^2+1)^4Q(-i\ell(iz))Q(i\ell(-iz))=\frac{1}{256(16t-1)^4}P_1(z)P_2(z)P_3(z),$$

where

$$\begin{aligned}P_1(z)&=(16t-1)^2z^8+(768t+16)z^6-(512t-96)z^4+256z^2+256;\\ P_2(z)&=(16t-1)^2z^8+(1024t^2+896t+4)z^6+(1536t^2-2240t+6)z^4\\ &\qquad+(1024t^2+896t+4)z^2+(16t-1)^2;\\ P_3(z)&=256z^8+256z^6-(512t-96)z^4+(768t+16)z^2+(16t-1)^2.\end{aligned}$$

The minimal polynomial of α is $\frac{1}{256}P_3$.

9. Polynomials in $\mathcal{C}_1\cap\mathcal{C}_2\cap\mathcal{C}_3$.

In this final section we study polynomials that are simultaneously minimal polynomials for an algebraic number of rational real part, an algebraic number of rational imaginary part and an algebraic number of rational modulus.

We know from Theorems 5 and 8 that for $P\in\mathcal{C}_1\cap\mathcal{C}_2\cap\mathcal{C}_3$ of degree at least 3, we have $c_1(P)=0$ or $c_1(P)=\pm\frac{1}{2}c_3(P)$ and $c_2(P)=0$ or $c_2(P)=\frac{1}{2}c_3(P)$. We now separate the four cases.

Theorem 11 ([0, 0, R])**.** *Let P be a polynomial of degree at least 3. Then $P\in\mathcal{C}_1\cap\mathcal{C}_2\cap\mathcal{C}_3$, and has both a real root and a purely imaginary root if and only if P is of the form $P(z)=(Rz)^{2n}Q((z/R+R/z)^2)$ for some positive $R\in\mathbb{Q}$ and monic irreducible polynomial $Q(z)\in\mathbb{Q}[z]$ of degree n that has a real root in each of the intervals $(-\infty,0),(0,4),(4,\infty)$. In this case, P has a root with rational modulus R.*

Proof. Suppose first that $P\in\mathcal{C}_1\cap\mathcal{C}_2\cap\mathcal{C}_3$ and has both a real root and a purely imaginary root. Applying Theorem 6, we know that

$$P(z)=(Rz)^{2n}Q((z/R+R/z)^2)$$

for some positive $R\in\mathbb{Q}$ and monic irreducible polynomial $Q(z)\in\mathbb{Q}[z]$ of degree n that has a root in each of the intervals $(-\infty,0)$ and $(0,4)$. We complete the proof of this direction by establishing that Q also has

a root in the interval $(4,\infty)$. But this follows from the hypothesis that $Q((z/R+R/z)^2)=0$ has a real root, which must be irrational, and therefore must correspond to a value of $(z/R+R/z)^2$ that is greater than 4.

Conversely, suppose that $P(z)=(Rz)^{2n}Q((z/R+R/z)^2)$ for some positive $R\in\mathbb{Q}$ and monic irreducible polynomial $Q(z)\in\mathbb{Q}[z]$ of degree n that has a real root in each of the intervals $(-\infty,0),(0,4),(4,\infty)$. Then, by Theorem 6, we know that $P\in\mathcal{C}_1\cap\mathcal{C}_3$. All that is left to prove is that P has a real root. But this follows from the fact that for a root $t>4$ of Q, the equation $(z/R+R/z)^2=t$ has a real solution. □

Theorem 11 is illustrated by the following example.

Example 12 ([0, 0, 1])**.** *Let* $Q(z)=z^3-4z^2-4z+8$*, with roots* $2+4\cos(2\pi k/7)$ $(k=1,2,3)$*, which lie in the intervals* $(-\infty,0),(0,4),(4,\infty)$*, respectively. Then* $P(z)=z^6Q((z+1/z)^2)=z^{12}+2z^{10}-5z^8-4z^6-5z^4+2z^2+1$ *is irreducible, has four imaginary roots (and so of rational real part), four real roots (and so of rational imaginary part), and four roots of modulus* 1*. Hence* $P\in\mathcal{C}_1\cap\mathcal{C}_2\cap\mathcal{C}_3$*.*

As in several cases in Sections 7 and 8, we cannot guarantee the irreducibility of the polynomial P. Further remarks on this can be found at the end of this section.

Theorem 12 ($[0,\frac{R}{2},R]$)**.** *Let* P *be a polynomial of degree at least* 3*. Then* $P\in\mathcal{C}_1\cap\mathcal{C}_2\cap\mathcal{C}_3$ *has a purely imaginary root and is such that* $c_2(P)=\frac{1}{2}c_3(P)$ *if and only if* P *is irreducible and has the form*

$$P(z)=(Rz)^{4n}(z^2+R^2)^{2n}Q(-\ell(iz/R)^2)Q(-\ell(-iz/R)^2) \tag{14}$$

for some positive $R\in\mathbb{Q}$ *and monic irreducible polynomial* $Q(z)\in\mathbb{Q}[z]$ *of degree* n *that has both a real positive root and a real negative root, where* ℓ *is given by* (3)*. In this case,* P *has a root with rational modulus* R*.*

Proof. Suppose first that $P\in\mathcal{C}_1\cap\mathcal{C}_2\cap\mathcal{C}_3$ has a purely imaginary root and is such that $c_2(P)=\frac{1}{2}c_3(P)$. By Theorem 10, we know that P has the form

$$P(z)=(Rz)^{2\deg Q_1}(z^2+R^2)^{\deg Q_1}Q_1(-i\ell(iz/R))Q_1(i\ell(-iz/R))$$

for some positive $R\in\mathbb{Q}$ and monic irreducible polynomial $Q_1(z)\in\mathbb{Q}[z]$ that has a nonzero real root β. By hypothesis, $P(i\gamma)=0$ for some irrational $\gamma\in\mathbb{R}$. It follows that one of $-i\ell(-\gamma/R)$ and $i\ell(\gamma/R)$ is a root of Q_1. In any case, Q_1 has a purely imaginary root. Since its negative must also be a root of Q_1, we see from Lemma 2 that $Q_1(z)=Q(z^2)$ for some monic irreducible

polynomial $Q(z) \in \mathbb{Q}[z]$. Since this implies that

$$P(z) = (Rz)^{4n}(z^2+R^2)^{2n}Q(-\ell(iz/R)^2)Q(-\ell(-iz/R)^2),$$

where n is the degree of Q, we are reduced to proving that Q has both a positive real root and a negative real root. But this follows from the fact that Q_1 has both a nonzero real root and a nonzero purely imaginary root.

Conversely, suppose that P is irreducible, of degree at least 3 and has the form

$$P(z) = (Rz)^{4n}(z^2+R^2)^{2n}Q(-\ell(iz/R)^2)Q(-\ell(-iz/R)^2)$$

for some positive $R \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has both a positive real root β and a negative real root γ. Defining $Q_1(z) = Q(z^2)$, we have $Q_1(iz) = Q_1(-iz) = Q(-z^2)$. We can therefore write

$$P(z) = (Rz)^{2\deg Q_1}(z^2+R^2)^{\deg Q_1}Q_1(-i\ell(iz/R))Q_1(i\ell(-iz/R)),$$

where Q_1 has a nonzero real root. We can therefore apply Theorem 10 to conclude that $P \in \mathcal{C}_2 \cap \mathcal{C}_3$ and that $c_2(P) = \frac{1}{2}c_3(P)$. The proof is completed by noticing that the equation $-\ell(iz/R)^2 = \gamma$ has a purely imaginary solution z. □

Theorem 12 is illustrated by the following example.

Example 13 ($[0, \frac{1}{2}, 1]$)**.** *Let $Q(z) = z^2 - z - 1$, with roots $(1 \pm \sqrt{5})/2$, (one positive and one negative), and*

$$\begin{aligned} P(z) &= z^8(z^2+1)^4Q(-\ell(iz)^2)Q(-\ell(-iz)^2) \\ &= \tfrac{1}{256}\left(256z^{24} + 4864z^{22} + 39136z^{20} + 175920z^{18} + 484345z^{16}\right. \\ &\quad +856564z^{14} + 1023126z^{12} + 856564z^{10} + 484345z^8 + 175920z^6 \\ &\quad \left.+39136z^4 + 4864z^2 + 256\right). \end{aligned}$$

Then P has 12 imaginary roots (and so of rational real part), two roots of imaginary part $\frac{1}{2}$, and four roots of modulus 1. Again $P \in \mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_3$.

Theorem 13 ($[\pm\frac{R}{2}, 0, R]$)**.** *Let P be a polynomial of degree at least 3. Then $P \in \mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_3$, has a real root and is such that $c_1(P) = \pm\frac{1}{2}c_3(P)$ if and only if P is irreducible and one of $P(z)$ or $P(-z)$ is given by*

$$(Rz)^{2n}(z-R)^{2n}Q(\ell(z/R)^2)$$

for some positive $R \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has both a positive real root and a negative real root. In this case, P has a root with rational modulus R.

Proof. Suppose first that $P \in \mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_3$, has a real root and is such that $c_1(P) = \pm\frac{1}{2}c_3(P)$. By Theorem 7, we know that one of $P(z)$, $P(-z)$ is of the form

$$(Rz)^{2n}(z-R)^{2n}Q(\ell(z/R)^2)$$

for some positive $R \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has a negative real root. Finally, the fact that P has a real root implies that Q has a positive real root.

Conversely, suppose that P is irreducible and $P(z)$ or $P(-z)$ has the form

$$(Rz)^{2n}(z-R)^{2n}Q(\ell(z/R)^2)$$

for some positive $R \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has both a positive real root and a negative real root. We know from Theorem 7 that P lies in $\mathcal{C}_1 \cap \mathcal{C}_3$ and is such that $c_1(P) = \pm\frac{1}{2}c_3(P)$. We are left with verifying that P has a real root. But this follows from setting $\ell(z/R)^2$ equal to a positive real root of Q and extracting a real root z from the resulting equation. □

The following example illustrates Theorem 13.

Example 14 ($[-1, 0, 2]$)**.** *Let $Q(z) = z^2 - z - 1$, with roots $(1 \pm \sqrt{5})/2$ (one positive and one negative). Then*

$$\begin{aligned} P(z) &= (2z)^4(z+2)^4Q(\ell(-z/2)^2) \\ &= z^{12} + 12z^{11} + 26z^{10} - 180z^9 - 755z^8 + 392z^7 + 4600z^6 \\ &\quad + 1568z^5 - 12080z^4 - 11520z^3 + 6656z^2 + 12288z + 4096 \end{aligned}$$

is irreducible, has two roots with real part -1, and six real roots (and so of rational imaginary part) and two roots of modulus 2. Again $P \in \mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_3$.

Theorem 14 ($[\pm\frac{R}{2}, \frac{R}{2}, R]$)**.** *Let P be a polynomial of degree at least 3. Then $P \in \mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_3$, and is such that $c_1(P) = \pm\frac{1}{2}c_3(P)$ and $c_2(P) = \frac{1}{2}c_3(P)$ if and only if P is irreducible and $P(z)$ or $P(-z)$ is given by*

(15)
$$\begin{aligned} &(Rz/2)^{4n}(z-R)^{4n}(z^2+R^2)^{2n}(z^2-2Rz+2R^2)^{2n} \\ &\quad\times(2z^2-2Rz+R^2)^{2n}Q\left(s\left(\tfrac{1}{2}\left(2z/R-1+i\right)^2\right)\right)Q\left(s\left(\tfrac{1}{2}\left(2z/R-1-i\right)^2\right)\right) \end{aligned}$$

for some positive $R \in \mathbb{Q}$ and monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has a real root, where

$$s(w) = \frac{w^6 + 3w^5 + 33w^4 + 6w^3 - 33w^2 + 3w - 1}{w(w^2+1)^2}. \tag{16}$$

In this case, P has a root with rational modulus R.

Proof. Suppose first that $P \in \mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_3$, and is such that $c_1(P) = \pm\frac{1}{2}c_3(P)$ and $c_2(P) = \frac{1}{2}c_3(P)$. As above, we may suppose that $R = 1$ and that $c_1(P) = c_2(P) = \frac{1}{2}$. It is sufficient to prove that

$$P(z) = (z/2)^{4n}(z-1)^{4n}(z^2+1)^{2n}(z^2-2z+2)^{2n} \\ \times (2z^2-2z+1)^{2n} Q\left(s\left(\tfrac{1}{2}(2z-1+i)^2\right)\right) Q\left(s\left(\tfrac{1}{2}(2z-1-i)^2\right)\right)$$

for some monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has a real root. Suppose that $\alpha = \gamma + i/2$ and α' with real part equal to $\frac{1}{2}$ are roots of P. Applying Lemma 1 to a polynomial corresponding to the equation $\alpha' + \overline{\alpha'} = 1$ yields $\alpha + \alpha'' = 1$ for some conjugate α'' of α. Applying a $\mathbb{Q}$-embedding that maps α to α'' to the equation $\alpha = \gamma + i/2$ shows that one of $\alpha'' + i/2$ and $\alpha'' - i/2$ is a conjugate of γ. That is, either $1-\gamma$ or $1-\gamma-i$ is a conjugate of γ. However, as $1-\gamma \in \mathbb{R}$,

$$\deg_{\mathbb{Q}}(1-\gamma-i) = 2\deg_{\mathbb{Q}}(1-\gamma) = 2\deg_{\mathbb{Q}}(\gamma).$$

Consequently, $1-\gamma-i$ is not a conjugate of γ and so $1-\gamma$ is a conjugate of γ. We recall as well from the proof of Theorem 10 that the quantity $F(\gamma)$ where F is given by (4) is also a conjugate of γ. Therefore, for every conjugate γ' of γ, both $F(\gamma')$ and $1-\gamma'$ are conjugates of γ. We conclude that the group H given by Lemma 5 acts on the set S_γ of $\mathbb{Q}$-conjugates of γ. This gives us the 12 conjugates $\{h(\gamma)\}_{h\in H}$ of γ having sums of squares equal to

$$\beta := s((2\gamma-1)^2/2),$$

where s is given by (5):

$$s(w) = \frac{v(w)^3 + 3v(w)^2 + 36v(w) + 12}{v(w)^2+4}, \qquad v(w) = w - 1/w.$$

This works out to be the same as is given in (16). By H-invariance, the 12 members of the set $\{h(\gamma)\}_{h\in H}$ are the solutions to the equation $s((2z-1)^2/2) = \beta$. We now take Q to be the minimal polynomial of β. Since $\gamma = \alpha - i/2$, we see that α is a root of $Q(s((2z-i-1)^2/2))$. It is therefore also a root of the numerator of the rational function $Q(s((2z+i-1)^2/2))Q(s((2z-i-1)^2/2))$, which has rational coefficients. This numerator is given by the special case of the right-hand side of (15) that we are considering. On comparing degrees, we see that this polynomial is the minimal polynomial of α and therefore equal to P. Indeed, $\deg P = \deg_{\mathbb{Q}}(\alpha) = 2\deg_{\mathbb{Q}}(\gamma) = 2 \cdot 12 \deg_{\mathbb{Q}}(\beta) = 24n =$ the degree of the right-hand side of (15). Finally, since Q has β as a real root, the proof of this direction is complete.

Conversely, we will for simplicity assume, as above, that $R = 1$ and that the irreducible polynomial P is given by

$$P(z) = (z/2)^{4n}(z-1)^{4n}(z^2+1)^{2n}(z^2-2z+2)^{2n} \\ (2z^2-2z+1)^{2n}Q\left(s\left(\tfrac{1}{2}(2z-1+i)^2\right)\right)Q\left(s\left(\tfrac{1}{2}(2z-1-i)^2\right)\right)$$

for some monic irreducible polynomial $Q(z) \in \mathbb{Q}[z]$ of degree n that has a real root β. Studying the graph of $s((2z-1)^2/2)$ shows that the equation $s((2z-1)^2/2) = \beta$ always has a real root γ. The set of all roots is then given by $\{h(\gamma)\}_{h\in H}$. Now define $\alpha = \gamma + i/2$, so that α has imaginary part $\frac{1}{2}$. It is sufficient to show that α has a conjugate with real part equal to $\frac{1}{2}$ as well as a conjugate of modulus 1. Now $\alpha' := F(\gamma) + i/2$ is a conjugate of α having modulus 1, and so $1/\alpha' = \overline{\alpha'}$ is also a conjugate of α. Further, as $1-\gamma$ is a conjugate of γ, $1-\alpha$ is a conjugate of α. It follows that the set S_α of conjugates of α is closed under the maps $z \mapsto 1/z$ and $z \mapsto 1-z$. Composing these maps yields the conjugate $\alpha'' = (1/z)\circ(1-z)(\alpha') = 1/(1-\alpha')$ that has real part equal to $\frac{1}{2}$. The proof is therefore complete. □

Our final example illustrates Theorem 14.

Example 15 ($[\frac{1}{2}, \frac{1}{2}, 1]$)**.** *Let $Q(z) = z$, and so, using (15),*

$$\begin{aligned} P(z) = \frac{1}{16}(&16z^{24} - 192z^{23} + 1200z^{22} - 5104z^{21} + 16644z^{20} - 44472z^{19} \\ &+ 100856z^{18} - 197028z^{17} + 333669z^{16} - 492808z^{15} + 640944z^{14} \\ &- 743916z^{13} + 780398z^{12} - 743916z^{11} + 640944z^{10} - 492808z^9 \\ &+ 333669z^8 - 197028z^7 + 100856z^6 - 44472z^5 + 16644z^4 - 5104z^3 \\ &+ 1200z^2 - 192z + 16) \end{aligned}$$

has four roots with real part $\frac{1}{2}$, two roots with imaginary part $\frac{1}{2}$ and four roots of modulus 1*. It is irreducible. Again $P \in \mathcal{C}_1 \cap \mathcal{C}_2 \cap \mathcal{C}_3$.*

As in some of the cases in Sections 7 and 8, we cannot guarantee the irreducibility of the polynomials P given in Theorems 12, 13 and 14. It turns out that Examples 11 and 8, respectively, may also serve as examples for the first two cases.

In fact, the polynomial Q in Example 11 always has a positive zero as polynomial in z^2, and thus it has both a real positive and a real negative zero as a polynomial in z. It therefore satisfies the conditions of Theorem 12. Similarly, the polynomial Q in Example 8 has a real negative root, namely β, with the second root being its conjugate which has to be real and positive in this case. Hence Q satisfies the conditions of Theorem 13, which means that Example 8 is indeed an example of reducibility also in this case.

Finally, using $Q(z) = z - k$ in Theorem 14 (where the case $k = 0$ is dealt with in Example 15), a calculation with Maple for k in the range $-10\,000 \le k \le 10\,000$ shows that P is reducible only for $k = -7$, 3 and 13.

References

[1] N. M. Berry, On relationships between conjugate algebraic numbers, Ph.D. thesis, Univ. of Edinburgh, Edinburgh, 2003.

[2] A. Dubickas and C. J. Smyth, Problem 11123 and solution (by R. Stong), Amer. Math. Monthly **113** (2006), 941–942.

[3] V. Ennola, Conjugate algebraic integers on a circle with irrational center. Math. Z. **134** (1973), 337–350.

[4] V. Ennola and C. J. Smyth, Conjugate algebraic numbers on a circle. Ann. Acad. Sci. Fenn. Ser. A I, No. 582 (1974), 31 pp.

[5] V. Ennola and C. J. Smyth, Conjugate algebraic numbers on circles. Acta Arith. **29** (1976), 147–157.

[6] Maple, `http://www.maplesoft.com/`.

[7] J. McKee, Conjugate algebraic numbers on conics: a survey. Number theory and polynomials, 211–240, London Math. Soc. Lecture Note Ser., 352, Cambridge Univ. Press, Cambridge, 2008.

[8] M. Newman, *Integral Matrices*, Academic Press, New York, 1972.

[9] R. M. Robinson, Conjugate algebraic integers on a circle, Math. Z. **110** (1969), 41–51.

[10] A. Schinzel, Polynomials with special regard to reducibility. Cambridge University Press, Cambridge, 2000.

[11] C. J. Smyth, Conjugate algebraic numbers on conics. Acta Arith. **40** (1981/82), 333–346.

[12] L. C. Washington, *Elliptic curves. Number theory and cryptography.* Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2003.

Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 3J5, Canada

E-mail address: `dilcher@mathstat.dal.ca`

Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 3J5, Canada

E-mail address: `rnoble@mathstat.dal.ca`

School of Mathematics and Maxwell Institute for Mathematical Sciences, University of Edinburgh, Edinburgh, EH9 3JZ, UK

E-mail address: `c.smyth@ed.ac.uk`