ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

582

CONJUGATE ALGEBRAIC NUMBERS ON A CIRCLE

BY

VEIKKO ENNOLA and C. J. SMYTH

HELSINKI 1974
SUOMALAINEN TIEDEAKATEMIA

doi:10.5186/aasfm.1975.582

ISSN 0066-1953
ISBN 951-41-0191-X

Communicated 11 March 1974

KESKUSKIRJAPAINO
HELSINKI 1974

1. Introduction

In this paper we are concerned with algebraic numbers all of whose conjugates lie on a circle whose centre γ is a cubic or quartic non-totally real irrational.

We show that there is at most one circle of centre γ which contains a set of conjugate algebraic numbers $\beta = \beta_1, \ldots, \beta_N$ with $N \geqq 3$. Further, when such a circle does exist, we obtain a one-to-one correspondence between sets of conjugate algebraic numbers on the circle, and totally real algebraic numbers whose conjugates lie in a certain interval (Theorem 1). We also obtain necessary and sufficient conditions for infinitely many of these numbers on the circle to be algebraic integers (Theorem 2).

Our paper extends work of Robinson [3] and the first author [1]. Robinson proved a theorem corresponding to our Theorem 2 for circles of rational centre. At the end of the paper we give an explicit result (implicit in Robinson's work) corresponding to our Theorem 1 for this case (Theorem 3). We also give an alternative proof of Robinson's theorem (Theorem 4); our proof gives an idea of the methods used in the proof of Theorem 2. In [1, Theorems 1 and 3], the first author has given the corresponding results for the case of circles whose centre is irrational and totally real.

Our main results are stated in Section 2. Section 3 is devoted to lemmas concerning the general problem, when γ is of degree n (not necessarily 3 or 4), and non-totally real. We then specialize to $n = 3$ or 4, and prove some more lemmas which we require (Section 4). In Section 5 we construct conjugate sets of algebraic numbers on a circle of centre γ; the proof of Theorem 1 is completed in Section 6. The proof of Theorem 2 occupies the next three sections. In Section 10 we have the discussion for circles of rational centre. We also make a few comments on [1]. Finally we give some examples in Section 11.

We denote by $\mathbf{A}$ the ring of all algebraic integers. As usual, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{C}$ denote the integers, the rationals, and complex numbers, respectively. For $z \in \mathbf{C}$, we fix $\sqrt{z}$ so that $0 \leqq \arg \sqrt{z} < \pi$. If p is prime, then $p^{\varkappa} \| C$ indicates that $p^{\varkappa} | C, p^{\varkappa+1} \nmid C$. If $C = 0$, we put $\varkappa = \infty$.

2. Statement of main results

Except in Section 10, γ will denote a real, but not totally real algebraic number of degree n, with conjugates $\gamma = \gamma_1, \dots, \gamma_n$, and minimal polynomial

$$g(z) = z^n - s_1 z^{n-1} + s_2 z^{n-2} - \dots + (-1)^n s_n \tag{1}$$

over **Q**. We always take γ_2 to be non-real, and $\gamma_3 = \bar{\gamma}_2$. Thus for $n = 4$, γ_4 is real.

For $n = 3,4$ we define

$$d = \begin{cases} s_1^2 - 3\, s_2 & \text{if } n = 3\,, \\ s_1^2 - \frac{8}{3}\, s_2 & \text{if } n = 4\,; \end{cases} \tag{2}$$

and, for $d \neq 0$,

$$b = \begin{cases} (s_2^2 - 3\, s_1 s_3)/d & \text{if } n = 3\,, \\ (\frac{4}{9}\, s_2^2 - s_1 s_3)/d & \text{if } n = 4\,; \end{cases} \tag{3}$$

$$c = \begin{cases} (9\, s_3 - s_1 s_2)/d & \text{if } n = 3\,, \\ (4\, s_3 - \frac{2}{3}\, s_1 s_2)/d & \text{if } n = 4\,. \end{cases} \tag{4}$$

The geometric significance of b and c will be seen from Lemma 4. The meaning of d is fixed throughout the paper, whereas the explicit values for b and c will not be used in Sections 3 and 4, in which b, c will denote arbitrary rationals.

With the fixed values (3), (4) for b and c, we define, for $d \neq 0$,

$$\Omega^* = b + c\gamma + \gamma^2\,,$$

and, for $d > 0$, the closed interval Δ by

$$\Delta = [2(s_1 - \sqrt{d})\,,\, 2(s_1 + \sqrt{d})]\,.$$

Next, we define polynomials $U(z)$, $V(z)$ as follows:

$$V(z) = \begin{cases} g(z)\,(z^2 + cz + \frac{1}{3}\,(c^2 - b)) & \text{if } n = 3\,, \\ g(z)\,(z^2 + cz + \frac{1}{2}\,c^2 - b)\,(z + \frac{1}{2}\,c) & \text{if } n = 4\,; \end{cases} \tag{5}$$

$$U(z) = (z^2 + cz + b)^n - nc\,V(z) \quad (n = 3\,,\,4). \tag{6}$$

Theorem 1. *Let γ be real, but not totally real, of degree $n = 3$ or 4 over* **Q**.

Suppose that there exists a positive real number Ω such that the circle $|z - \gamma|^2 = \Omega$ contains a set of conjugate algebraic numbers with at least three members. Then

$$\Omega = \Omega^*, \quad d > 0\,, \tag{7}$$

and, in the case $n = 4$

$$27\, ds_4 = 9\, s_1 s_2 s_3 - 2\, s_2^3 - 27\, s_3^2\,, \tag{8}$$

$$|\gamma - \gamma_2| > |\gamma_4 - \gamma_2|\,\cdot \tag{9}$$

Conversely, suppose that $d > 0$, *and that* (8), (9) *hold if* $n = 4$. *Let* α *be a totally real algebraic number, all of whose conjugates* α_i *lie in* Δ. *Take*

$$l = \begin{cases} 2 & \textit{if } \alpha \textit{ is an endpoint of } \Delta\,, \\ 1 & \textit{otherwise}\,. \end{cases}$$

Then the condition

$$P(z)^l = \prod_i \left(U(z) - \alpha_i V(z)\right) \tag{10}$$

defines a monic polynomial $P(z) \in \mathbf{Q}[z]$, *which is irreducible over* $\mathbf{Q}$, *and has all its zeros on* $|z - \gamma|^2 = \Omega^*$. *Furthermore, the minimal polynomial of any algebraic number, all of whose conjugates lie on* $|z - \gamma|^2 = \Omega^*$, *must be of the form* $P(z)$, *defined by* (10), *for some totally real* α *having all its conjugates in* Δ.

Condition (8) in the theorem expresses the fact that for $n = 4$, γ and its conjugates lie on a circle (trivially true, of course, for $n = 3$). The condition $d > 0$ for $n = 3$, and condition (9) for $n = 4$, state that γ and the centre of gravity of the γ_i lie on opposite sides of the centre of this circle. The condition $d > 0$ for $n = 4$ is, in fact, a consequence of (8), as is easily seen from (44).

The restriction to sets of conjugates with at least three members is not a serious one, as a simple argument shows that any circle containing more than one set of conjugate quadratic irrationals must have rational centre.

Lemma 11 gives some more information concerning the quartic case. At the end of Section 6 there are also some further remarks regarding the case when α is an endpoint of Δ.

For the statement of Theorem 2, we need the following additional notation:

$$s_1 = S/q\,, \quad s_2 = \begin{cases} T/q & \text{if } n = 3\,, \\ 3\,T/q & \text{if } n = 4\,, \end{cases} \quad c = C/r\,.$$

where $q, r, S, T, C, \in \mathbf{Z}$; $q\,, r > 0$; and $(S\,, T\,, q) = (C\,, r) = 1$. Note that $q^2 d$ is an integer. We define, for $n = 3$, $E = 3\,qC^2 + rSC + r^2T$ and

$$\varkappa = \begin{cases} 2 & \text{if } 3 \nmid qr\,,\ 3^1 \| E\,,\ 3 \nmid S\,, \\ 1 & \text{if } 3 \nmid qr\,,\ 3^1 \| E\,,\ 3 \mid S\,, \\ 0 & \text{otherwise}\,; \end{cases} \qquad \lambda = \begin{cases} 2 & \text{if } 3 \mid q\,,\ 3\,q \nmid E, \\ 1 & \text{if } 3 \mid q\,,\ 3q \mid E\,,\ 9\,q \nmid E\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

For $n = 4$ put

$$\varkappa = \begin{cases} 1 & \text{if } 2^1 \| S , 2 \nmid C , \\ 0 & \text{otherwise ;} \end{cases} \qquad \lambda = \begin{cases} 1 & \text{if } 4 | S , 2 \nmid C , \\ 0 & \text{otherwise .} \end{cases}$$

Theorem 2. *Let* γ *be a real, but not totally real, algebraic number of degree* $n = 3$ *or* 4, *which satisfies* $d > 0$, *and, if* $n = 4$, (8) *and* (9).

Suppose that there is at least one set of conjugate algebraic integers on the circle $|z - \gamma|^2 = \Omega^*$. *Then*

$$(q , r) = 1 , \tag{11}$$

$$(3 , q) \, rb \in \mathbf{Z} \quad \textit{and} \quad (3 , r)^2 r^4 \mid q^2 d \quad \textit{for} \quad n = 3 . \tag{12.3}$$

$$r \, b \in \mathbf{Z} \quad \textit{and} \quad 2^{4\lambda} r^6 \mid q^2 d \quad \textit{for} \quad n = 4 . \tag{12.4}$$

Conversely, if (11) *and* (12 . n) *are satisfied, then there are infinitely many sets of conjugate algebraic integers on* $|z - \gamma|^2 = \Omega^*$ *if and only if*

$$d \geqq \begin{cases} 3^{2\varkappa + 4\lambda} (3 , r)^2 q^2 r^4 & \textit{for} \quad n = 3 , \\ 2^{6\varkappa + 4\lambda} q^2 r^6 & \textit{for} \quad n = 4 . \end{cases} \tag{13}$$

For $n = 4$ equality cannot, in fact, hold in (13), because, as we shall see in Lemma 11, d cannot be a square in **Q**. For $n = 3$ we shall give an example in Section 11 to show that equality can occur in this case.

We shall prove Theorem 2 by showing that there is a one-to-one correspondence between sets of conjugate algebraic integers on $|z - \gamma|^2 = \Omega^*$ and those in a certain real interval obtained from Δ by translation and contraction. If equality holds in (13), then this interval has critical length 4. In our case, however, the interval will then have integral endpoints. Therefore we also obtain infinitely many sets of conjugate algebraic integers on the circle in the case of equality, and we can even write them down explicitly. (Cf. [2].)

The proof of Theorem 2 is unfortunately rather complicated. This is caused in part by the ancmalous behaviour of the primes 3, 2 for $n = 3, \ 4$ respectively.

It might be of interest to have a simpler, but slightly weaker form of Theorem 2 (using also the results of Theorem 1), which we state as follows:

Corollary. *Let* γ *be real, not totally real, of degree* $n = 3$ *or* 4. *Then there is a circle with centre* γ *containing infinitely many sets of conjugate algebraic integers if and only if* (11), (12 . n), (13) *hold, and also, if* $n = 4$, (8) *and* (9) *hold.*

3. General lemmas

For any non-zero complex numbers $\Omega_1 = \Omega, \Omega_2, \ldots, \Omega_n$ we define linear transformations $\Gamma_j : \mathbf{C} \cup \{\infty\} \to \mathbf{C} \cup \{\infty\}$ by

$$(14) \qquad (\Gamma_j z - \gamma_j)(z - \gamma_j) = \Omega_j \quad (j = 1, \ldots, n)$$

or, equivalently,

$$(15) \qquad \Gamma_j z = \frac{\gamma_j z + \Omega_j - \gamma_j^2}{z - \gamma_j}.$$

Put $\Gamma = \Gamma_1$. Note that $\Gamma_j^2 = 1$ $(j = 1, \ldots, n)$. The fixed points of Γ_j are $\gamma_j \pm \Omega_j^{1/2}$. Let $\mathfrak{H}$ denote the group generated by $\Gamma_1, \ldots, \Gamma_n$.

If Ω is real and positive, we let $\mathcal{S}$ denote the circle $|z - \gamma|^2 = \Omega$. We have $\Gamma z = \bar{z}$ if and only if $z \in \mathcal{S}$. In particular, $\Gamma\mathcal{S} = \mathcal{S}$.

Lemma 1. *If Ω is real, then for each $j = 2, \ldots, n$, the following three conditions are equivalent:*

(i) $\Omega_j = (\gamma - \gamma_j)^2 - \Omega(\gamma - \gamma_j)/(\gamma - \bar{\gamma}_j)$,

(ii) $\Gamma_j \gamma = \Gamma \bar{\gamma}_j$,

(iii) $\Gamma_j \Gamma = \Gamma \bar{\Gamma}_j$.

If, in addition, Ω is positive, then these conditions are further equivalent to

(iv) $\Gamma_j \mathcal{S} = \mathcal{S}$.

Proof. (i) $\Leftrightarrow$ (ii). Straightforward computation.

(ii) $\Rightarrow$ (iii). We have $\Gamma_j \Gamma \infty = \Gamma \bar{\Gamma}_j \infty$. Also $\Gamma \Gamma_j \Gamma \gamma = \Gamma \Gamma_j \infty = \Gamma \gamma_j = \bar{\Gamma}_j \gamma$, so $\Gamma_j \Gamma \gamma = \Gamma \bar{\Gamma}_j \gamma$. Similarly $\Gamma_j \Gamma \bar{\gamma}_j = \Gamma \bar{\Gamma}_j \bar{\gamma}_j$. Since two linear transformations are identical if they are equal for more than two values of z, the result follows.

(iii) $\Rightarrow$ (ii). Trivial by looking at the images of ∞.

(iii) $\Leftrightarrow$ (iv) for $\Omega > 0$. If $z \in \mathcal{S}$, we have $\Gamma_j z \in \mathcal{S} \Leftrightarrow \overline{\Gamma_j z} = \Gamma(\Gamma_j z) \Leftrightarrow \bar{\Gamma}_j \Gamma z = \Gamma \Gamma_j z$, and the result follows by the above remark.

Supposing that $\Omega > 0$, we let β be an algebraic number of degree $N \geqq 3$, and assume for the moment that all the conjugates β_i of β lie on $\mathcal{S}$. Proceeding in a similar manner to [1], we then note that by an easy geometric argument we can express γ and Ω in terms of the β_i. Hence, defining $\mathfrak{K}$ to be the field obtained by adjoining the conjugates of γ and Ω to $\mathbf{Q}$, and $\mathfrak{N} = \mathbf{Q}(\beta_1, \ldots, \beta_N)$, we have $\mathfrak{K} \subseteq \mathfrak{N}$. Let $\mathfrak{G} = \mathrm{Gal}(\mathfrak{K}/\mathbf{Q})$ and $\mathfrak{G}_\beta = \mathrm{Gal}(\mathfrak{N}/\mathbf{Q})$. For $j = 2, \ldots, n$, we pick an element $\sigma_j \in \mathfrak{G}_\beta$ such that $\sigma_j \gamma = \gamma_j$, and put $\sigma_1 = 1$. We then fix $\Omega_j = \sigma_j \Omega$ $(j = 1, \ldots, n)$.

From the fact that

$$(16)\qquad \Gamma\beta_k = \bar{\beta}_k \quad (k = 1, \dots, N)$$

we obtain, by applying σ_j,

$$(17)\qquad \Gamma_j\beta_i = \beta_m \quad (i = 1, \dots, N\,; j = 1, \dots, n)$$

for some m depending on i and j. Hence Γ_j permutes the conjugates of β. But $\Gamma_j S$ is either a circle or a straight line, and has at least three points in common with S, namely the β_i. So $\Gamma_j S = S$. More generally, A permutes the conjugates of β, and $AS = S$, for each $A \in \mathfrak{H}$.

From Lemma 1 (i), we see that Ω_j is independent of the choice of the automorphism σ_j satisfying $\sigma_j\gamma = \gamma_j$. However, a simple argument (given in the case of γ irrational and totally real in [1, Section 2]) shows that this is not the case if $\Omega \notin \mathbf{Q}(\gamma)$. Hence $\Omega \in \mathbf{Q}(\gamma)$.

Lemma 2. *Let* $\beta_i \in S$ $(i = 1, \dots, N)$, *where* β *is as above. Define* $\varkappa \in \mathfrak{G}_\beta$ *by* $z \mapsto \bar{z}$. *Then there is a monomorphism* $\psi : \mathfrak{H} \to \mathfrak{G}_\beta$ *satisfying* $\psi(\Gamma_j) = \sigma_j\varkappa\sigma_j^{-1}$. *In particular,* $\mathfrak{H}$ *is a finite group.*

Proof. Let $\mathfrak{S}_N$ be the symmetric group on $\beta_1, \dots, \beta_N$, and let ψ_1: $\mathfrak{G}_\beta \to \mathfrak{S}_N$ denote the obvious monomorphism. Since $N \geqq 3$, the natural mapping $\psi_2 : \mathfrak{H} \to \mathfrak{S}_N$ is also a monomorphism. By (16) and (17), we have $\Gamma_j\beta_i = \sigma_j\varkappa\sigma_j^{-1}\beta_i$. It follows that $\mathrm{Im}(\psi_2) \subseteq \mathrm{Im}(\psi_1)$, and we can define ψ by $\psi_1\psi = \psi_2$.

Using the canonical projection $\mathfrak{G}_\beta \to \mathfrak{G}$ we can also define a homomorphism from $\mathfrak{H}$ to $\mathfrak{G}$. However, this map is not, in general, either injective or surjective.

We now drop the assumption that S contains β and its conjugates. From now on, except in Section 10, we shall always take $\Omega \in \mathbf{Q}(\gamma)$. Note that we do not necessarily suppose that $\Omega > 0$, unless we expressly say so. As before, we put $\mathfrak{K} = \mathbf{Q}(\gamma_1, \dots, \gamma_n)$ and $\mathfrak{G} = \mathrm{Gal}(\mathfrak{K}/\mathbf{Q})$. We define $\Omega_j = \sigma_j'\Omega$, where $\sigma_j' \in \mathfrak{G}$ maps γ to γ_j. Now if $\Omega > 0$ and β and its conjugates do lie on S, this definition of Ω_j is the same as the previous one, and furthermore we have shown that then

$$(18)\qquad \Omega \in \mathbf{Q}(\gamma) \text{ and } \Omega_j = (\gamma - \gamma_j)^2 - \Omega(\gamma - \gamma_j)/(\gamma - \bar{\gamma}_j) \ (j = 2, \dots, n)\,.$$

Of course the condition on Ω_j in (18) could be replaced by either one of the conditions (ii), (iii) of Lemma 1.

We shall eventually show that, for $n = 3, 4$, the truth of (18) for $\Omega > 0$ is also sufficient for the existence of a set of conjugate algebraic numbers on S.

Lemma 3. *If* Ω *is of the form* $\Omega = b + c\gamma + \gamma^2$ *for some* $b, c \in \mathbf{Q}$ (*cf. Lemma* 4), *then*

$$(19) \qquad \Gamma_i \Gamma_j z = \frac{z \Gamma_i \gamma_j - b}{z - \Gamma_j \gamma_i} \quad (i, j = 1, \ldots, n\,;\ i \neq j)\,,$$

and condition (i) *of Lemma* 1 *takes the form*

$$(20) \qquad b(2\gamma - \gamma_j - \bar{\gamma}_j) + c(\gamma^2 - \gamma_j \bar{\gamma}_j) + \gamma^2(\gamma_j + \bar{\gamma}_j) - 2\gamma \gamma_j \bar{\gamma}_j = 0\,.$$

Proof. Direct calculation in both cases.

Lemma 4. *Suppose that* $\Omega > 0$ *satisfies* (18), *and that the products* $\Gamma_j \Gamma (j = 1, \ldots, n)$ *generate a finite cyclic subgroup* $\mathfrak{H}_0$ *of* $\mathfrak{H}$. *Then the following results hold:*

(i) *There exist rational numbers* b, c *such that* $\Omega = b + c\gamma + \gamma^2$.

(ii) *The roots* ϱ_1, ϱ_2 *of the equation* $x^2 + cx + b = 0$ *are real and unequal, and are inverse with respect to the circle* S.

(iii) *For any* $A \in \mathfrak{H}$, *we have* $A \in \mathfrak{H}_0$ *if and only if* $A \varrho_j = \varrho_j$ $(j = 1, 2)$.

(iv) *For each* $j = 1, \ldots, n$, γ_j *lies on the circle*

$$(21) \qquad |z - (\gamma^2 - b)/(2\gamma + c)| = \Omega/|2\gamma + c|$$

which lies inside S.

(v) *The fixed points of* Γ_j *lie on* S $(j = 1, \ldots, n)$.

Proof. Now $\Gamma_j \Gamma_k = \Gamma_j \Gamma (\Gamma_k \Gamma)^{-1} \in \mathfrak{H}_0$, for each j and k, so $\mathfrak{H}_0$ has index 2 in $\mathfrak{H}$. Since $\mathfrak{H}$ is finite, every element $A \neq 1$ of $\mathfrak{H}$ is elliptic, so that the two fixed points of A are distinct. (See e.g. [4, Chapter 9] for elementary results concerning linear transformations.) Since $\mathfrak{H}_0$ is cyclic, all the elements $\neq 1$ in $\mathfrak{H}_0$ have the same two fixed points, ϱ_1 and ϱ_2, say. So for any $j, k = 1, \ldots, n$ and $m = 1, 2$, we have $\Gamma_j \Gamma_k \varrho_m = \varrho_m$. Clearly ϱ_1 and ϱ_2 are algebraic numbers. We now apply all the automorphisms of a suitable normal extension of $\mathfrak{K}$, containing ϱ_1 and ϱ_2, to this equation. Then we see that such automorphisms permute ϱ_1 and ϱ_2. Hence, putting $c = -\varrho_1 - \varrho_2$, $b = \varrho_1 \varrho_2$, we obtain $c, b \in \mathbf{Q}$.

From the elementary theory, we know that the fixed points of an elliptic linear transformation, which keeps a circle invariant, must either be inverse with respect to the circle, or actually lie on the circle. In the latter case the transformation is necessarily an involution. But $\mathfrak{H}_0$ contains the element $\Gamma_2 \Gamma$, which is not an involution, by Lemma 1 (iii). Thus (ii) follows. Since ϱ_1 and ϱ_2 are inverse with respect to S, we have $\Omega = (\varrho_1 - \gamma)(\varrho_2 - \gamma)$, and (i) follows.

The line Re $z = -\frac{1}{2}c$ is the right bisector of the line joining ϱ_1 and ϱ_2, so that it belongs, together with S, to the elliptic pencil of circles with limiting points ϱ_1 and ϱ_2. Thus this line lies outside S, and is carried into itself by every element of $\mathfrak{H}_0$. (See [4;9.4.3].) Therefore the image of this line under any transformation Γ_j is the same. Since $\Gamma\infty = \gamma$, this image must be a circle S', say, lying inside S. Now $\Gamma_j\infty = \gamma_j \in S'$, whence (20) shows that S' has the equation

$$b(2\gamma - z - \bar{z}) + c(\gamma^2 - z\bar{z}) + \gamma^2(z + \bar{z}) - 2\gamma z\bar{z} = 0\,,$$

which gives (21). This proves (iv).

We also find that each Γ_j interchanges the two regions whose boundary is S. Hence (iii) and (v) are true.

Lemma 5. *Suppose that* (18) *holds, and that* γ_i *is non-real. Let* $\sigma \in \mathfrak{G}$ *be such that* $\sigma\gamma = \gamma_i$. *Put* $\gamma_k = \sigma(\overline{\sigma^{-1}\gamma})$, *and* $\eta_j = (\gamma - \gamma_j)^{-1}$ $(j = 2\,, \ldots, n)$. *Then* $\gamma_k \neq \gamma$, *and*

$$\Omega^{-1} = \eta_i\bar{\eta}_k + \bar{\eta}_i\eta_k - \eta_i\bar{\eta}_i\,, \tag{22}$$

$$\eta_i + \bar{\eta}_i = \eta_k + \bar{\eta}_k\,. \tag{23}$$

Proof. Let $\gamma_m = \sigma^{-1}\gamma$. Then applying σ to (18) with $j = m$, and substituting for Ω_i (again using (18)), we obtain $\gamma_k \neq \gamma$ and

$$\Omega^{-1} = \eta_i^2 - \eta_i\eta_k + \bar{\eta}_i\eta_k\,. \tag{24}$$

Now $\Omega^{-1} = \bar{\Omega}^{-1}$ gives (23), as $\eta_i \neq \bar{\eta}_i$. Hence replacing η_i^2 by $\eta_i(\eta_k + \bar{\eta}_k - \bar{\eta}_i)$ in (24), we get (22).

4. Cubic and quartic lemmas

We now assume that γ has degree $n = 3$ or 4. We recall that $\gamma_3 = \bar{\gamma}_2$, and that γ_4 is real in the case $n = 4$.

Lemma 6. *Suppose that* (18) *holds. Then for* $n = 3\,, 4$, *both* $\mathfrak{G}$ *and* $\mathfrak{H}$ *are isomorphic to the dihedral group* $\mathfrak{D}_{2n}$ *of order* $2n$.

Proof. We regard $\mathfrak{G}$ as a permutation group on the symbols $1\,, \ldots, n$. From Lemma 1 (iii) we have

$$\Gamma_2\Gamma = \Gamma\Gamma_3\,,\quad \Gamma_3\Gamma = \Gamma\Gamma_2 \tag{25}$$

and for $n = 4$

$$\Gamma_4\Gamma = \Gamma\Gamma_4\,. \tag{26}$$

Put $\Lambda_0 = \Gamma_2\Gamma$. From (25) we obtain

$$\Lambda_0^{-1} = \Gamma_3\Gamma\,,\quad \Lambda_0^2 = \Gamma_2\Gamma_3\,,\quad \Gamma\Lambda_0 = \Lambda_0^{-1}\Gamma\,. \tag{27}$$

To prove that $\mathfrak{H} \cong \mathfrak{D}_{2n}$, it is therefore enough to show that Λ_0 is of order n, and that $\mathfrak{H}$ is generated by Λ_0 and Γ.

(a) $n = 3$. The result for $\mathfrak{G}$ is trivial. Applying the permutation (123) to (25), we obtain $\Lambda_0 = \Gamma_3\Gamma_2$, so that $\Lambda_0^3 = 1$ by (27). The rest is clear.

(b) $n = 4$. Let $\sigma \in \mathfrak{G}$ map 1 onto 4. Applying σ to (25), we see, by (26), that σ cannot map 2 or 3 onto 1. Hence $\sigma = (14)$ or $(14)(23)$, and Γ_4 does not commute with Γ_2 or Γ_3.

Next let $\sigma 1 = 2$. Applying σ to (26), we find that $\sigma 4 = 3$, because Γ_2 does not commute with Γ or Γ_4. We also find that Γ_2 and Γ_3 do commute, whence Λ_0 is of order 4 by (27). Clearly $\sigma = (12)(34)$ or (1243). Applying σ to (25), we obtain $\Lambda_0 = \Gamma_4\Gamma_2$ in both cases. It is now easily seen that $\mathfrak{H}$ is generated by Λ_0 and Γ, whence the result for $\mathfrak{H}$ follows.

If $\sigma 1 = 3$, a similar argument shows that $\sigma = (13)(24)$ or (1342). Finally, if $\sigma 1 = 1$, then σ must be (1) or (23), by (25) and (26).

Now $\mathfrak{G}$ has more than four elements, as γ is not totally real, so it must consist precisely of the eight permutations mentioned in the proof:

$$\mathfrak{G} = \{(1)\,,(14)\,,(23)\,,(12)(34)\,,(13)(24)\,,(14)(23)\,,(1243)\,,(1342)\} \tag{28}$$

This completes the proof of Lemma 6.

If there is a positive Ω satisfying (18), then from the structure of $\mathfrak{H}$ we see that the $\Gamma_j\Gamma$ belong to the cyclic subgroup generated by Λ_0, and so the results of Lemma 4 hold.

Lemma 7. *Suppose that* $\Omega > 0$ *satisfies* (18). *Let* $\varphi = \Gamma_2\gamma$. *Then* $\varphi, \bar{\varphi}$ *are the roots of the equation*

$$z^2 + cz + \tfrac{1}{3}(c^2 - b) = 0 \quad \textit{if} \quad n = 3\,, \tag{29.3}$$

$$z^2 + cz + \tfrac{1}{2}c^2 - b = 0 \quad \textit{if} \quad n = 4\,, \tag{29.4}$$

where $b\,,c$ *are as in Lemma* 4. *Furthermore, for* $n = 4$

$$\Gamma_4\gamma = \Gamma\gamma_4 = -\tfrac{1}{2}c\,. \tag{30}$$

Proof. From the proof of Lemma 4, we know that $\mathrm{Re}\ \Gamma_j\gamma_k = -\frac{1}{2}c$ for $j \neq k$. Thus $\varphi + \bar{\varphi} = -c$. By Lemma 1 (ii), we now have (30) and also

$$\varphi = \Gamma_2\gamma = \Gamma\gamma_3\,,\ \bar{\varphi} = \Gamma_3\gamma = \Gamma\gamma_2\,. \tag{31}$$

Before proceeding further, we call attention to the following general principle. Consider any valid relation in $\mathfrak{H}$, say of the form $\Gamma_i\Gamma_k = \Gamma_j\Gamma_l$. Looking at the images of ∞, we find $\Gamma_i\gamma_k = \Gamma_j\gamma_l$.

Using this principle and the structure of $\mathfrak{H}$ determined above, one can easily verify that the set $\{\Gamma_j\gamma_k | j = 1\,,\ldots,n;\ j \neq k\} = \{\varphi\,,\bar{\varphi}\}$ for $n = 3$, $= \{\varphi\,,\bar{\varphi}\,,-\frac{1}{2}c\}$ for $n = 4$.

Now for $n = 3$, we use the relation $(\Gamma_2\Gamma)^2 = \Gamma_3\Gamma$, which by (31) gives $\Gamma_2\Gamma\varphi = \bar{\varphi}$. From Lemma 3 and (31) we have $\bar{\varphi} = (\varphi^2 - b)/(\varphi - \bar{\varphi})$, and thus $3\,\varphi\bar{\varphi} = (\varphi + \bar{\varphi})^2 - b = c^2 - b$. Hence (29.3) holds.

For $n = 4$, we found in the proof of Lemma 6 that $\Gamma_2\Gamma = \Gamma_4\Gamma_2$. Hence $(\Gamma_2\Gamma)^2 = \Gamma_4\Gamma$. This relation gives $\Gamma_2\Gamma\varphi = -\frac{1}{2}c$ by (30), so using Lemma 3 and (31) again, $-\frac{1}{2}c = (\varphi^2 - b)/(\varphi - \bar{\varphi})$. It follows that φ satisfies (29.4). This completes the proof.

As an immediate consequence of (29. n) we have the following fact:

$$-(\varphi - \bar{\varphi})^2 = \begin{cases} \frac{1}{3}(c^2 - 4b) & \text{for } n = 3\,, \\ c^2 - 4b & \text{for } n = 4\,. \end{cases} \tag{32}$$

Lemma 8. *Suppose that* (18) *holds. Then*

$$\Omega = (\gamma - \gamma_2)^2(\gamma - \gamma_3)^2/d \qquad \textit{for} \quad n = 3\,, \tag{33}$$

$$\Omega = (\gamma - \gamma_2)(\gamma - \gamma_3)(\gamma - \gamma_4)/(\gamma + \gamma_4 - \gamma_2 - \gamma_3) \qquad \textit{for} \quad n = 4\,, \tag{34}$$

$$(\gamma + \gamma_4)(\gamma_2 + \gamma_3) = 2(\gamma\gamma_4 + \gamma_2\gamma_3) = \tfrac{2}{3}s_2 \qquad \textit{for} \quad n = 4\,. \tag{35}$$

Proof. Take $i = 2$ in Lemma 5. For $n = 3$, let σ be the transposition (12). Then $k = 3$, and (33) follows from (22). For $n = 4$, take $\sigma = (12)(34)$. Then $k = 4$, so that (34) and the first part of (35) follow from (22) and (23). A short calculation now shows that the second part of (35) is true.

Lemma 9. *For* $n = 3$ *there is an* $\Omega > 0$ *satisfying* (18) *if and only if* $d > 0$. *Furthermore, then* $\Omega = \Omega^*$.

Proof. By Lemma 4, such an Ω is necessarily of the form $\Omega = b + c\gamma + \gamma^2$ for some $b, c \in \mathbf{Q}$. By Lemma 3, we have to look for $b, c \in \mathbf{Q}$ such that $b + c\gamma + \gamma^2 > 0$ and (20) holds for $j = 2$. Substitute $\gamma\gamma_2\gamma_3 = s_3$, $\gamma_2 + \gamma_3 = s_1 - \gamma$, $\gamma_2\gamma_3 = s_2 - s_1\gamma - \gamma^2$, followed by $\gamma^3 = s_1\gamma^2 - s_2\gamma + s_3$ in this equation. This gives

$$-(s_1b + s_2c + 3s_3) + \gamma(3b + s_1c + s_2) = 0\,,$$

which is equivalent to

$$\begin{cases} s_1b + s_2c + 3s_3 = 0\,, \\ 3b + s_1c + s_2 \quad = 0\,. \end{cases} \tag{36}$$

If now $\Omega > 0$ satisfies (18), then $d > 0$ by (33). The equations (36) have the unique solution b, c given by (3), (4) (for $n = 3$). Thus $\Omega = \Omega^*$. Conversely, if $d > 0$, then we can solve the equations (36) for b, c. Hence we obtain an Ω satisfying (18), and this Ω is positive by (33).

Lemma 10. *For* $n = 4$ *there is an* $\Omega > 0$ *satisfying* (18) *if and only if* (8), (9) *hold, and* $d > 0$. *Furthermore, then* $\Omega = \Omega^*$.

Proof. Assume that $\Omega > 0$ satisfies (18). As before, $\Omega = b + c\gamma + \gamma^2$ for $b, c \in \mathbf{Q}$. From (20) for $j = 4$, we have

$$b + \tfrac{1}{2}c(\gamma + \gamma_4) + \gamma\gamma_4 = 0\,. \tag{37}$$

By (28) we can apply the permutation (1243) to (37), and get

$$b + \tfrac{1}{2}c(\gamma_2 + \gamma_3) + \gamma_2\gamma_3 = 0 \,. \tag{38}$$

From (34), $\gamma + \gamma_4 \neq \gamma_2 + \gamma_3$, so that, by (35), $\gamma + \gamma_4$ and $\gamma_2 + \gamma_3$ are the two roots of the equation $x^2 - s_1 x + \frac{2}{3}s_2 = 0$. Therefore

$$\gamma + \gamma_4 = \tfrac{1}{2}(s_1 + \varepsilon\sqrt{d}) \,, \quad \gamma_2 + \gamma_3 = \tfrac{1}{2}(s_1 - \varepsilon\sqrt{d}) \,, \tag{39}$$

where $\varepsilon = \pm 1$. As γ, γ_4 are real, $d > 0$. Also we cannot have $\gamma + \gamma_4 \in \mathbf{Q}$, for otherwise $\gamma\gamma_4 \in \mathbf{Q}$ by (37), and γ would not be of degree 4. Therefore d is not a square in $\mathbf{Q}$. From (37), (38), (35) we have first

$$2b + \tfrac{1}{2}cs_1 + \tfrac{1}{3}s_2 = 0 \,, \tag{40}$$

and then

$$\gamma\gamma_4 = \tfrac{1}{6}s_2 - \tfrac{1}{4}\varepsilon c\sqrt{d} \,, \quad \gamma_2\gamma_3 = \tfrac{1}{6}s_2 + \tfrac{1}{4}\varepsilon c\sqrt{d} \,. \tag{41}$$

Writing $s_3 = (\gamma + \gamma_4)\,\gamma_2\gamma_3 + (\gamma_2 + \gamma_3)\,\gamma\gamma_4$, we find

$$s_3 = \tfrac{1}{6}s_1 s_2 + \tfrac{1}{4}cd \,. \tag{42}$$

This gives the expression (4) for c, and hence, using (40) and (2), the expression (3) for b. Thus $\Omega = \Omega^*$. Since $s_4 = \gamma\gamma_4\gamma_2\gamma_3$, we obtain (8) from (41), (2), (4).

We have the identity

$$|\gamma - \gamma_2|^2 - |\gamma_4 - \gamma_2|^2 = (\gamma - \gamma_4)(\gamma + \gamma_4 - \gamma_2 - \gamma_3) \,. \tag{43}$$

Since $\Omega > 0$, (9) follows from (34) and (43).

Conversely, assume that $d > 0$, and that (8), (9) are satisfied. Define b, c by (3), (4). Then (40) holds. The minimal polynomial $g(z)$ of γ factorizes as

$$\begin{aligned} g(z) = {} & (z^2 - \tfrac{1}{2}(s_1 + \sqrt{d})\, z + \tfrac{1}{6}s_2 - \tfrac{1}{4}c\sqrt{d}) \\ & (z^2 - \tfrac{1}{2}(s_1 - \sqrt{d})\, z + \tfrac{1}{6}s_2 + \tfrac{1}{4}c\sqrt{d}) \,. \end{aligned} \tag{44}$$

From (44), (40) we have (39), (41), (37), (38), (35). By (37), (20) holds for $j = 4$. Consider now the condition (20) for $j = 2$ (or $j = 3$). Substituting for b from (37), and using (35), we find that this condition is satisfied. Therefore $\Omega^* = b + c\gamma + \gamma^2$ satisfies (18), by Lemma 3. Finally (9), (43), (34) imply $\Omega^* > 0$.

The purpose of the next lemma is to enable us to construct quartic polynomials one of whose zeros may be taken to be γ. We therefore temporarily drop our previous assumptions concerning γ.

Lemma 11. *Let $g(z)$, given by* (1), *have degree* 4, *and satisfy $d > 0$ and* (8). *Define b , c by* (3), (4). *Then $g(z)$ has two unequal real zeros and two non-real zeros if and only if*

$$d < (s_1 + 2c)^2 . \tag{45}$$

Suppose that (45) *holds. Then $g(z)$ is irreducible over* **Q** *if and only if d is not a square in* **Q**. *Further, $b + c\gamma + \gamma^2$ is positive for precisely one of the two possible choices of γ as a real zero of $g(z)$, namely the one which is further from the non-real zeros.*

Proof. Since (8) is satisfied, $g(z)$ factorizes as in (44). The discriminants of the factors are $\frac{1}{2}d \pm (\frac{1}{2}s_1 + c)\sqrt{d}$. Now $g(z)$ has two unequal real zeros and two non-real zeros if and only if the product of these numbers is negative. Hence the first assertion is true.

Suppose now that (45) is satisfied. The result concerning the irreducibility of $g(z)$ is obvious. Using the same notation for the zeros of $g(z)$ as before, we obtain (39), (41) from (44), and (40) from (3), (4). Hence (37) holds. From the expression for the two discriminants we find $\varepsilon = \operatorname{sgn}(\frac{1}{2}s_1 + c)$. Using (37), we obtain $b + c\gamma + \gamma^2 = (\gamma - \gamma_4)(\gamma + \frac{1}{2}c)$, $b + c\gamma_4 + \gamma_4^2 = (\gamma_4 - \gamma)(\gamma_4 + \frac{1}{2}c)$. From (39), (41), (45), we have $16(\gamma + \frac{1}{2}c)(\gamma_4 + \frac{1}{2}c) = (s_1 + 2c)^2 - d > 0$. This shows the uniqueness of the choice of γ. Finally $\operatorname{sgn}(\gamma + \frac{1}{2}c) = \operatorname{sgn}(\gamma + \gamma_4 + c) = \operatorname{sgn}(\frac{1}{2}s_1 + c + \varepsilon\sqrt{d}) = \varepsilon$, so that the last assertion follows from (43).

5. Construction of algebraic numbers on circles

We assume in this section that γ has degree $n = 3$ or 4, and is such that there is an $\Omega > 0$ satisfying (18). Then we know from Lemmas 9 and 10 that $\Omega = \Omega^*$. Let S denote the circle $|z - \gamma|^2 = \Omega^*$. As we saw in the preceding section, the results of Lemma 4 hold.

We now define $H(z)$ by

$$H(z) = \sum_{A \in \mathfrak{H}} Az .$$

Then $H(z)$ is an automorphic function with respect to the group $\mathfrak{H}$. For $n = 3, 4$ we have, explicitly,

$$H(z) = z + \Gamma_2\Gamma z + \Gamma_3\Gamma z + [\Gamma_4\Gamma z] + \Gamma z + \Gamma_2 z + \Gamma_3 z + [\Gamma_4 z] ,$$

the terms in brackets occuring only for $n = 4$. From (15), (19), (31), (29. n), (30), we see that $H(z)$ can be written as a rational function $H(z) = U(z)/V(z)$, where $V(z)$ is given by (5), and $U(z)$ is a monic polynomial of degree $2n$. We shall work out $U(z)$ explicitly following the next lemma.

Lemma 12. *If z_0 is one root of $H(z) = \alpha$, then all the roots (counted with multiplicities) are given by Az_0, as A varies over $\mathfrak{H}$. If z_0 is not a fixed point of any $A \in \mathfrak{H}$, $A \neq 1$, then these roots are all different.*

Proof. As $H(Az_0) = H(z_0) = \alpha$, we see that Az_0 is a root of $H(z) = \alpha$, for each A in $\mathfrak{H}$. If z_0 is not a fixed point of any $A \in \mathfrak{H}$, $A \neq 1$, then all the Az_0 must be distinct, and so they exhaust the $2n$ roots of the equation $U(z) - \alpha V(z) = 0$. Thus the lemma is proved in this case. Since the roots of $U(z) - \alpha V(z) = 0$ are continuous functions of α, we see that the result is also true when z_0 is a fixed point of some $A \in \mathfrak{H} \setminus \{1\}$.

In particular, we see from Lemmas 12 and 1 that if one of the roots of $H(z) = \alpha$ lies on $\mathcal{S}$, then they all do.

We now calculate $U(z)$. To do this we evaluate $H(\varrho_1)$, where ϱ_1 is a fixed point of $\mathfrak{H}_0$, as in Lemma 4. We have $A\varrho_1 = \varrho_1$ for each $A \in \mathfrak{H}_0$, and $A\varrho_1 = \varrho_2$ for each $A \in \Gamma\mathfrak{H}_0$. Hence $H(\varrho_1) = n(\varrho_1 + \varrho_2) = - nc$. This means that the $2n$ roots of the equation $U(z) + ncV(z) = 0$ are ϱ_1 and ϱ_2, each repeated n times. So $U(z) + ncV(z) = (z^2 + cz + b)^n$, which gives (6).

We next remark that $H(z)$ is real, and varies continuously with z, for $z \in \mathcal{S}$. For $\overline{H(z)} = H(\bar{z}) = H(\Gamma z) = H(z)$ when $z \in \mathcal{S}$. Also the poles of $H(z)$ are γ_i, , $\Gamma\gamma_i$ $(i = 1, \ldots, n)$, and from Lemma 4 we know that none of these numbers lies on $\mathcal{S}$.

Lemma 13. *Only a fixed point of some $A \in \mathfrak{H}$, $A \neq 1$, can be an extreme point of $H(z)$, as z varies on $\mathcal{S}$.*

Proof. Let z_0 be a (relative) extreme point on $\mathcal{S}$. Choose $z_k \in \mathcal{S}$ such that $z_k \neq z_0$ for each k, and $\lim_{k \to \infty} z_k = z_0$. We may suppose that all the z_k lie in a sufficiently small neighbourhood of z_0. Since z_0 is an extreme point, it follows that for each k there exists $z_k' \neq z_k$ such that $H(z_k') = H(z_k)$ and $\lim_{k \to \infty} z_k' = z_0$. By Lemma 12, there is an element of $\mathfrak{H}$ which maps z_k onto z_k'. Since $\mathfrak{H}$ is finite, we may suppose that this element is the same for each k, i.e. $z_k' = Az_k$ for some $A \in \mathfrak{H}$, $A \neq 1$. Taking limits, we have $z_0 = Az_0$.

Lemma 14. *For $n = 3, 4$, the roots of $H(z) = \alpha$ lie on $\mathcal{S}$ if and only if $\alpha \in \Delta$.*

Proof. In order to find the extreme values of $H(z)$ for $z \in \mathcal{S}$, it is sufficient, by the previous lemma, to evaluate $H(z)$ at those $z \in \mathcal{S}$ which are fixed points of some $A \in \mathfrak{H} \setminus \{1\}$. However, we know from Lemma 4 that the $\Gamma_j (j = 1, \ldots, n)$ are the only elements of $\mathfrak{H} \setminus \{1\}$ which have their fixed points on $\mathcal{S}$. Therefore let z_0 be a fixed point of some Γ_i, and let $\mathcal{M} = \mathfrak{H} z_0$, the orbit of z_0 under $\mathfrak{H}$. Then in fact $\mathcal{M} = \{\Gamma_j z_0 | j =$

$1, \ldots, n\}$, because $\Gamma_j z_0 \neq \Gamma_k z_0$ for $j \neq k$, by Lemma 4 (iii). Further, for any $A \in \mathfrak{H}$, Az_0 is a fixed point of $A\Gamma_i A^{-1}$, i.e. the points in $\mathfrak{M}$ are fixed points of elements of $\mathfrak{H}$ belonging to the same conjugacy class as Γ_i.

Consider first the case $n = 4$. Then in $\mathfrak{H}$ the Γ_j $(j = 1, \ldots, 4)$ split into two conjugacy classes $\{\Gamma, \Gamma_4\}$ and $\{\Gamma_2, \Gamma_3\}$. Correspondingly, there are two orbits $\mathfrak{M}_1$ and $\mathfrak{M}_2$, where e.g. $\mathfrak{M}_1$ contains the two fixed points of both Γ and Γ_4.

Since the sum of the fixed points of Γ_j is $2\gamma_j$, we have, using (39), for $\mathfrak{M} = \mathfrak{M}_1$,

$$H(z_0) = 2 \sum_{z \in \mathfrak{M}_1} z = 4(\gamma + \gamma_4) = 2(s_1 + \varepsilon\sqrt{d}) ,$$

where $\varepsilon = \pm 1$. Similarly, for $\mathfrak{M} = \mathfrak{M}_2$, $H(z_0) = 2(s_1 - \varepsilon\sqrt{d})$.

Consider now the case $n = 3$. Then all the involutions Γ_j $(j = 1, 2, 3)$ belong to the same conjugacy class in the group $\mathfrak{H}$. Therefore the two fixed points of each Γ_j must belong to different orbits. We thus again get two orbits, and hence the extreme values of $H(z)$ on $\mathcal{S}$ are $H(\gamma - R)$ and $H(\gamma + R)$, where R is an abbreviation for $\Omega^{*1/2}$.

It is possible to calculate $H(\gamma \pm R)$ directly. However, we shall use a different method. Consider the set $\mathfrak{M}_0 = \{\gamma_j \pm \Omega_j^{*1/2} \mid j = 1, 2, 3\}$, which is the union of the two orbits. Since it clearly contains a set of conjugate algebraic numbers on $\mathcal{S}$ with at least three members, we can choose an element of $\mathfrak{M}_0$ to be the β of Section 3, and apply the results of that section. Let $\mathfrak{L}$ be the smallest normal extension of $\mathbf{Q}$ containing $\mathfrak{M}_0$. Then, as we have seen, $\mathfrak{L}$ contains $\mathfrak{K}$. Since from (33),

$$d\Omega_j^* = (\gamma_j - \gamma_k)^2(\gamma_j - \gamma_l)^2 \tag{46}$$

for any permutation $\{j, k, l\}$ of $\{1, 2, 3\}$, we clearly have $\mathfrak{L} = \mathbf{Q}(\gamma, \gamma_2, \gamma_3, \sqrt{d})$. Choose $\sigma_2 \in \mathrm{Gal}\,(\mathfrak{L}/\mathbf{Q})$ so that it interchanges γ and γ_2, and leaves γ_3 fixed. Using the notation of Lemma 2, we see that $\sigma_2\varkappa\sigma_2^{-1}$ interchanges γ and γ_3, and leaves γ_2 and $\sqrt{d}$ fixed. By the proof of Lemma 2, we obtain from (46)

$$\begin{aligned}\Gamma_2(\gamma + \varepsilon R) = \sigma_2\varkappa\sigma_2^{-1}(\gamma + \varepsilon R) &= \gamma_3 + \varepsilon\sigma_2\varkappa\sigma_2^{-1}(d^{-1/2}(\gamma - \gamma_2)(\gamma - \gamma_3)) \\ &= \gamma_3 - \varepsilon d^{-1/2}(\gamma_3 - \gamma_2)(\gamma_3 - \gamma) ,\end{aligned}$$

where $\varepsilon = \pm 1$. Since $\Gamma_3 = \bar{\Gamma}_2$, and $\gamma + \varepsilon R$ is a fixed point of Γ, we have

$$\begin{aligned}H(\gamma + \varepsilon R) = 2s_1 + 2\varepsilon d^{-1/2}((\gamma - \gamma_2)(\gamma - \gamma_3) &+ (\gamma_3 - \gamma_2)(\gamma_3 - \gamma) \\ &+ (\gamma_2 - \gamma_3)(\gamma_2 - \gamma)) = 2(s_1 + \varepsilon\sqrt{d}) .\end{aligned} \tag{47}$$

This completes the proof of Lemma 14. From these considerations it also follows immediately, by Lemma 12, that the following is true:

Lemma 15. *For* $n = 3, 4,$ *the polynomial* $F(z;\alpha) = U(z) - \alpha V(z)$ *has all its zeros on* S *if and only if* $\alpha \in \Delta$. *Furthermore, the* $2n$ *zeros of* $F(z;\alpha)$ *are distinct if* α *is not an endpoint of* Δ. *If* α *is an endpoint of* Δ, *then each zero of* $F(z;\alpha)$ *occurs exactly twice.*

6. Proof of Theorem 1

We can now prove Theorem 1. First suppose that there is an $\Omega > 0$ such that the circle $|z-\gamma|^2 = \Omega$ contains a set of conjugate algebraic numbers with at least three members. Then as we saw in Section 3, (18) is true. Lemmas 9 and 10 now show that (7) holds, and that (8), (9) hold when $n = 4$. This proves the first part of the theorem.

Conversely, suppose that $d > 0$, and that (8), (9) hold if $n = 4$. Then we know from Lemmas 9 and 10 that Ω^* is pcsitive and satisfies (18). We can therefore apply the results of the previous section.

Let α be an algebraic number, all of whose conjugates α_i lie in Δ. Then it follows from Lemma 15 that condition (10) determines a monic polynomial $P(z)$. Furthermore, all the zeros of $P(z)$ lie on $|z-\gamma|^2 = \Omega^*$. Clearly $P(z) \in \mathbf{Q}[z]$. We now show that $P(z)$ is irreducible over $\mathbf{Q}$. Let β be a zero of $P(z)$ such that $U(\beta)/V(\beta) = \alpha$, and let β' be any other zero of $P(z)$. Then $U(\beta')/V(\beta') = \alpha_i$ for some index i. Choosing an automorphism of a suitable normal extension of $\mathbf{Q}$ which maps α to α_i, we see that β is mapped to some conjugate β'', and $U(\beta'')/V(\beta'') = \alpha_i$. But now by Lemma 12, $\beta'' = A\beta'$ for some $A \in \mathfrak{H}$, and so, as we saw in Section 3, β' and β'' are conjugate. Hence β' and β are conjugate, which proves the irreducibility of $P(z)$.

On the other hand, let β be any algebraic number, all of whose conjugates β_j lie on $|z-\gamma|^2 = \Omega^*$. Let $P(z)$ denote the minimal polynomial of β over $\mathbf{Q}$. The numbers $H(\beta_j)$ form a complete set of conjugate algebraic numbers contained in Δ. Denote these numbers by α_i, each one being counted only once. Since each $A \in \mathfrak{H}$ permutes the conjugates β_j, we can divide the β_j into orbits under $\mathfrak{H}$. From Lemmas 12 and 15 it now readily follows that (10) holds. This completes the proof of Theorem 1.

Further remarks. If α is an interior point of Δ, then we see from (10) that $P(z)$ always has degree divisible by $2n$ $(n = 3, 4)$. If α is an endpoint of Δ, then we have two cases:

(a) $\sqrt{d} \in \mathbf{Q}$. Then from Lemma 11, we must have $n = 3$. Further

α is rational, and we have two polynomials $P_\varepsilon(z)(\varepsilon = \pm 1)$ of degree 3, defined by

$$P_\varepsilon(z)^2 = U(z) - 2(s_1 + \varepsilon \sqrt{d})\, V(z)\,. \tag{48}$$

By (47), $P_\varepsilon(z)$ is the minimal polynomial of $\gamma + \varepsilon \Omega^{*1/2}$. The zeros of $P_1(z)P_{-1}(z)$ comprise all the fixed points of the Γ_j.

(b) $\sqrt{d} \notin \mathbf{Q}$. Here α has degree 2, so

$$P(z)^2 = (U(\mathrm{z}) - 2(s_1 + \sqrt{d})\, V(z))(U(z) - 2(s_1 - \sqrt{d})\, V(z))\,. \tag{49}$$

In this case $P(z)$ has degree $2n$ $(n = 3\ ,\ 4)$, and it is the common minimal polynomial of the fixed points of all the Γ_j.

7. First part of Theorem 2. Cubic case

In this section and the next we prove the first part of Theorem 2. The converse part is proved in Section 9.

Let γ be as in the statement of Theorem 2. Suppose that there exists at least one set of conjugate algebraic integers on the circle $|z - \gamma|^2 = \Omega^*$. Then it follows from Theorem 1 that there is a number $\alpha \in \Delta$ such that $U(z) - \alpha V(z) \in \mathbf{A}[z]$. Since the coefficient of z^{2n-1} is $-\alpha$, we have $\alpha \in \mathbf{A}$. The coefficients of $z^{2n-2},\ z^{2n-3}, \ldots , z^0$ give us $2n-1$ other conditions.

We now separate the cubic and quartic cases, the latter being dealt with in the next section. For the cubic case, we introduce the following notation, additional to that used in the statement of Theorem 2. Put

$$B = -SC - rT\ ,\quad D = S^2 - 3qT\ ,$$

and

$$\delta = r\alpha + 3C\ ,\quad \theta = q\alpha - 2S\ .$$

Then from (36) and (2),

$$b = B/3qr\ ,\quad d = D/q^2\ .$$

Further

$$E = 3qC^2 - rB\ . \tag{50}$$

The conditions (12.3) in Theorem 2 can be written as

$$3(3\ ,\ q)^{-1}q \mid B\ ,\quad (3\ ,\ r)^2 r^4 \mid D\ . \tag{51}$$

From (36) we obtain $s_2 = -s_1c - 3b$, $3s_3 = -s_1b - s_2c = -s_1b + s_1c^2 + 3bc$. Therefore, expressing $F(z\ ;\alpha) = U(z) - \alpha V(z)$ in the form $(z^2 + cz + b)^3 - (\delta/r)V(z)$, it is easy to verify that the $2n - 1 = 5$ conditions mentioned above can be written in the form:

$$(52.4)\qquad (-qC + rS)\delta + 3qC^2 + rB \equiv 0 \qquad \mod qr^2 ,$$

$$(52.3)\qquad (-3qC^2 + 18rSC + 10rB)\delta + 9qC^3 + 18rBC \equiv 0 \qquad \mod 9qr^3 ,$$

$$(52.2)\qquad (15qSC^2 + 12qBC - 2rSB)\delta + 9qBC^2 + 3rB^2 \equiv 0 \qquad \mod 9q^2r^3 ,$$

$$(52.1)\qquad (-6qTC^2 - 2SBC - B^2)\delta + 3B^2C \equiv 0 \qquad \mod 9q^2r^3 ,$$

$$(52.0)\qquad (-3qC^2 + rB)(3qTC + SB)\delta + 3rB^3 \equiv 0 \qquad \mod 81q^3r^4 .$$

Here $(52 . j)$ expresses the fact that the coefficient of z^j in $F(z ; \alpha)$ belongs to **A**.

Replacing $-qC\delta$ by $-qrC\alpha - 3qC^2$ in (52.4), we obtain

$$(53)\qquad S\delta \equiv - B \mod q .$$

We shall also need the three congruences obtained by forming $3CL_4 - L_3$, $3BL_4 - L_2$, $2TL_3 - L_1$, where L_j stands for the left-hand side of $(52 . j)$. These give

$$(54)\qquad (B + 3rT)\alpha + 9TC \equiv 0 \mod 3q(5 , q)^{-1} ,$$

$$(55)\qquad (3qTC + SB)\delta \equiv 0 \mod 3qr(B , 3qr)(5 , qr)^{-1} ,$$

$$(56)\quad (-B^2 + 36rSTC + 18rTB)\delta + 18qTC^3 - 3B^2C + 36rTBC \equiv 0 \mod 9qr^3 .$$

Lemma 16. *The congruences* (52) *imply that* $(q , r) = (q , S) = 1$.

Proof. We need the following results, which we also use later:

$$(57)\qquad (3 , r)q|B , \quad q|S\delta .$$

By (53) it is enough to prove the first result. Let p be any prime, and let $p^\sigma\|q$, $p^\tau\|r$, $p^\nu\|B$. Suppose first that $p \neq 3 , 5$, and that $\nu < \sigma$. Then (55) shows that the term containing δ in (52.0) is divisible by $p^{\sigma+\tau+2\nu}$, while the other term is divisible exactly by $p^{\tau+3\nu}$. This is impossible, so that $\nu \geqq \sigma$. For $p = 3$, a similar argument shows that $\nu \geqq \sigma$, and that $\nu \geqq \sigma + 1$ for $\tau > 0$. Consider finally the case $p = 5$. If $\tau > 0$, the same argument again gives $\nu \geqq \sigma$. Suppose therefore that $5 \nmid r$, and that $\nu < \sigma$. Then $5 \nmid S$, by (53) and the definition of B. Using (53) again we obtain from (52.0), $2rB^3 \equiv 0 \mod 5^{\sigma+2\nu}$, which is impossible. This proves (57).

Write $u = (q , r)$. Then $(u , S , T) = (u , C) = 1$. From (57) and the definition of B, we obtain $(3 , u)u|B$, $u|S$. Hence $(u , T) = 1$. From (54), $(3 , u)u|45$, so that $u|15$. Furthermore, $5|u$ is possible only if $5^1\|q$. In this case, however, (55) leads to a contradiction, because $5 \nmid \delta$, by the definition of δ. Thus $u|3$. If $u = 3$, then (57) implies $3^{\sigma+1}|B$, $3^\sigma|S\delta$.

But this contradicts (56), because $3^{\sigma+3}$ divides every term except $18qTC^3$. We have thus proved that $u = 1$. The second assertion of the lemma follows immediately from (53) and the definition of B.

Lemma 17. *Suppose that* $q | B$, $(q , r) = (q , S) = 1$, $\lambda = 2$. *Then there exists a rational integer* δ_0 *such that*

$$(58) \qquad 3q | \delta_0 , \quad 3^{3\sigma+4} | L_0(\delta_0) ,$$

where $L_0(\delta)$ *denotes the left-hand side of* (52.0), *and* $3^\sigma \| q$.

Proof. Using the identity

$$(59) \qquad r(3qTC + SB) = - 3qBC - SE ,$$

we can write (52.0) in the following equivalent form:

$$(60) \qquad E(3qBC + SE)\delta + 3r^2B^3 \equiv 0 \mod 81q^3r^5 .$$

Since $3^\sigma | B$, $3^\sigma | E$ by (50). As $\lambda = 2$, $\sigma \geqq 1$ and $3^\sigma \| E$. Consider now (60) mod $3^{3\sigma+4}$. We can solve this congruence for δ. If δ_0 is a solution, then $3^{\sigma+1} | \delta_0$, and the result follows.

For the proof of the next lemma, it is convenient to have the congruences (52) expressed in terms of θ and D:

$$(61.4) \qquad (- qC + rS)\theta + 5qrT + 2rD \equiv 0 \qquad \mod q^2r ,$$

$$(61.3) \qquad (- 3qC^2 + 8rSC - 10r^2T)\theta - 20r^2ST + 16rCD \equiv 0 \qquad \mod 9q^2r^2 ,$$

$$(61.2) \qquad (3qSC^2 - 12qrTC - 2rSB)\theta + 15qr^2T^2 + (15qC^2 - 4rB)D \equiv 0 \qquad \mathrm{mcd}\ 9q^3r^2 ,$$

$$(61.1) \qquad - rT(3qC^2 + r^2T)\theta - 2r^3ST^2 + (6qC + 2rS + r\theta)C^2D \equiv 0 \qquad \mod 9q^3r^3 ,$$

$$(61.0) \qquad r(3qC^2 + rSC + r^2T)(CD + rST)\theta + 3qr^4T^3 + (9q^2C^4 + 6qrSC^3 + 9qr^2TC^2 + 2r^2C^2D + 4r^3STC + 2r^4T^2)D \equiv 0 \mod 81q^4r^4 .$$

Here $(61 . j)$ is a reformulation of $(52 . j)$.

Lemma 18. *The congruences* (52) *imply that* (51) *holds, and that*

$$(62) \qquad 3^{\varkappa-2\lambda}q | \delta - \delta_0 , \quad (3 , r)r^2 | \theta ,$$

where δ_0 *is defined as in Lemma* 17 *if* $\lambda = 2$, *and* $\delta_0 = 0$ *if* $\lambda \neq 2$.

Proof. Note that, for $\lambda = 2$, the supposition of Lemma 17 is satisfied by Lemma 16 and (51). We divide the argument into five cases, which show that (51) and (62) are true locally, for each prime p dividing $3qr$. The congruences (52) are more suitable for dealing with the prime divisors of q, while the congruences (61) are more suitable for prime divisors of r.

Case I: $p \neq 3\,, p^{\sigma} \| q\,, \sigma \geqq 1$. We have $p \nmid rS$ by Lemma 16. The required results follow immediately from (57).

Case II: $p \neq 3\,, p^{\tau} \| r\,, \tau \geqq 1$. We have $p \nmid qC$. From (61.4), $p^{\tau} | \theta$, and so using (61.1), $p^{2\tau} | 2D$. Next, from (61.3), $p^{2\tau} | \theta$, and then (61.0) gives $p^{4\tau} | D$.

Case III: $p = 3\,, 3^{\sigma} \| q\,, \sigma \geqq 1$. We have $3 \nmid rS\,, \varkappa = 0$. From (57), $3^{\sigma} | B\,, 3^{\sigma} | \delta$. Hence (51) is true at the prime 3. To prove that (62) also holds at the prime 3, we have to show that $3^{\sigma+2\lambda} | \delta - \delta_0$. If $\lambda = 2$, then δ and δ_0 both satisfy (60), and the result follows, because $3^{\sigma} \| E$. Let $\lambda \neq 2$. Then $\delta_0 = 0$. For $\lambda = 0$, we already have the result. Suppose therefore that $\lambda = 1$. Then $3^{\sigma-1} | E$, whence $3^{\sigma-1} | B$ by (50). From (60) we now deduce $3^{\sigma+2} | \delta$.

Case IV: $p = 3\,, 3^{\tau} \| r\,, \tau \geqq 1$. We have $3 \nmid qC\,, \varkappa = \lambda = 0$. From (57), $3 | B$, whence $3 | S\,, 3 | D$. From (61.4), $3^{\tau} | \theta$, and so using (61.1), $3^{2\tau} | D$. In particular, $3 | T$. From (61.3), $3^{2\tau} | \theta$, and then $3^{4\tau} | D$ by (61.0). Using (61.3) and (61.0) again, we finally have $3^{2\tau+1} | \theta\,, 3^{4\tau+2} | D$.

Case V: $p = 3\,, 3 \nmid qr$. Then $\lambda = 0\,, \delta_0 = 0$, and we have to prove that $3 | B\,, 3^{\varkappa} | \delta$. Suppose that $3 \nmid B$. Then (52.3) implies $9 | \delta$, which contradicts (52.2). To prove the second assertion, we obtain from (52.3) and (60)

$$(63) \qquad E\delta \equiv 0 \mod 9\,, \quad SE^2\delta \equiv 0 \mod 81\,,$$

and the result follows easily by the definition of $\varkappa$.

This completes the proof of Lemma 18, and hence the first part of Theorem 2 in the case $n = 3$.

8. First part of Theorem 2. Quartic case

We now prove two lemmas for $n = 4$, which correspond to Lemmas 16 and 18. The method of proof is similar to that in the last section, though the results here are somewhat simpler. In particular, there is no analogue to Lemma 17.

Let $n = 4$. Put

$$B = -SC - 2rT\,, \quad D = S^2 - 8qT\,,$$

and

$$\delta = r\alpha + 4C\,, \quad \theta = q\alpha - 2S\,.$$

Then from (40) and (2),

$$b = B/4qr\ ,\quad d = D/q^2\ .$$

The conditions (12.4) can be written in the form

$$4q|B\ ,\quad 2^{4\lambda}r^6|D\ . \tag{64}$$

From (2), (40), (42), (44), we have $s_2 = -\frac{3}{2}s_1c - 6b$, $s_3 = -s_1b + s_1c^2 + 4bc$, $s_4 = \frac{1}{2}s_1bc - \frac{1}{4}s_1c^3 + b^2 - bc^2$. Therefore the $2n - 1 = 7$ conditions mentioned in Section 7 can be written as

$$(-3qC + 2rS)\delta + 12qC^2 + 2rB \equiv 0 \qquad \mod 2qr^2\ , \tag{65.6}$$

$$(-4qC^2 + 12rSC + 7rB)\delta + 16qC^3 + 12rBC \equiv 0 \qquad \mod 4qr^3\ , \tag{65.5}$$

$$(-2q^2C^3 - 7qrBC - 68qr^2TC - 4r^2SB)\delta + 8q^2C^4 + 24qrBC^2 + 3r^2B^2 \equiv 0 \qquad \mod 8q^2r^4\ , \tag{65.4}$$

$$(-4qBC^2 - 112qrTC^2 - 16rSBC - 7rB^2)\delta + 16qBC^3 + 12rB^2C \equiv 0 \qquad \mod 16q^2r^4\ , \tag{65.3}$$

$$(-112q^2TC^3 - 28qSBC^2 - 17qB^2C + 2rSB^2)\delta + 12qB^2C^2 + 2rB^3 \equiv 0 \qquad \mod 32q^3r^4\ , \tag{65.2}$$

$$(-64q^2TC^4 - 24qSBC^3 - 16qB^2C^2 + 4rSB^2C + rB^3)\delta + 4rB^3C \equiv 0 \qquad \mod 64q^3r^5\ , \tag{65.1}$$

$$2qC(2qC^2 - rB)(-4T(2qC^2 - rB) + B^2)\delta + r^2B^4 \equiv 0 \qquad \mod 256q^4r^6\ . \tag{65.0}$$

Again we need these congruences expressed in terms of θ and D:

$$(-3qC + 2rS)\theta + 28qrT + 4rD \equiv 0 \qquad \mod 2q^2r\ , \tag{66.6}$$

$$(-4qC^2 + 5rSC - 14r^2T)\theta - 28r^2ST + 10rCD \equiv 0 \qquad \mod 4q^2r^2\ , \tag{66.5}$$

$$(-2q^2C^3 + 7qrSC^2 - 54qr^2TC - 4r^2SB)\theta + 140qr^3T^2 + (33qrC^2 - 8r^2B)D \equiv 0 \qquad \mod 8q^3r^3\ , \tag{66.4}$$

$$(4qSC^3 - 104qrTC^2 + 9rB^2 + 32r^2TB)\theta - 56r^3ST^2 + (56qC^3 + 18rSC^2 + 8r^2TC)D \equiv 0 \qquad \mod 16q^3r^3\ , \tag{66.3}$$

$$(-112q^2rTC^3 + 11qrS^2C^3 - 12qr^2STC^2 - 68qr^3T^2C + 2r^2SB^2)\theta + 112qr^4T^3 + (56q^2C^4 + 28qrSC^3 + 28qr^2TC^2 + 4r^2B^2)D \equiv 0 \qquad \mod 32q^4r^4\ , \tag{66.2}$$

$$(66.1)\quad \begin{aligned}&(-16qr^2STC^3-64qr^3T^2C^2+3r^2S^3C^3+10r^3S^2TC^2+4r^4ST^2C\\&-8r^5T^3)\theta-16r^5ST^3+(32q^2C^5+24qrSC^4+32qr^2TC^3\\&+6r^2S^2C^3+20r^3STC^2+8r^4T^2C+8qrC^4\theta)D\equiv 0\\&\hspace{6cm}\bmod\ 64q^4r^5\,,\end{aligned}$$

$$(66.0)\quad \begin{aligned}&(-48qr^3T^2C^3+4r^3S^2TC^3-8r^4ST^2C^2-16r^5T^3C)\theta+16r^6T^4\\&+(16q^2C^6+16qrSC^5+64qr^2TC^4+5r^2C^4D+16r^3STC^3\\&+8r^4T^2C^2+4qrC^5\theta+2r^2SC^4\theta)D\equiv 0\qquad\bmod\ 256q^4r^6\,.\end{aligned}$$

As before $(66\,.\,j)$ is equivalent to $(65\,.\,j)$.

Replacing $-3qC\delta$ by $-3qrC\alpha-12qC^2$ in (65.6), we obtain

$$(67)\qquad S\delta\equiv -B \mod q(2\,,C)(2\,,qC)^{-1}\,.$$

We need the two congruences obtained by forming $4CL_6-3L_5$ and $-BL_5+L_3$, where L_j denotes the left-hand side of $(65\,.\,j)$. These give

$$(68)\qquad (B+8rT)\alpha+32TC\equiv 0 \mod 4q(2\,,r)(7\,,q)^{-1}\,,$$

$$(69)\qquad (-4T(2qC^2-rB)+B^2)\delta\equiv 0 \mod 2qr^2(B\,,4qr)(7\,,qr)^{-1}\,.$$

Lemma 19. *The congruences* (65) *imply that* $(q\,,r)=1\,,(q\,,S)|2$.

Proof. We need the following results, which are again also used later:

$$(70)\qquad 4q|(2\,,r)B\,,\quad (2\,,C)q|(2\,,qC)S\delta\,,\quad 2|SC\,.$$

By (67) and the definition of B, it is enough to prove the first result. Let p be prime, and let $p^\sigma\|q\,,p^\tau\|r\,,p^\nu\|B$. Consider first the case $p\neq 2$. If $\nu<\sigma$, then (69) shows that the term containing δ in (65.0) is divisible by $p^{2\sigma+2\tau+2\nu-1}$ (-1 in the exponent is only needed for $p=7$), while the other term is divisible exactly by $p^{2\tau+4\nu}$. This is impossible, so that $\nu\geqq\sigma$. For $p=2$, we similarly obtain $\nu\geqq\sigma+1$. Furthermore, if r is odd and $\nu=\sigma+1$, then $2^{\sigma+2}|C(2qC^2-rB)$, which again leads to a contradiction. Thus $\nu\geqq\sigma+2$ in this case. This proves (70).

Suppose now that p divides both q and r, so that σ and τ are positive. Then $p\nmid C$. From (70) and the definition of $B\,,p|B\,,p|S$, so that $p\nmid T$. If $p\neq 2$, then (68) shows that $p=7\,,7^1\|q$. However, in this case (69) leads to a contradiction, because $7\nmid\delta$. Therefore necessarily $p=2$, so that $(q\,,r)$ is a power of 2.

If $\sigma\geqq 2$, it is easy to see (using (70)) that the factor of δ in (69) is divisible exactly by $2^{\sigma+3}$, whence $2^{\sigma+1}|\delta$. But this contradicts (65.4), because $2^{2\sigma+4}$ divides every term except $8q^2C^4$. Thus $\sigma=1$. If $8|B$, then similarly $8|\delta$, and the same contradiction arises. Hence $2^2\|B$, so that $4 | S$, $16 | D$, by the definition of B and D. From (66.6), $2^{\tau+2} | \theta$. Using (66.0) we obtain

$$(71) \quad 2^{3\tau+5}\xi\theta + 16r^6T^4 + (16q^2C^6 + 5r^2C^4D + 128\eta)D \equiv 0 \mod 2^{6\tau+12} ,$$

for some $\xi , \eta \in \mathbf{A}$. If $\tau = 1$, consider (71) modulo 2^{11}. Then the terms containing ξ and η disappear, and it is easy to deduce a contradiction. Thus $\tau \geqq 2$, and it follows from (71) that $2^{4\tau+1} | D$. By the definition of D, $2^2 \| S$. Applying (66.4), we find that $2^{3\tau} | \theta$, so that (71) gives $2^{6\tau-2} | D$. Write $q = 2q_1 , r = 2^\tau r_1 , \theta = 2^{3\tau}\theta_1$. Then (66.4) modulo $2^{3\tau-5}$ and (66.2) modulo $2^{4\tau-7}$ yield

$$C\theta_1 + q_1r_1 \equiv 2\theta_1 + C\theta_1 + r_1T \equiv 0 \mod 4 .$$

Hence $2 \nmid \theta_1$ and $q_1T \equiv -1 \mod 4$. However.

$$q_1T \equiv (S/4)^2 - D/16 \equiv 1 \mod 4 .$$

a contradiction.

We have proved that $(q , r) = 1$. The second assertion of the lemma follows from (70) and the definition of B.

Lemma 20. *The congruences* (65) *imply that* (64) *holds, and that*

$$(72) \qquad 2^{3\varkappa}q | \delta , \quad 2^{2\lambda}r^3 | \theta .$$

Proof. The proof is similar in structure to that of Lemma 18. We prove the results locally at each prime p dividing $2qr$.

Case I: $p \neq 2 , p^\sigma \| q , \sigma \geqq 1$. We have $p \nmid rS$. The required results follow from (70).

Case II: $p \neq 2 , p^\tau \| r , \tau \geqq 1$. We have $p \nmid qC$. From (66.5), $p^\tau | \theta$. Hence from (66.0), $p^{4\tau} | D$. Then (66.4) implies $p^{3\tau} | \theta$, and using (66.0) again we find $p^{6\tau} | D$.

Case III: $p = 2 , 2^\sigma \| q , \sigma \geqq 1$. We have $2 \nmid r$. If S is odd, then $\varkappa = \lambda = 0$, and (70) shows that C is even, whence the results follow from (70). Suppose therefore that S is even. Then T is odd, so that necessarily $2 \nmid C$, $2^1 \| S$, because $4 | B$. Thus $\varkappa = 1 , \lambda = 0$. Now (70) gives $2^{\sigma+2} \| B$, so that $2^{\sigma+3} | \delta$ by (65.0).

Case IV: $p = 2 , 2^\tau \| r , \tau \geqq 1$. We have $2 \nmid qC$. By (66.6), $2^{\tau+2} | \theta$. From (66.5) we get $8 | D$, so that $4 | S$. Thus $\varkappa = 0 , \lambda = 1$. It follows from (66.0) that $2^{4\tau+2} | D$. Hence T is even. From (66.4) we have $2^{3\tau-2} | \theta$, and then, from (66.0), $2^{6\tau-4} | D$. Plainly $4 | B$.

Case V: $p = 2 , 2 \nmid qr$. By (70), $4 | B$. If C is even, then $\varkappa = \lambda = 0$, and there is nothing more to prove. Suppose therefore that C is odd, so that S is even. From (65.4), $4 | \delta$.

If $2^1 \| S$, then $\varkappa = 1 , \lambda = 0$. By the definition of B , T is odd. Now (65.0) gives $8 | \delta$.

For $4 \mid S$, we have $\varkappa = 0$, $\lambda = 1$. In this case T is even, whence $16 \mid D$. By the definition of δ, $4 \mid \alpha$, so that also $4 \mid \theta$.

This completes the proof of Lemma 20, and thus proves the first part of Theorem 2.

9. Converse part of Theorem 2

We need the following lemma, which is a trivial generalization of well-known results concerning sets of conjugate algebraic integers in a real interval.

Lemma 21. *Let* $\alpha_0 \in \mathbf{Q}$, $w \in \mathbf{Z}$ $(w > 0)$ *be fixed, and let* Δ *be any closed interval of length* $|\Delta|$ *with midpoint* a.

If $|\Delta| < 4w$, *then* Δ *contains only finitely many sets of conjugate algebraic numbers of the form* $\alpha_0 + w\xi$, *for* $\xi \in \mathbf{A}$.

If $|\Delta| > 4w$, *or if* $|\Delta| = 4w$ *and* $(a - \alpha_0)/w \in \mathbf{Z}$, *then* Δ *contains infinitely many such sets.*

Proof. We have $\alpha_0 + w\xi \in \Delta$ if and only if $(a - \alpha_0)/w - |\Delta|/2w \leqq \xi \leqq (a - \alpha_0)/w + |\Delta|/2w$, and the lemma follows easily from results of Schur, Pólya, and Robinson. (See [2].)

Now let γ be as in the statement of Theorem 2, and suppose that (11) and (12 . n) hold. In the cubic case note that $(q, S) = 1$, by (51), (11), and the definition of B. Hence the supposition of Lemma 17 is satisfied for $\lambda = 2$.

From Theorem 1 we know that to each set of conjugate algebraic integers on $|z - \gamma|^2 = \Omega^*$, there corresponds a set of conjugate algebraic numbers contained in Δ. If α is a member of the latter set, then we saw in Sections 7 and 8 that α is an algebraic integer, and satisfies the conditions (62) for $n = 3$, (72) for $n = 4$ (given in terms of δ and θ). Conversely, it is easy to verify that when α does satisfy these conditions, then the congruences (52) for $n = 3$, (65) for $n = 4$, are satisfied. The verification is done locally, for each prime p dividing nqr. For primes dividing r we verify the equivalent congruences (61) for $n = 3$, (66) for $n = 4$, instead of (52) or (65) directly. There are, however, a few points to note when carrying out this verification. All the cases with $p \nmid n$ are very easy, whence we only consider more closely the primes $p = 3, 2$, respectively. We use the same numbering of cases as in Lemmas 18 and 20.

(a) $n = 3$. First consider case III. For $\lambda \neq 2$, we have $3^{\sigma+1} \mid B$, and the result follows readily, using (59). For $\lambda = 2$, we have $3^{\sigma} \| E$, $3^{\sigma} \| B$, $3^{\sigma+1} \mid \delta$ Now (52.0) modulo $3^{3\sigma+4}$ follows trivially from (62). Further, from (52.0), $S\delta \equiv 6B \bmod 3^{\sigma+2}$. Using this, one can then verify that the other congruences (52) hold. In case IV use the fact that $3|S$ and $3|T$, as $9|D$. In case V we have $3|B$, $3^{\varkappa}|\delta$, and that (63) holds. Then the required results follow from (59).

(b) $n = 4$. In case III we have $4 \nmid S$, as $4|B$. Therefore $2|C$ when $\varkappa = 0$. In case IV we have $4|S$, $2|T$, as $16|D$. Hence $\lambda = 1$. Finally, in case V it is readily seen that the congruences (65) hold when C is even. If C is odd, note that either $2^1\|S$, $\varkappa = 1$ or $4|S$, $\lambda = 1$. In the former case $8|\delta$ by (72). In the latter case, from (64) and (72), $16|D$ and $4|\theta$, whence $2|T$ and $4|\alpha$, $4|\delta$.

Now since $(3^{\varkappa+\lambda}q\,, r) = 1$ for $n = 3$, and $(2^{\varkappa}q\,, 2^{\lambda}r) = 1$ for $n = 4$, we see that α is determined mod w by (62) or (72), where

$$w = \begin{cases} 3^{\varkappa+2\lambda}(3\,, r)qr^2 & \text{if } n = 3\,, \\ 2^{3\varkappa+2\lambda}qr^3 & \text{if } n = 4\,. \end{cases}$$

Hence the α which satisfy (62) or (72) are the numbers of the form $\alpha = \alpha_0 + w\xi$, where α_0 is a fixed rational integer, and ξ is any algebraic integer. We therefore have a one-to-one correspondence between sets of conjugate algebraic integers on the circle $|z - \gamma|^2 = \Omega^*$, and sets of conjugate algebraic integers of the form $\alpha_0 + w\xi$ in Δ.

Now Δ has length $|\Delta| = 4\sqrt{d}$, and the condition (13) is equivalent to $d \geqq w^2$. So the converse part of Theorem 2 follows from Lemma 21 if $d \neq w^2$. Let us therefore consider the special case when $d = w^2$. As we already remarked in Section 2, this is only possible when γ is cubic. We have

$$S^2 - 3qT = 3^{2\varkappa+4\lambda}(3\,, r)^2q^4r^4\,,$$

so that $(q\,, S) = 1$ implies $q = 1\,, \lambda = 0$. Thus

$$S^2 - 3T = 3^{2\varkappa}(3\,, r)^2r^4\,. \tag{73}$$

Let us calculate a value for α_0 in this case. It is determined by

$$r\alpha_0 \equiv -\,3C \mod 3^{\varkappa}\,, \quad \alpha_0 \equiv 2S \mod (3\,, r)r^2\,.$$

For $\varkappa = 0$ or 1, we can take $\alpha_0 = 2S$, because $3|S$ for $\varkappa = 1$, by (73). But (73) also shows that the case $\varkappa = 2$ cannot occur.

The midpoint a of the interval Δ is $2s_1 = 2S = \alpha_0$. Hence, trivially, $(a - \alpha_0)/w \in \mathbf{Z}$. It now follows from Lemma 21 that we also have infinitely many sets of conjugate algebraic integers on $|z - \gamma|^2 = \Omega^*$ in the case $d = w^2$. This completes the proof of Theorem 2.

10. Circles with rational or totally real centre

We shall reproduce the earlier work by Robinson concerning algebraic integers on a circle with rational centre γ, using arguments similar to those we have used when γ is not totally real. The argument for $\gamma \in \mathbf{Q}$ is slightly different, however, one reason being that we do not have the result $\Omega \in \mathbf{Q}(\gamma)$, as we have when γ is irrational.

Let β be an algebraic number, all of whose conjugates lie on $|z-\gamma|^2 = \Omega$, where $\gamma \in \mathbf{Q}$ and Ω is a positive real number. Looking at the constant term of the minimal polynomial of $\beta - \gamma$ as in [3, §2], we find that $\Omega^K \in \mathbf{Q}$ for some positive integer K. Choose K as small as possible. Instead of β it is more convenient for the moment to consider $(\beta-\gamma)^K$, all of whose conjugates lie on $|z|^2 = \Omega^K$.

We now proceed as in the case of γ not totally real (though now everything is much simpler). We define the group of linear transformations

$$\mathfrak{H} = \{1, z \mapsto \Omega^K/z\}$$

of order 2. The corresponding automorphic function is now $H(z) = \sum_{A \in \mathfrak{H}} Az = (z^2 + \Omega^K)/z$. It is clear that $H(z) = \alpha$ has its zeros on $|z|^2 = \Omega^K$ if and only if $\alpha \in \Delta$, where $\Delta = [-2\Omega^{K/2}, 2\Omega^{K/2}]$. We then obtain, in a similar way to Theorem 1:

Theorem 3. *Let $\gamma \in \mathbf{Q}$ and suppose that there exists a positive real number Ω such that the circle $|z-\gamma|^2 = \Omega$ contains a set of conjugate algebraic numbers. Then there is a positive integer K such that $\Omega^K \in \mathbf{Q}$.*

Conversely, suppose that $\gamma \in \mathbf{Q}$, $\Omega > 0$ and that $\Omega^K \in \mathbf{Q}$ for some positive integer K. Choose K to be the smallest positive integer with this property. Let α be a totally real algebraic number, all of whose conjugates α_i lie in Δ. Define l as in Theorem 1. Then the condition

$$P(z)^l = \prod_i \left((z-\gamma)^{2K} + \Omega^K - \alpha_i(z-\gamma)^K\right) \tag{74}$$

defines a monic polynomial $P(z) \in \mathbf{Q}[z]$, which is irreducible over $\mathbf{Q}$, and has all its zeros on $|z-\gamma|^2 = \Omega$. Furthermore, the minimal polynomial of any algebraic number, all of whose conjugates lie on $|z-\gamma|^2 = \Omega$, must be of the form $P(z)$, defined by (74), for some totally real α having all its conjugates in Δ.

Proof. It is sufficient to take $\gamma = 0$. We have already proved the first assertion. To prove the second one, let Ω and K be as stated in the theorem. Write $a = \Omega^K$. For $l = 2$, $\alpha_i = \pm 2\sqrt{a}$, and we have $P(z) = z^K \mp \sqrt{a}$ or $z^{2K} - a$, according as $\sqrt{a} \in \mathbf{Q}$ or $\sqrt{a} \notin \mathbf{Q}$. The irreducibility of $P(z)$ over $\mathbf{Q}$ is a consequence of the minimality of K.

Suppose now that $l = 1$. The zeros of $P(z)$ lie on $|z|^2 = \Omega$, and none of them is real. To prove that $P(z)$ is irreducible over $\mathbf{Q}$, let $G(z)$ be a monic polynomial ($\neq 1$) dividing $P(z)$ in $\mathbf{Q}[z]$. Following Robinson [3, §2], we can conclude that $G(z) = G_0(z^K)$, say. Hence $G_0(x)$ divides $\prod_i (x^2 - \alpha_i x + a)$, which is obviously possible only for $G(z) = P(z)$.

Finally, let $\{\beta_j\}$ be a set of conjugate algebraic numbers on the circle $|z|^2 = \Omega$. We want to show that their minimal polynomial is of the form $P(z)$. Now the numbers $(\beta_j^{2K} + a)/\beta_j^K$ form a complete set of conjugate algebraic numbers in Δ. Denote them by α_i, each one being counted only once. Clearly the polynomial $P(z)$ corresponding to these α_i is the required minimal polynomial.

Using Theorem 3 we give another proof of

Theorem 4 (Robinson [3]). *Let* $\gamma = S/q$, *where* $S, q \in \mathbf{Z}, q > 0$, $(S, q) = 1$. *Assume that the circle* $|z - \gamma|^2 = \Omega$ *contains at least one set of conjugate algebraic integers. Then one of the following conditions holds:*

(i) $q = 1$ *and* $\Omega^K \in \mathbf{Z}$ *for some integer* $K \geqq 1$,

(ii) $q \geqq 2$ *and* $q(\Omega - \gamma^2) \in \mathbf{Z}$,

(iii) $q = 2, \Omega \notin \mathbf{Q}$, *and* $4(\Omega^2 - 1/16) \in \mathbf{Z}$.

Conversely, assume that one of these conditions is satisfied for $\Omega > 0$. *Then there are infinitely many sets of conjugate algebraic integers lying on* $|z - \gamma|^2 = \Omega$ *if and only if either* (i) *holds, or* $\Omega > q^2$ *and* (ii) *or* (iii) *holds.*

Proof. Let $|z - \gamma|^2 = \Omega$ contain at least one set of conjugate algebraic integers. We know from Theorem 3 that $\Omega^K \in \mathbf{Q}$ for some (minimal) $K \geqq 1$, and that for some $\alpha \in \Delta$

$$(z - \gamma)^{2K} + \Omega^K - \alpha(z - \gamma)^K \in \mathbf{A}[z]\,. \tag{75}$$

Assume first that $\Omega \in \mathbf{Q}$, so $K = 1$. Then the left-hand side of (75) becomes $z^2 - (\alpha + 2\gamma)z + \Omega - \gamma^2 + \gamma(\alpha + 2\gamma)$. Hence $q(\Omega - \gamma^2) \in \mathbf{Z}$ and α is determined mod q by

$$\alpha + 2\gamma \in \mathbf{A}\,,\ S(\alpha + 2\gamma) + q(\Omega - \gamma^2) \equiv 0 \mod q. \tag{76}$$

Thus (i) or (ii) holds in this situation.

Now assume that $\Omega \notin \mathbf{Q}$, so $K \geqq 2$. If $q = 1$, i.e. $\gamma \in \mathbf{Z}$, then (75) implies first $\alpha \in \mathbf{A}$ and then $\Omega^K \in \mathbf{A}$. Hence (i) holds. Suppose therefore that $q \geqq 2$. We look at the coefficients of z and z^2 in (75), and obtain

$$(-1)^K K q^K S^{K-1} \alpha - 2K S^{2K-1} \equiv 0 \qquad \mod q^{2K-1}\,, \tag{77}$$

$$(-1)^K K(K - 1) q^K S^{K-2} \alpha - 2K(2K - 1) S^{2K-2} \equiv 0 \mod 2q^{2K-2}\,. \tag{78}$$

Eliminating α we get $q^{2K-2} | 2K^2$. This is impossible for $K \geqq 4$ as $2^{2K-2} > 2K^2$. Also, for $K = 3$, we cannot have $q^4 | 18$. So $K = 2$, and $q^2 | 8$, whence $q = 2$. Looking at the constant term in (75), we have $-4S^2\alpha + S^4 + 16\Omega^2 \equiv 0 \mod 16$. From (78), $\alpha - \frac{1}{2} \in \mathbf{A}$. As $S^2 \equiv 1 \mod 8$, $S^4 \equiv 1 \mod 16$, we obtain

$$\alpha - \tfrac{1}{2} \equiv 4(\Omega^2 - 1/16) \mod 4\,. \tag{79}$$

Hence (iii) holds.

Conversely, assume that one of the conditions (i), (ii), (iii) is true. Then choosing α such that $\alpha \in \mathbf{A}$ in case (i), α satisfies (76) in case (ii), and α satisfies (79) in case (iii), we can easily verify that (75) holds. Now all α of this kind are of the form $\alpha = \alpha_0 + w\xi$, where $\xi \in \mathbf{A}$, α_0 is a fixed rational, and $w = 1, q, 4$ in cases (i), (ii), (iii), respectively. We thus have a one-to-one correspondence between algebraic integers on $|z - \gamma|^2 = \Omega$ and algebraic numbers of the form $\alpha_0 + w\xi$, all of whose conjugates lie in Δ. The length of Δ is $|\Delta| = 4\Omega^{K/2}$. In cases (ii), (iii) we cannot have $|\Delta| = 4w$, and the result follows from Lemma 21. In case (i) equality can occur, but taking $\alpha_0 = 0$, we see that the additional condition in Lemma 21 is satisfied. In this case we always have $|\Delta| \geqq 4$. This completes the proof of Theorem 4.

The case when γ is irrational and totally real, which was treated in [1], can also be dealt with using similar methods. Lemma 1 applies also to this case, and using it we can show that the corresponding group $\mathfrak{H}$ of linear transformations is a four-group. We can again define $H(z) = \sum_{A \in \mathfrak{H}} Az$, and this turns out to be the rational function $f(z)/g(z)$ in equation (5) of [1]. Thus the construction of conjugate algebraic numbers on $|z - \gamma|^2 = \Omega$ is made by essentially the same technique as in the cases we have considered. The methcd of dealing with the integrity conditions in [1] is basically the same we have used here.

11. Examples

1. Our first example shows that, for $n = 3$, the critical case of equality can indeed occur in (13), in addition to (11) and (12.3) holding. For such an example we are able to write down the minimal polynomials of all sets of conjugate algebraic integers on $|z - \gamma|^2 = \Omega^*$.

Take $g(z) = z^3 - (3h + 1)z^2 + (3h^2 + 2h)z - k$, where h and k are suitably chosen integers such that $g(z)$ is irreducible over $\mathbf{Q}$ and has only one real zero. (E.g. take k to be a large prime.) Then $d = q = r = 1$, $\Delta = [6h, 6h + 4]$, $\lambda = 0$. Further $9|E$, so that $\varkappa = 0$. Hence we do have equality in (13), while the other conditions are clearly satisfied. By a well-known theorem of Kronecker, exactly all totally real algebraic integers ξ, all of whose conjugates lie in $[-2, 2]$, are given by $\xi = 2\cos t\pi$, for $t \in \mathbf{Q}$. Since $w = 1$, any set of conjugate algebraic integers on $|z - \gamma|^2 = \Omega^*$ has minimal polynomial of the form

$$P(z)^l = \prod_{\substack{j=0 \\ (j,m)=1}}^{[\frac{1}{2}m]} (U(z) - (6h + 2 + 2\cos(2\pi j/m))V(z)) ,$$

for some positive integer m.

It is also easy to construct similar examples for $d > 1$. One such is given by $g(z) = z^3 - 6z^2 + 9z - 5$.

2. Take $\gamma = \sqrt{m} + (2m + c\sqrt{m})^{\frac{1}{2}}$, where $m, c \in \mathbf{Q}, m > 0, m$ is not a square in $\mathbf{Q}$, and $c > 2\sqrt{m}$. Then γ is a root of $g(z) = z^4 - 6mz^2 - 4mcz + m^2 - mc^2 = 0$. Further $d = 16m > 0$, c has the meaning (4), and (8) holds. From Lemma 11 and (43), we find that the requirements in Theorem 1, ensuring the existence of infinitely many sets of conjugate algebraic numbers on $|z - \gamma|^2 = \Omega^*$, are satisfied for this γ with $n = 4$. As $s_1 = 0$, the integrity conditions take a much simplified form, and it is not hard to see that the following is true: There is no set of conjugate algebraic integers on $|z - \gamma|^2 = \Omega^*$ unless $m \in \mathbf{Z}$, $r^6 | m$. If these conditions are satisfied, then there are, in fact, infinitely many such sets.

3. In spite of the previous examples, it is not necessary that γ be an algebraic integer in order for the circle $|z - \gamma|^2 = \Omega^*$ to contain infinitely many sets of conjugate algebraic integers. For instance, we can take γ to be the relevant root of

$$z^3 - t(z^2 + z + \tfrac{1}{3}) = 0 \quad \text{for} \quad n = 3$$

or

$$z^4 - t(z^2 + z + \tfrac{1}{2})(z + \tfrac{1}{2}) = 0 \quad \text{for} \quad n = 4 ,$$

where t is a positive rational number such that the ratio of t and its denominator is at least n^2.

Department of Mathematics
University of Turku
Finland

References

[1] Ennola, V.: Conjugate algebraic integers on a circle with irrational center. Math. Z. 134, 337—350 (1973).

[2] Robinson, R. M.: Intervals containing infinitely many sets of conjugate algebraic integers. In: Studies in Mathematical Analysis and Related Topics: Essays in Honor of George Pólya, pp. 305—315. Stanford: Stanford University Press 1962.

[3] —»— Conjugate algebraic integers on a circle. Math. Z. 110, 41—51 (1969).

[4] Sansone, G. and Gerretsen, J.: Lectures on the theory of functions of a complex variable II. Geometric theory. Groningen: Wolters — Noordhoff 1969.

Printed June 1974