Conspectus materiae tomi XL, fasciculi 4

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange | Address of the Editorial Board and of the exchange | Die Adresse der Schriftleitung und des Austausches | Адрес редакции и книгообмена

ACTA ARITHMETICA

ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

ISBN 83-01-02438-0 ISSN 0065-1036

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

Conjugate algebraic numbers on conics

by

C. J. Smyth (Townsville)

0. Introduction. The aim of this paper is to find all algebraic numbers which lie with their conjugates on a conic. One consequence of our main results (Theorems 2, 3, and 4) is the following:

Theorem 1. (1) *If a parabola contains infinitely many sets of conjugate algebraic numbers, its focus is rational.*

(2) *If an ellipse or hyperbola contains infinitely many sets of conjugate algebraic numbers, its foci are either both rational, or are conjugate quadratic irrationals.*

As an immediate

Corollary. *No ellipse or hyperbola with irrational centre contains infinitely many sets of conjugate algebraic numbers.*

In 1969 Robinson [4] conjectured that no circle with irrational centre contained infinitely many sets of conjugate algebraic integers. Although Ennola [1] showed that this conjecture is false, we see that the corresponding result for ellipses and hyperbolas is true. (Throughout the paper, ellipses are assumed to be non-circular.)

Since the theory for circles has been covered ([1], [2], [3], [4]), we devote our attention to parabolas, ellipses and hyperbolas.

1. Notation. Let $\boldsymbol{U}$ denote the unit circle $|z| = 1$. Let $\mathscr{C}$ be the conic under consideration; it can be either a parabola ($\mathscr{C} = \mathscr{P}$), an ellipse ($\mathscr{C} = \mathscr{E}$) or a hyperbola ($\mathscr{C} = \mathscr{H}$).

We let C be a real number which is the focus of the parabola if $\mathscr{C} = \mathscr{P}$, otherwise the centre of the conic. The parabola $\mathscr{P}(C, F)$ with equation $y^2 = F(x + \frac{1}{4}F - C)$, $F > 0$ has focus C and is parametrized by

$$z(t) = x + iy = \frac{1}{F}(t + \tfrac{1}{2}iF)^2 + C. \tag{1.1}$$

We also let $R > 0$, $\varepsilon = \pm 1$ be fixed, and $B > 1$ ($\mathscr{C} = \mathscr{E}$), $|B| = 1$, $B^2 \neq 1$ ($\mathscr{C} = \mathscr{H}$). Then for t on $\boldsymbol{U}$ ($\mathscr{C} = \mathscr{E}$), or t real ($\mathscr{C} = \mathscr{H}$)

$$z(t) = C + R\left(B^{1/2}t + \varepsilon(B^{1/2}t)^{-1}\right) \tag{1.2}$$

parametrizes a certain ellipse $\mathscr{E}(C, R, B, \varepsilon)$ or hyperbola $\mathscr{H}(C, R, B, \varepsilon)$ with centre C. Note that the conic is the same if $B^{1/2}$ is replaced by $-B^{1/2}$, the sign being incorporated into t. Unless otherwise stated, we will however always assume that a square root is uniquely defined to have argument in $[0, \pi)$.

The above ellipse and hyperbola have equations

$$\frac{(x-C)^2}{R^2(B+B^{-1}+2\varepsilon)} + \frac{y^2}{R^2(B+B^{-1}-2\varepsilon)} = 1$$

and

$$\frac{(x-C)^2}{R^2(2+B+B^{-1})} - \frac{y^2}{R^2(2-B-B^{-1})} = \varepsilon,$$

respectively. Note that the ellipse is non-circular, but that the equations are otherwise completely general, given that they must be symmetric about the real axis. The foci of the above conics are at $C \pm 2R\varepsilon^{1/2}$.

Let T_k denote the Tchebycheff polynomial of degree k, so that

$$T_k(t+t^{-1}) = t^k + t^{-k}.$$

Let $\mathscr{A}(I)$ be the set of those algebraic numbers which lie with their conjugates in a subset I of the reals $\boldsymbol{R}$. Also define the following sets of algebraic numbers:

$S_{\mathscr{P}} = \{F: F > 0$ and all other conjugates of F are $< 0\}$,

$S_{\mathscr{E}} = \{B: B > 1$ and all conjugates of B not equal to $B^{\pm 1}$ are on $\boldsymbol{U}\}$,

$S_{\mathscr{H}} = \{B: B$ is on $\boldsymbol{U}$, $B^2 \neq 1$, and all conjugates of B except $B^{\pm 1}$ are real$\}$.

For B algebraic, let $k(B)$ be the least positive integer k such that B^k has no conjugate of the form $\varrho B^{\pm k}$ for $\varrho \neq 1$ a root of unity.

2. The main theorems.

THEOREM 2 (Parabolas). *Let z be an algebraic number of degree at least 9 which lies with its conjugates on a parabola $\mathscr{P}(C, F)$. Then*

(1) *C is rational, and $F \in S_{\mathscr{P}}$;*

(2) *z has a conjugate of the form*

$$\frac{1}{4}\left(\alpha^{1/2} + \sum_{j=1}^{n} (-F_j)^{1/2}\right)^2 + C \tag{2.1}$$

where $F = F_1, \ldots, F_n$ are the conjugates of F, and $\alpha \in \mathscr{A}([0, \infty))$. Conversely, given C rational, $F \in S_{\mathscr{P}}$ and $\alpha \in \mathscr{A}([0, \infty))$, the algebraic number given by (2.1) lies with all its conjugates on $\mathscr{P}(C, F)$.

It is not difficult to check that z has degree $2^n \deg \alpha$ ($\alpha \neq 0$), 2^{n-1} ($\alpha = 0$). It may be that the 9 in this theorem can be replaced by 5. It cannot be reduced any further, since it is easy to find such z of degree 4 on a parabola with non-rational focus.

THEOREM 3 (Ellipses). *Let z be an algebraic number of degree at least 25, which lies with its conjugates on an ellipse $\mathscr{E}(C, R, B, \varepsilon)$. Then*

(1) *C and R^2 are rational, and $B^{k(B)} \in S_{\mathscr{E}}$.*

(2) *Defining*

$$z^* = T_{k(B)}\left(\frac{(z-C)\,\varepsilon^{1/2}}{R}\right) \tag{2.2}$$

then z^* and all its conjugates lie on $\mathscr{E}(0, 1, B^{k(B)}, 1)$.

(3) *In view of (2) we need only consider the special case $C = 0$, $R = 1$, $k(B) = 1$, $\varepsilon = 1$. In this situation z has a conjugate of the form $\theta + \theta^{-1}$, where*

$$\theta = \tfrac{1}{2}\left(\alpha + (\alpha^2-4)^{1/2}\right)\left(\prod_{j=1}^{n} B_j\right)^{1/2}. \tag{2.3}$$

Here $B = B_1$ and either B is rational and $n = 1$, or $B_1^{\pm 1}, B_2^{\pm 1}, \ldots, B_n^{\pm 1}$ are the conjugates of B. Also $\alpha \in \mathscr{A}([-2, 2])$. Conversely, let $B \in S_{\mathscr{E}}$ and $\alpha \in \mathscr{A}([-2, 2])$. Then

(4) *$z = \theta + \theta^{-1}$, where θ is given by (2.3), lies with its conjugates on the ellipse $\mathscr{E}(0, 1, B, 1)$.*

(5) *Let C, R and B satisfy (1), put $k = k(B)$ and use (4) to define z^* on $\mathscr{E}(0, 1, B^k, 1)$. Then if z is a root of (2.2), z lies with all its conjugates on $\mathscr{E}(C, R, B, \varepsilon)$.*

THEOREM 4 (Hyperbolas). *Let z be an algebraic number of degree at least 25, which lies with all its conjugates on a hyperbola $\mathscr{H}(C, R, B, \varepsilon)$. Then*

(1) *C and R^2 are rational, $k(B) = 1$ or 2, and $B^{k(B)} \in S_{\mathscr{H}}$.*

(2) *If $B \neq \pm i$ and z^* is defined by (2.2), then z^* and all its conjugates lie on the hyperbola $\mathscr{H}\left(0, 1, (\varepsilon B)^{k(B)}, 1\right)$. Further if $k(B) = 2$ then the parameters of z^* and its conjugates are all positive.*

(3) *If $B = \pm i$, then $z^* = (z-C)^2$ and all its conjugates lie on the line $\mathrm{Re}\, z^* = 2\varepsilon R^2$, and*

$$z^* = 2\varepsilon R^2 + i\alpha \quad \text{for some } \alpha \in \mathscr{A}(\boldsymbol{R}). \tag{2.4}$$

(4) *In view of (2), (3) we need only consider the special case $B \neq \pm i$, $C = 0$, $R = 1$, $k(B) = 1$, $\varepsilon = 1$. In this situation z has a conjugate of the form $\theta + \theta^{-1}$, where θ is given by (2.3), with $B = B_1$, and $B_1^{\pm 1}, \ldots, B_n^{\pm 1}$ the conjugates of B, and $\alpha \in \mathscr{A}\left((-\infty, -2] \cup [2, \infty)\right)$.*

Conversely, let $B \in S_{\mathscr{H}}$ and $\alpha \in \mathscr{A}\left((-\infty, -2] \cup [2, \infty)\right)$. Then

(5) $z = \theta + \theta^{-1}$, *where* θ *is given by* (2.3), *lies with all its conjugates on* $\mathscr{H}(0, 1, B, 1)$.

(6) *Let* C, R *and* B *satisfy* (1), $B \neq \pm i$, *and use* (5) *to define* z^* *on* $\mathscr{H}\{0, 1, (\varepsilon B)^{k(B)}, 1\}$, *with* z^* *and all its conjugates having positive parameter. Then if* z *is a root of* (2.2), z *lies with all its conjugates on* $\mathscr{H}(C, R, B, \varepsilon)$.

(7) *Let* C, R *and* B *satisfy* (1), $B = \pm i$, *and* $\alpha \in \mathscr{A}(\boldsymbol{R})$. *Then*

$$z = C + (2\varepsilon R^2 + i\alpha)^{1/2}$$

lies with all its conjugates on $\mathscr{H}(C, R, B, \varepsilon)$.

Again perhaps the lower bound of 25 on the degree of z in Theorems 3 and 4 can be reduced to 7. It is easy to find z of degree 6 lying with its conjugates on an ellipse or hyperbola with irrational centre.

The proofs of Theorems 2, 3 and 4 are contained in Sections 4 to 7, and of Theorem 1 in Section 8.

3. In this section we present lemmas needed for the proofs of the theorems.

LEMMA 1. *Let* $\alpha, \alpha_2, \alpha_3$ *be distinct conjugate algebraic numbers. Then*

(a) $\alpha_2 \pm \alpha_3 \neq \pm 2\alpha$,

(b) *If*

$$\alpha_2 \alpha_3^{\delta} = \alpha^{2\varepsilon}, \tag{3.1}$$

where $\delta, \varepsilon = \pm 1$, *then* $\alpha_2^k = \alpha^{ek}$ *for some positive integer* k.

Proof. (a) If $\alpha_2 \pm \alpha_3 = \pm 2\alpha$, then by applying a suitable automorphism which maps α to a conjugate α_4 with maximal absolute value, we have $\alpha_5 \pm \alpha_6 = \pm 2\alpha_4$ for some conjugates $\alpha_5 \neq \alpha_6$ of α. But $|\alpha_5 \pm \alpha_6| < 2|\alpha_4|$, a contradiction.

(b) Use Dirichlet's Theorem to find a $k > 0$ such that

$$\max_j(|\arg \beta_j|) < \pi/4 \tag{3.2}$$

where $\beta = \alpha^k$ and the β_j are the conjugates of β. Here we take $\arg \beta_j \in (-\pi, \pi]$. Now order the complex numbers by $\gamma < \gamma'$ if $|\gamma| < |\gamma'|$ or if $|\gamma| = |\gamma'|$ and $\arg \gamma < \arg \gamma'$. With this ordering, choose the conjugate β_4 of β and $\eta = \pm 1$ such that among all conjugates of β and β^{-1}, β_4^{η} is maximal. Then applying a suitable automorphism τ to (3.1) to map $\beta \mapsto \beta_4$ we get

$$\beta_5^{\varepsilon\eta} \beta_6^{\delta\varepsilon\eta} = \beta_4^{2\eta} \tag{3.3}$$

for some conjugates $\beta_5 = \tau(\alpha_2^k)$, $\beta_6 = \tau(\alpha_3^k)$ of β.

Since $|\beta_5^{\varepsilon\eta}|, |\beta_6^{\delta\varepsilon\eta}| \leqslant |\beta_4^{\eta}|$, $|\beta_5^{\varepsilon\eta}| = |\beta_6^{\delta\varepsilon\eta}| = |\beta_4^{\eta}|$. Also, using (3.2),

$$\arg \beta_5^{\varepsilon\eta} + \arg \beta_6^{\delta\varepsilon\eta} = 2 \arg \beta_4^{\eta}$$

so, as $\arg \beta_5^{\varepsilon\eta}, \arg \beta_6^{\delta\varepsilon\eta} \leqslant \arg \beta_4^{\eta}$, in fact $\arg \beta_5^{\varepsilon\eta} = \arg \beta_6^{\delta\varepsilon\eta} = \arg \beta_4^{\eta}$. Hence $\beta_5 = \beta_6^{\delta} = \beta_4^{\varepsilon}$, so, applying τ^{-1}, $\alpha_2^k = \alpha^{ek}$ as required.

COROLLARY 1. *Any algebraic number* z *which lies with its conjugates on a line* $\mathrm{Re}\, z = \text{constant}$ *must be of the form* $q + i\alpha$, *where* q *is rational, and* α *is totally real.*

Proof. Let $q = \frac{1}{2}(z + \bar{z})$. For any conjugate q' of q, choose an automorphism which maps $q \to q'$. Then $q' = \frac{1}{2}(z_2 + z_3)$ say, so $\mathrm{Re}\, q' = \frac{1}{2}(\mathrm{Re}\, z_2 + \mathrm{Re}\, z_3) = q$. Hence $q = \frac{1}{2}(q' + \bar{q}')$. By Lemma 1(a), $q' = \bar{q}' = q$, so q is rational.

LEMMA 2. *Suppose we are given* $n-1$ *real numbers* $d_2, \ldots, d_n$ *which are linearly independent over the rationals* $\boldsymbol{Q}$. *Suppose further that* $\mathscr{T}$ *is a finite real set with the following properties*:

(1) $t \in \mathscr{T} \Rightarrow -t \in \mathscr{T}$,

(2) $t \in \mathscr{T} \Rightarrow$ *exactly one of* $t \pm d_i \in \mathscr{T}$ $(i = 2, \ldots, n)$.

Then $\mathscr{T}$ *is a union of disjoint sets* $\mathscr{T}_a$, *where*

$$\begin{cases} \mathscr{T}_a = \left\{t \mid t = \varepsilon_1\left(a + \frac{1}{2}\sum_{i=2}^{n} \varepsilon_i d_i\right),\ \varepsilon_i = \pm 1\ (i = 1, \ldots, n)\right\}\ (a \neq 0), \\ \mathscr{T}_0 = \left\{t \mid t = \frac{1}{2}\sum_{i=2}^{n} \varepsilon_i d_i,\ \varepsilon_i = \pm 1\ (i = 2, \ldots, n)\right\}. \end{cases} \tag{3.4}$$

Further $|\mathscr{T}_a| = 2^n$ $(a \neq 0)$ *and* $|\mathscr{T}_0| = 2^{n-1}$.

Proof. Say $t \sim t'$ if $t - t' = \pm d_i$ for some i, or $t' = \pm t$. Then $\sim$ generates an equivalence relation on $\mathscr{T}$. Let $\mathscr{T}^{\sim}$ be one of the equivalence classes, and fix $t \in \mathscr{T}^{\sim}$. Define $d_i' = \pm d_i$, choosing the sign by the property $t + d_i' \in \mathscr{T}$ $(i = 2, \ldots, n)$. We first claim that all elements of $\mathscr{T}^{\sim}$ can now be written in the form $\pm\left(t + \sum_{i=2}^{n} \mu_i d_i'\right)$, where $\mu_i = 0$ or 1. To show this, we assume the contrary. This implies that there is a least integer $p \geqslant 1$ such that for some integer j and set $I \subset \{2, \ldots, n\} \setminus \{j\}$ with $|I| = p$, $t + \sum_{i \in I} d_i' - d_j' \in \mathscr{T}^{\sim}$. Choose and fix $k \in I$, and denote $t + \sum_{i \in I \setminus \{k\}} d_i' + \lambda d_k' + \mu d_j'$ by (λ, μ). Then by our assumptions $(0, 0)$, $(1, 0)$, $(0, 1)$ and $(1, -1) \in \mathscr{T}^{\sim}$. Now by property (2) of $\mathscr{T}$,

$$(\lambda, \mu) \in \mathscr{T}^{\sim} \Rightarrow \text{exactly one of } (\lambda, \mu \pm 1) \in \mathscr{T}^{\sim} \tag{3.5}$$

$$\text{and} \Rightarrow \text{exactly one of } (\lambda \pm 1, \mu) \in \mathscr{T}^{\sim}. \tag{3.6}$$

So $(0, -1) \notin \mathscr{T}^{\sim}$ by (3.5) and so $(2, -1) \in \mathscr{T}^{\sim}$ by (3.6).

We now assert that $(l, -l)$ and $(l+1, -l) \in \mathscr{T}^{\sim}$ for all $l \geqslant 0$. We have already proved this for $l = 0, 1$, and the truth for all l follows by induction, using (3.5) and (3.6).

By the $\boldsymbol{Q}$-independence of the d_i, the $(l, -l)$ are all distinct. This contradicts the finiteness of $\mathscr{T}$. Hence all elements of $\mathscr{T}^{\sim}$ are of the form

$\pm\left(a+\frac{1}{2}\sum_{i=2}^{n}\varepsilon_i'd_i'\right)$, where $\varepsilon_0' = \pm 1$ and $a = t+\frac{1}{2}\sum_{i=2}^{n} d_i'$. Finally put $\varepsilon_i'd_i' = \varepsilon_i d_i$ and we obtain (3.4) for $a \neq 0$.

It remains only to see whether any of the elements $\pm\left(a+\sum \varepsilon_i d_i\right)$ can be equal. Now all the $a+\sum \varepsilon_i d_i$ are clearly distinct by $\boldsymbol{Q}$-independence of the d_i. However, it may be that

$$a+\tfrac{1}{2}\sum \varepsilon_i d_i = -\left(a+\tfrac{1}{2}\sum \varepsilon_i'' d_i\right) \tag{3.7}$$

for some ε_i, ε_i'' $(i = 2, \ldots, n)$. But then for any j

$$a+\tfrac{1}{2}\sum_{i\neq j} \varepsilon_i d_i - \tfrac{1}{2}\varepsilon_j d_j = -\left\{a+\tfrac{1}{2}\sum_{i\neq j} \varepsilon_i'' d_i + \tfrac{1}{2}(\varepsilon_j''+2\varepsilon_j)d_j\right\}.$$

Since the left term belongs to $\mathscr{T}^{\sim}$ so does the right, and hence $\varepsilon_j''+2\varepsilon_j = \pm 1$, or $\varepsilon_j'' = -\varepsilon_j$. Hence $2a = 0$, $a = 0$ from (3.7). This completes the proof of the lemma.

The above result can easily be put into multiplicative form, which gives the following.

Corollary 2. *Suppose we are given $n-1$ non-zero numbers $d_2, \ldots, d_n$ either all on $\boldsymbol{U}$, or all real, and multiplicatively independent. Suppose further that $\mathscr{T}$ is a finite set on $\boldsymbol{U}$ if the d_i are on $\boldsymbol{U}$, and real if the d_i are real, with the following properties:*

(1) $t \in \mathscr{T} \Rightarrow 1/t \in \mathscr{T}$,

(2) $t \in \mathscr{T} \Rightarrow$ *exactly one of* $td_i^{\pm 2} \in \mathscr{T}$ $(i = 2, \ldots, n)$.

Then $\mathscr{T}$ is a union of disjoint sets $\mathscr{T}_a$, where for $a \neq \pm 1$

$$\mathscr{T}_a = \left\{t \mid t = a^{\varepsilon_1}\prod_{i=2}^{n} d_i^{\varepsilon_i},\ \varepsilon_i = \pm 1\ (i = 1, \ldots, n)\right\}$$

and for $a = \pm 1$

$$\mathscr{T}_a = \left\{t \mid t = a\prod_{i=2}^{n} d_i^{\varepsilon_i},\ \varepsilon_i = \pm 1\ (i = 2, \ldots, n)\right\}.$$

Further $|\mathscr{T}_a| = 2^n$ $(a \neq \pm 1)$ and $|\mathscr{T}_{\pm 1}| = 2^{n-1}$.

The proof is almost identical to that of the lemma, except that at the end when one gets (3.7) implies $2a = 0$, $a = 0$ the multiplicative equivalent is $a^2 = 1$, $a = \pm 1$.

Lemma 3. *The polynomial ax^2+bx+c, where $a \neq 0$, has a real (resp. imaginary) zero iff $\varepsilon_0 = 1$ (resp. -1) and*

$$(a\bar{c}-\bar{a}c)^2-(\varepsilon_0 a\bar{b}-\bar{a}b)(b\bar{c}-\varepsilon_0\bar{b}c) \tag{3.8}$$

is zero. It has two real (resp. imaginary) zeros iff any two (and hence all three) of $ac-\bar{a}c$, $\varepsilon_0 a\bar{b}-\bar{a}b$ and $b\bar{c}-\varepsilon_0\bar{b}c$ are zero.

Proof. The expression (3.8) is the resultant of ax^2+bx+c and $\bar{a}x^2+\bar{b}x+\bar{c}$ if $\varepsilon_0 = 1$, and of $-ax^2+ibx+c$ and $-\bar{a}x^2-i\bar{b}x+\bar{c}$ if $\varepsilon_0 = -1$. The second part is trivial.

Lemma 4. (a) *Let $F \in S_{\mathscr{D}}$, with conjugates $F = F_1, F_2, \ldots, F_n$, $n \geqslant 2$. Then $F_2^{1/2}, \ldots, F_n^{1/2}$ are linearly independent over the rationals.*

(b) *Let $B \in S_{\mathscr{E}}$ or $S_{\mathscr{H}}$ with conjugates $B = B_1, B_1^{-1}, B_2^{\pm 1}, \ldots, B_n^{\pm 1}$, $n \geqslant 2$. Then $B_2, \ldots, B_n$ are multiplicatively independent.*

Proof. (a) Suppose $\sum_{j=2}^{n} q_j F_j^{1/2} = 0$ for some $q_2, \ldots, q_n$ rational, and q_2 (say) non-zero. Choose an automorphism τ which maps $F_2 \mapsto F$. Then $\tau(q_2F_2^{1/2})$ is real and non-zero, while $\tau\left(\sum_{j=3}^{n} q_j F_j^{1/2}\right)$ is imaginary.

(b) First note that since $n \geqslant 2$, B is not a root of unity. Now suppose $B_2^{m_2} \ldots B_n^{m_n} = 1$ for some integers $m_2, \ldots, m_n$ with m_2 (say) non-zero. Map $B_2 \mapsto B$ as in (a) above. Then $\tau(B_2^{m_2})$ is not ± 1 and is real ($\mathscr{C} = \mathscr{E}$) or on $\boldsymbol{U}$ ($\mathscr{C} = \mathscr{H}$), while $\tau(B_3^{m_3} \ldots B_n^{m_n})$ is on $\boldsymbol{U}$ ($\mathscr{C} = \mathscr{E}$) or real ($\mathscr{C} = \mathscr{H}$).

4. In the next four sections we prove Theorems 2, 3, and 4. We start by considering the three proofs concurrently, though we shall separate them after this section. In Sections 4, 5, 6 we assume that z lies with its conjugates on $\mathscr{C}$, and, in time-honoured fashion, deduce enough consequences from this fact to be able, in Section 7, to show conversely that these consequences imply that $\mathscr{C}$ contains complete sets of conjugate algebraic numbers.

We also need to assume that the degree ∂z of z is at least 9 ($\mathscr{C} = \mathscr{P}$), and at least 25 ($\mathscr{C} = \mathscr{E}$, $\mathscr{H}$). The equation of $\mathscr{C}$ can be written in the form

$$z^2+\bar{z}^2+Ez\bar{z}+2F(z+\bar{z})+G = 0, \tag{4.1}$$

where E, F, and G are real. The conjugates of z determine E, F and G, which are therefore algebraic. Equation (4.1) represents a parabola when $E = -2$ and $F \neq 0$, an ellipse when $|E| > 2$ and $4F^2-G(E+2) > 0$, and a hyperbola when $|E| < 2$ and $4F^2 \neq G(E+2)$. For $\mathscr{C} = \mathscr{P}$ we shall in fact assume that $F > 0$. If $F < 0$ we simply replace z by $-z$. For $\mathscr{C} = \mathscr{P}$, G is given in terms of the parameters F, C by $G = F(F-4C)$. For $\mathscr{C} = \mathscr{E}, \mathscr{H}$, $E = -\varepsilon\varepsilon^*(B+B^{-1})$, where $\varepsilon^* = 1$ ($\mathscr{C} = \mathscr{E}$), $= \varepsilon$ ($\mathscr{C} = \mathscr{H}$), $F = -\frac{1}{2}(E+2)C$, $G = -2CF+\varepsilon R^2(E^2-4)$.

Now (4.1) holds when z is replaced by any of its conjugates. On applying an automorphism $\tau\colon \mathscr{F} \to \mathscr{F}$ to (4.1) we obtain say

$$z_i^2+z_{i'}^2+E'z_iz_{i'}+2F'(z_i+z_{i'})+G' = 0 \tag{4.2}$$

for each conjugate z_i of z. Here $\mathscr{F}$ is a suitable large field, say the smallest normal extension of $\boldsymbol{Q}$ containing z, E, F, G, C, R and B,

$$z_{i'} = \tau\sigma\tau^{-1}z_i, \tag{4.3}$$

where $\sigma: \mathscr{F} \to \mathscr{F}$ is the complex conjugate automorphism, and $'$ denotes application of τ, e.g. $E' = \tau E$, etc.

We now fix t to be the parameter of $z = z_1$, and u to be the parameter of z_1', in all three cases $\mathscr{C} = \mathscr{P}, \mathscr{E}, \mathscr{H}$. We put

$$s = \begin{cases} t+u & (\mathscr{C} = \mathscr{P}), \\ (tu)^{1/2} & (\mathscr{C} = \mathscr{E}, \mathscr{H}); \end{cases} \qquad d = \begin{cases} t-u & (\mathscr{C} = \mathscr{P}), \\ t/s & (\mathscr{C} = \mathscr{E}, \mathscr{H}), \end{cases} \tag{4.4}$$

where $\arg(tu)^{1/2} \in [0, \pi)$.

Note that then $t = sd, u = sd^{-1}$ $(\mathscr{C} = \mathscr{E}, \mathscr{H})$. Next, we substitute the parametrizations (1.1), (1.2) into (4.2). After some tedious manipulating we obtain, using (4.4), for $\mathscr{C} = \mathscr{P}$

$$(d^2+FF')q(s)+\lambda = 0, \tag{4.5}$$

where $q(s) = (s+iF)^2+FF'$, $\lambda = 4F^2F'(C'-C)$, and for $\mathscr{C} = \mathscr{E}, \mathscr{H}$,

$$((d+d^{-1})^2+E'-2)p_2(s)+\mu p_1(s)(d+d^{-1})+\lambda = 0 \tag{4.6}$$

where

$$p_1(s) = B^{1/2}s+\varepsilon B^{-1/2}s^{-1},$$

$$p_2(s) = Bs^2+B^{-1}s^{-2}+\varepsilon E' = (Bs^2-\varepsilon^* B')\big(1-\varepsilon^*(BB's^2)^{-1}\big), \tag{4.7}$$

$$\begin{cases} \mu = (E'+2)(C-C')/R, \\ \lambda = \{(E'+2)(C-C')^2+\varepsilon(R'^2-R^2)(E'^2-4)\}/R^2. \end{cases} \tag{4.8}$$

Note also that

$$(d+d^{-1})^2+E'-2 = (d^2-\varepsilon\varepsilon^* B')(1-d^{-2}\varepsilon\varepsilon^* B'^{-1}). \tag{4.9}$$

For later use we now prove

LEMMA 5. *Let $\mathscr{C} = \mathscr{P}$, $\mathscr{E}$ or $\mathscr{H}$, and $E \neq 0$. Then given z_i, only one conjugate $z_{i'}$ of z satisfies* (4.2).

Proof. On applying the automorphism τ^{-1} to (4.2), we obtain (4.1) with $z, \bar{z}$ replaced by $z_1 = \tau^{-1}z_i, z_{1'} = \tau^{-1}z_{i'}$. Going over to the parametrized form of this equation, namely (4.5) and (4.6), we obtain

$$s(d^2+F^2)(s+2iF) = 0 \qquad (\mathscr{C} = \mathscr{P})$$

and, since $\lambda = \mu = 0$,

$$(d^2-\varepsilon\varepsilon^* B)(1-d^{-2}\varepsilon\varepsilon^* B^{-1})(s^2-\varepsilon^*)\big(1-\varepsilon^*(B^2s^2)^{-1}\big) = 0 \tag{4.10}$$

$$(\mathscr{C} = \mathscr{E}, \mathscr{H})$$

using (4.7) and (4.8). Hence $s = 0$ for $\mathscr{C} = \mathscr{P}$. Since $|s^2| = |d^2| = 1$ and $B > 1$ for $\mathscr{C} = \mathscr{E}$, and $|B| = 1$, B non-real, d^2, s^2 real for $\mathscr{C} = \mathscr{H}$, (4.10) gives $s^2 = \varepsilon^*$, for $\mathscr{C} = \mathscr{E}, \mathscr{H}$, provided $B^2 \neq -1$, i.e. $E \neq 0$. So in all cases $z_{1'}$ is uniquely determined by z_1, so $z_{i'}$ is uniquely determined by z_i.

5. We restrict ourselves to $\mathscr{C} = \mathscr{P}$ for this section. From (4.5) and its complex conjugate, we obtain

$$q(s)\big(\bar{\lambda}+F\bar{F}'\,\bar{q}(s)\big) = \bar{q}(s)\big(\lambda+FF'q(s)\big). \tag{5.1}$$

If $q(s) = 0$, then as s is real, $\mathrm{Rl}(F'^{1/2}) = \pm F^{1/2}$, so that $F'^{1/2}+\bar{F}'^{1/2} = \pm 2F^{1/2}$. This implies $F' = F$, by Lemma 1 (a). Hence $s = 0$, and, from (4.5), $C' = C$.

Now assume $q(s) \neq 0$. Then once s is given, d^2 and hence the unordered pair t, u is uniquely determined by (4.5). Thus for $F' \neq F$ two distinct unordered pairs $\{z_i, z_{i'}\}$ satisfying (4.2) cannot give the same value of $s = t+u$. Since $\partial z \geqslant 9$, there are at least 5 pairs $\{z_i, z_{i'}\}$ satisfying (4.2), and so at least 5 values of s satisfying (5.1). Hence (5.1) is identically 0, and from the coefficients of the powers of s we obtain $\bar{F}' = F'$, and $\lambda = 0$, so $C' = C$.

Since $C' = C$ whether or not $q(s) = 0$, C must be rational, and F totally real. By translating z by C we can now assume that $C = 0$. Since $q(s) \neq 0$ for $F' \neq F$, (4.5) gives

$$d^2 = -FF' \tag{5.2}$$

for $F' \neq F$. So $F' < 0$, and $u = t-d = t \pm (-FF')^{1/2}$. Now, applying Lemma 2 and Lemma 4(a) we obtain

LEMMA 6. *Let $F = F_1 > 0$ have other conjugates $F_2, \ldots, F_n$ all negative, and let $\mathscr{T}$ be the set of parameters of z and its conjugates. Then, for $\mathscr{C} = \mathscr{P}$, $\mathscr{T}$ is the union of disjoint sets $\mathscr{T}_a$, a real, where for $a \neq 0$*

$$\mathscr{T}_a = \Big\{t \mid\ t = \varepsilon_1\Big(a+\tfrac{1}{2}\sum_{i=2}^{n}\varepsilon_i(-FF_i)^{1/2}\Big), \varepsilon_i = \pm 1\ \ (i = 1, \ldots, n)\Big\}$$

and

$$\mathscr{T}_0 = \Big\{t \mid\ t = \tfrac{1}{2}\sum_{i=2}^{n}\varepsilon_i(-FF_i)^{1/2},\ \varepsilon_i = \pm 1\ \ (i = 2, \ldots, n)\Big\}.$$

Note that $|\mathscr{T}_a| = 2^n$ $(a \neq 0)$, and $|\mathscr{T}_0| = 2^{n-1}$.

Further, a straightforward calculation using (1.1) gives

LEMMA 7. *Let $z(t)$ be the conjugate of z with parameter t. Then for $C = 0$*

$$\Sigma_a = \sum_{t \in \mathscr{T}_a} z(t) = \begin{cases} 2^n\Big\{\dfrac{a^2}{F}-\tfrac{1}{4}\mathrm{tr}F\Big\} & (a \neq 0), \\ -2^{n-3}\mathrm{tr}F & (a = 0), \end{cases} \tag{5.3}$$

where $\mathrm{tr}F = F_1+\ldots+F_n$ is rational.

Now if τ_i $(i = 1, \ldots, n)$ are any automorphisms of $\mathscr{F}$ which map $F \mapsto F_i$, then using (4.3)

$$\Sigma_a = \prod_{i=1}^{n}(1+\tau_i\sigma\tau_i^{-1})z(t) \qquad (a \neq 0)$$

where $z(t)$ is any conjugate of z with parameter $t \in \mathscr{T}_a$. Then for any automorphism $\tau\colon \mathscr{F} \to \mathscr{F}$,

$$\tau\Sigma_a = \prod_{i=1}^{n} \big(1+(\tau\tau_i)\sigma(\tau\tau_i)^{-1}\big)\tau\big(z(t)\big) = \prod_{j=1}^{n} (1+\tau_j'\sigma\tau_j'^{-1})\,\tau\big(z(t)\big),$$

where τ_j' $(j = 1, \ldots, n)$ in some order have the same property as the τ_i. Hence $\tau\Sigma_a = \Sigma_{a'}$ for some other real number a'. So Σ_a is totally real. So by (5.3) $\tau(a^2/F) = a'^2/F$, so that a^2/F is totally real, and totally non-negative (of course a'^2 need not be a conjugate of a^2). Putting $\alpha = 4a^2/F$, we see that z has a conjugate of the form $\frac{1}{4}\big(a^{1/2} + \sum_{j=1}^{n} (-F_j)^{1/2}\big)^2$. This proves the first two parts of Theorem 2.

6. In this section we apply to $\mathscr{C} = \mathscr{E}, \mathscr{H}$ similar arguments to those used for $\mathscr{P}$ in the last section. Here, however, the details are more complicated. We have first that

LEMMA 8. *If μ and λ are not both 0, then $s^2 = y$ (say) satisfies the polynomial*

$$L^2 - yR_1R_2 = 0, \tag{6.1}$$

where

$$L = (By^2+\varepsilon E'y+B^{-1})(B^{-1}y^2+\varepsilon\bar{E}'y+B)(\bar{E}'-E') + \\ +\bar{\lambda}y(By^2+\varepsilon E'y+B^{-1}) - \lambda y(B^{-1}y^2+\varepsilon\bar{E}'y+B), \tag{6.2}$$

$$R_1 = \mu^*(By^2+\varepsilon E'y+B^{-1})(\varepsilon y+B) - \mu(B^{-1}y^2+\varepsilon\bar{E}'y+B)(By+\varepsilon), \tag{6.3}$$

$$R_2 = \mu(\bar{E}'-2)(y+\varepsilon B^{-1})(B^{-1}y^2+\varepsilon\bar{E}'y+B) - \mu^*(\varepsilon B^{-1}y+1)\times \\ \times(By^2+\varepsilon E'y+B^{-1})(E'-2) + \mu\bar{\lambda}(y+\varepsilon B^{-1})y - \mu^*\lambda(\varepsilon B^{-1}y+1)y. \tag{6.4}$$

Here $\mu^* = \varepsilon^*\bar{\mu}$.

Proof. Assume μ, λ not both 0. Note that $d+d^{-1}$ is real unless $\mathscr{C} = \mathscr{H}$ and $t/u < 0$, when it is imaginary. So put $\varepsilon_0 = 1$ if $d+d^{-1}$ real, -1 if $d+d^{-1}$ imaginary, so that $\overline{d+d^{-1}} = \varepsilon_0(d+d^{-1})$. Then as (4.6) is not identically 0 as a polynomial in $d+d^{-1}$, we have, by Lemma 3, that

$$[p_2(s)\{\bar{\lambda}+(\bar{E}'-2)\overline{p_2(s)}\} - \overline{p_2(s)}\{\lambda+(E'-2)p_2(s)\}]^2 \\ = [\varepsilon_0 p_2(s)\bar{\mu}\overline{p_1(s)} - \overline{p_2(s)}\mu p_1(s)]\times \\ \times[\mu p_1(s)\{\bar{\lambda}+(\bar{E}'-2)\overline{p_2(s)}\} - \varepsilon_0\bar{\mu}\overline{p_1(s)}\{\lambda+(E'-2)p_2(s)\}].$$

Now $\overline{p_2(s)} = B^{-1}s^3+Bs^{-2}+\varepsilon\bar{E}'$, $\varepsilon_0\overline{p_1(s)} = B^{1/2}\varepsilon^*(\varepsilon B^{-1}s+s^{-1})$, so that we get the required result on substitution.

LEMMA 9. *If (6.1) is identically 0, then $\mu = 0$, and, if $E \neq 0$, $\lambda = 0$.*

Proof. Assume (6.1) is identically 0. Then as the degree $\partial(yR_1R_2)$ is at most 7, $\partial L \leqslant 3$, so $\bar{E}' = E'$, E' is real and

$$L = y[\bar{\lambda}(By^2+\varepsilon E'y+B^{-1}) - \lambda(B^{-1}y^2+\varepsilon E'y+B)]. \tag{6.5}$$

Also R_2 can now be written as

$$R_2 = -B^{-1}(E'-2)R_1 + yR_3$$

where

$$R_3 = \mu\bar{\lambda}(y+\varepsilon B^{-1}) - \mu^*\lambda(\varepsilon B^{-1}y+1). \tag{6.6}$$

So from (6.1)

$$L^2 = y\big(-B^{-1}(E'-2)R_1^2 + yR_1R_3\big). \tag{6.7}$$

Now $\partial\big(L^2+B^{-1}y(E'-2)R_1^2\big) \leqslant 6$, so that, as $E \neq 2$, $\partial R_1 \leqslant 2$. Hence $\mu^*\varepsilon B = \mu$, which, for $\mathscr{C} = \mathscr{E}$ implies $\mu = 0$, as $B > 1$. So $R_1 \equiv R_3 \equiv 0$ for $\mathscr{C} = \mathscr{E}$, and now the coefficient of y^3 in (6.5) gives $\lambda = 0$.

For $\mathscr{C} = \mathscr{H}$, we can conclude only that $\mu = B^{1/2}\tau$, where τ is real. But now $\partial(L^2) \leqslant 5$, $\partial L \leqslant 2$ and $\lambda = B\tau'$ for some τ' real. Hence $\mu\bar{\lambda} = \mu^*\lambda\varepsilon B^{-1}$, so $\partial R_3 = 0$. Now $\partial\big(L^2+B^{-1}y(E'-2)R_1^2\big) \leqslant 4$, so $\partial R_1 \leqslant 1$, implying that $-\tau\varepsilon(B-B^{-1})(E'-1) = 0$.

Since $B^2 \neq 1$, $\tau = 0$ or $E = 1$ so $\tau = 0$ for $E = 0$. Now $\partial L \leqslant 1$, $\varepsilon E'(\bar{\lambda}-\lambda) = 0$, so $\tau' = 0$ or $E = 0$. So if $E \neq 0$, $\tau' = 0$ and $R_3 = 0$, $L = 0$ and so from the constant term of R_1 we get $\tau = 0$.

LEMMA 10. *We have $\mu = 0$, C rational, and for $E \neq 0$, $\lambda = 0$ and R^2 is rational.*

Proof. It is sufficient to prove that $\mu = 0$ and, for $E \neq 0$, $\lambda = 0$. Then $C' = C$ and, for $E \neq 0$, $R'^2 = R^2$, from (4.8). Since this is true for any conjugates C', R'^2 of C, R^2, we have the result.

Assume that $\mu \neq 0$ if $E = 0$, and that μ, λ are not both 0 if $E \neq 0$. Then by Lemma 8, $s^2 = y$ satisfies (6.1), which is not identically 0, by Lemma 9. So not all of L, R_1, R_2 are identically 0. Since by Lemma 3 (4.6) has two real ($\varepsilon_0 = 1$), or imaginary ($\varepsilon_0 = -1$) roots $d+d^{-1}$ iff $L = R_1 = R_2 = 0$, there can be at most four values of s^2 for which (4.6) has two real ($\varepsilon_0 = 1$) or imaginary ($\varepsilon_0 = -1$) roots. Hence there are at most $4\cdot 2+4\cdot 1 = 12$ pairs s^2, $d+d^{-1}$ which satisfy (4.6). Now s^2 determines s, as $\arg s \in [0, \pi)$, and if t' is one solution to $t'/s+s/t' = d+d^{-1}$, then $u' = s^2/t'$ is the other. So each pair s^2, $d+d^{-1}$ corresponds to a unique unordered pair $\{t', u'\}$ of parameters of conjugates of z. Hence there are at most 24 values for t', u', so $\partial z \leqslant 24$. Since $\partial z \geqslant 25$, the result is proved.

LEMMA 11. (a) *For $\mathscr{C} = \mathscr{H}$, $k(B) = 1$ or 2. (There is no restriction on $k(B)$ for $\mathscr{C} = \mathscr{E}$.)*

(b) *When $\mathscr{C} = \mathscr{E}$ and $k(B) = 1$, all conjugates of B not equal to $B^{\pm 1}$ lie on U.*

(c) *When $\mathscr{C} = \mathscr{H}$ and $k(B) = 1$, all conjugates of B except $B^{\pm 1}$ are real.*

Proof. (a) If $E = 0$, $B = \pm i$, $k(B) = 2$. So we can assume $E \neq 0$. Then $\mu = \lambda = 0$, and (4.6), (4.7) and (4.9) give

$$(6.8) \qquad (d^2 - \varepsilon\varepsilon^* B')(d^2 - \varepsilon\varepsilon^* B'^{-1})(s^2 - \varepsilon^* B' B^{-1})(s^2 - \varepsilon^* B'^{-1} B^{-1}) = 0.$$

For $\mathscr{C} = \mathscr{H}$, d^2 and s^2 are real. If $k(B) > 1$, B has a conjugate $B' \neq B$ with $|B'| = 1$. Since $B \neq \pm 1$, $B' \neq \pm 1$ and so $d^2 = \varepsilon\varepsilon^* B'$ or $\varepsilon\varepsilon^* B'^{-1}$. Hence by (6.8) one of $B'^{\pm 1} B^{-1}$ is real, which implies $B' = \pm B^{\pm 1}$, $B'^2 = B^{\pm 2}$, and $k(B) = 1$ or 2.

(b) For $\mathscr{C} = \mathscr{E}$, d^2 and s^2 are on $\boldsymbol{U}$, so that from (6.8) either B' or $B' B^{-\delta} (\delta = \pm 1)$ is on $\boldsymbol{U}$. In the latter cases $B' \overline{B}' = B^{2\delta}$, so by Lemma 1(b), some power B'^k of B' is equal to $B^{\delta k}$. So $B' = \varrho B^{\delta}$ for some root of unity ϱ. As $k(B) = 1$, we can take $\varrho = 1$.

(c) For $\mathscr{C} = \mathscr{H}$, from (4.6) either B' is real, or $\arg B'^2 = \arg B^{2\delta}$, $\delta = \pm 1$. Hence $B'^2 \overline{B}'^{-2} = B^{4\delta}$, so by Lemma 1(b), $B'^k = B^{\delta k}$ for some k, and the argument of (b) above applies.

For $E = 0$, we now define $z^* = (z - C)^2$. Then z^* lies with its conjugates on the line $\mathrm{Rl}\, z = 2\varepsilon R^2$, and, by Corollary 2 to Lemma 1, R^2 is rational, and $z^* = 2\varepsilon R^2 + ia$, where $a \in \mathscr{A}(\boldsymbol{R})$. Note that R^2 rational implies that in fact $\lambda = 0$ in the case $E = 0$ also.

For $E \neq 0$, we define z^* by (2.2). Then note that if $z_j = C + R\left(B^{1/2} t_j + \varepsilon (B^{1/2} t_j)^{-1}\right)$ is a conjugate of z,

$$z_j^* = (B^{*k})^{1/2} t_j^{*k} + \left((B^{*k})^{1/2} t_j^{*k}\right)^{-1},$$

where

$$t_j^* = \begin{cases} \varepsilon^{1/2} t_j & \text{if } \mathscr{C} = \mathscr{E}, \\ t_j & \text{if } \mathscr{C} = \mathscr{H}; \end{cases} \qquad B^* = \begin{cases} B & \text{if } \mathscr{C} = \mathscr{E}, \\ \varepsilon^{1/2} B & \text{if } \mathscr{C} = \mathscr{H}. \end{cases}$$

Also, if $k = 2$, z_j^* has positive parameter t_j^2 for $\mathscr{C} = \mathscr{H}$. Now any automorphism τ_i of $\mathscr{F}$ which maps $z \mapsto z_j$ maps $z^* \mapsto T_{k(B)}\left(\frac{\pm \varepsilon^{1/2}(z_j - C)}{R}\right)$ $= \pm z_j^*$, and so lies on $\mathscr{C}(0, 1, B^{*k(B)}, 1)$, $\mathscr{C} = \mathscr{E}$ or $\mathscr{H}$. This conic is non-degenerate unless $\mathscr{C} = \mathscr{H}$ and $B^{*k(B)} = \pm 1$. This is impossible as $B \neq \pm 1$ and, since $E \neq 0$, $B \neq \pm i$.

We now replace z by z^*, i.e. we assume that z and all its conjugates lie on $\mathscr{C}(0, 1, B, 1)$, where $B \in S_{\mathscr{C}}$, $\mathscr{C} = \mathscr{E}, \mathscr{H}$.

From (6.8), since now $\varepsilon = \varepsilon^* = 1$, we get $s^2 = 1$ if $B' = B^{\pm 1}$, and otherwise $d^2 = B'^{\pm 1}$. Hence $u = 1/t$ if $s^2 = 1$, and $u = tB'^{\pm 1}$ otherwise. Putting $B = B_1$ and letting $B_2^{\pm 1}, \ldots, B_n^{\pm 1}$ be the conjugates of B on $\boldsymbol{U}$ $(\mathscr{C} = \mathscr{E})$ or $\boldsymbol{R}$ $(\mathscr{C} = \mathscr{H})$, we see that $B_2, \ldots, B_n$ are multiplicatively independent by Lemma 4(b). Hence we can apply Corollary 2 to obtain analogously with Lemma 6, that

LEMMA 12. *For $\mathscr{C} = \mathscr{E}, \mathscr{H}$, the set $\mathscr{T}$ of parameters of z and its conjugates is a disjoint union of sets $\mathscr{T}_a$ (a on $\boldsymbol{U}$ for $\mathscr{C} = \mathscr{E}$, a real for $\mathscr{C} = \mathscr{H}$) where for $a \neq \pm 1$*

$$\mathscr{T}_a = \left\{t \mid t = a^{\varepsilon_1}\left(\prod_{j=2}^{n} B_j^{\varepsilon_j}\right)^{1/2},\ \varepsilon_j = \pm 1\ (j = 1, \ldots, n)\right\}$$

and

$$\mathscr{T}_a = \left\{t \mid t = a\left(\prod_{j=2}^{n} B_j^{\varepsilon_j}\right)^{1/2},\ \varepsilon_j = \pm 1\ (j = 2, \ldots, n)\right\} \qquad (a = \pm 1).$$

The square roots are chosen as follows: fix $\left(\prod_{j=2}^{n} B_j\right)^{1/2}$ to have argument in $[0, \pi)$, then

$$\left(\prod_{j=2}^{n} B_j^{\varepsilon_j}\right)^{1/2} = \left(\prod_{j=2}^{n} B_j\right)^{1/2} \prod_{\substack{j: \\ \varepsilon_j = -1}} B_j^{-1}.$$

Note that $|\mathscr{T}_a| = 2^n$ $(a \neq \pm 1)$ and $|\mathscr{T}_{\pm 1}| = 2^{n-1}$.

Again, we have

LEMMA 13. *For z and its conjugates on $\mathscr{C}(0, 1, B, 1)$ $(\mathscr{C} = \mathscr{E}, \mathscr{H})$,*

$$\Sigma_a = \sum_{t \in \mathscr{T}_a} z(t) = (a + a^{-1})\left(\prod_{j=2}^{n} B_j\right)^{1/2} B^{1/2} \prod_{j=1}^{n} (1 + B_j^{-1}) = (a + a^{-1}) r^{1/2},$$

where $r \in \boldsymbol{Q}$, $r > 0$.

By the same argument as for the parabolic case, all conjugates of Σ_a are of the form $\pm(a' + a'^{-1}) r^{1/2}$, where a' is on $\boldsymbol{U}$ $(\mathscr{C} = \mathscr{E})$, and real $(\mathscr{C} = \mathscr{H})$. Hence Σ_a is totally real, so $\alpha := a + a^{-1} \in \mathscr{A}([-2, 2])$ $(\mathscr{C} = \mathscr{E})$ and $\in \mathscr{A}\left((-\infty, -2] \cup [2, \infty)\right)$ $(\mathscr{C} = \mathscr{H})$. Then $a = \frac{1}{2}\left(\alpha \pm (\alpha^2 - 4)^{1/2}\right)$, so z has a conjugate $\theta + \theta^{-1}$, where $\theta = \frac{1}{2}\left(\alpha + (\alpha^2 - 4)^{1/2}\right)\left(\prod_{j=1}^{n} B_j\right)^{1/2}$.

7. We now prove the converse parts of Theorems 2, 3, and 4. For Theorem 2, let z be given by (2.1). Then every conjugate of z is of form

$$z' = \tfrac{1}{4}\left(\varepsilon_a \alpha_k^{1/2} + \sum_{j=1}^{n} \varepsilon_j (-F_j)^{1/2}\right)^2 + C$$

where α_k is a conjugate of α, and $\varepsilon_a, \varepsilon_1, \ldots, \varepsilon_n$ are ± 1. So

$$z' = \frac{1}{F}\left(\tfrac{1}{2}\varepsilon_a (\alpha_k F)^{1/2} + \tfrac{1}{2}\varepsilon_1 iF + \sum_{j=2}^{n} \varepsilon_j (-FF_j)^{1/2}\right)^2 + C$$

$$= \frac{1}{F}\left(\tfrac{1}{2}\varepsilon_1 \varepsilon_a (\alpha_k F)^{1/2} + \sum_{j=2}^{n} \varepsilon_1 \varepsilon_j (-FF_j)^{1/2} + \tfrac{1}{2} iF\right)^2 + C$$

which, since $\alpha_k > 0$, $F > 0$ and $-F_j > 0$ $(j = 2, \ldots, n)$, is of the form (1.1) for real t, as required.

For Theorems 3 and 4, consider the conjugates of θ given by (2.3), where $\alpha \in \mathscr{A}([-2, 2])$ ($\mathscr{C} \in \mathscr{E}$), $\alpha \in \mathscr{A}((-\infty, -2] \cup [2, \infty))$ ($\mathscr{C} = \mathscr{H}$), and $B \in S_{\mathscr{C}}$ ($\mathscr{C} = \mathscr{E}, \mathscr{H}$). Then all conjugates of $\frac{1}{2}(\alpha + (\alpha^2-4)^{1/2})$ are on U for $\mathscr{C} = \mathscr{E}$, and real for $\mathscr{C} = \mathscr{H}$. Further all conjugates of $(\prod_{j=1}^{n} B_j)^{1/2}$ are of the form $B^{\pm 1/2} \cdot w$, where w is on U ($\mathscr{C} = \mathscr{E}$) and real ($\mathscr{C} = \mathscr{H}$). Thus the result follows from the parametrization (1.2) of $\mathscr{C}$.

It remains only to show that, given z^* on $\mathscr{C}(0, 1, B^k, 1)$, where $k = k(B)$ and $B^k \in S_{\mathscr{C}}$ ($\mathscr{C} = \mathscr{E}, \mathscr{H}$), then the zeros z of

$$z^* = T_k\left(\frac{(z-C)\varepsilon^{1/2}}{R}\right)$$

lie on $\mathscr{C}(C, R, B, \varepsilon)$, where $k = 1$ or 2 for $\mathscr{C} = \mathscr{H}$.

Let $z^* = (\varepsilon B)^{k/2} t + ((\varepsilon B)^{k/2} t)^{-1}$, where $t > 0$ in the case $k = 2$, $\mathscr{C} = \mathscr{H}$. Then the k roots z_j are given by

$$\frac{(z_j - C)\varepsilon^{1/2}}{R} = \omega^j (\varepsilon B)^{1/2} t^{1/k} + (\omega^j (\varepsilon B)^{1/2} t^{1/k})^{-1} \qquad (j = 0, \ldots, k-1)$$

where $\omega = \exp(2\pi i/k)$, so

$$z_j = C + R(\omega^j B^{1/2} t^{1/k} + (\omega^j B^{1/2} t^{1/k})^{-1}) \qquad (j = 0, \ldots, k-1).$$

For $\mathscr{C} = \mathscr{E}$, $\omega^j t^{1/k}$ is on U, and $\omega^j t^{1/k}$ is real for $\mathscr{C} = \mathscr{H}$. Thus we have a parametrization (1.2) for z_j, which proves the result.

8. We now prove Theorem 1. Suppose that we have a parabola $\mathscr{P}(C, F)$ with C having a conjugate $C' \neq C$. Then as we saw in the proof of Theorem 2, there are at most 8 possible values for the parameter of an algebraic number z_i with conjugate $z_{i'}$, both on $\mathscr{P}(C, F)$. Hence the sum of the degrees of all algebraic numbers lying with their conjugates on $\mathscr{P}(C, F)$ is at most 8.

A similar argument holds for $\mathscr{C} = \mathscr{E}, \mathscr{H}$, if C or R^2 is irrational, except that 8 is replaced by 24.

References

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

[2] V. Ennola and C. J. Smyth, *Conjugate algebraic numbers on a circle*, Ann. Acad. Sci. Fennicae A I 582 (1974).

[3] — — *Conjugate algebraic numbers on circles*, Acta Arith. 29 (1976), pp. 147–157.

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

Received on 25.5.1979
and in revised form on 20.9.1979 (1162)

ACTA ARITHMETICA
XL (1982)

A new cubic character sum

by

A. R. Rajwade and J. C. Parnami (Chandigarh, India)

1. Introduction and the statement of the main result. For a polynomial $f(x)$ with integer coefficients, the character sum Σ_f is defined by $\sum_{x \pmod p} (f(x)|p)$, where p is a prime and $(a|p)$ the Legendre symbol. If $f(x)$ is linear, then clearly $\Sigma_f = 0$ and it is well known that

$$\Sigma_{ax^2+bx+c} = \left(\frac{a}{p}\right)\begin{cases} -1 & \text{if} \quad b^2-4ac \not\equiv 0 \pmod p, \\ p-1 & \text{if} \quad b^2-4ac \equiv 0 \pmod p. \end{cases}$$

It is surprising that beyond this little is known even for cubics, except some estimates. It is therefore equally remarkable that the exact value of Σ_f is known for the following cubics:

(i) $x^3 + ax$,

(ii) $x(x^2 + 4ax + 2a^2)$,

(iii) $x^3 + a$, and

(iv) $x(x^2 + 21ax + 112a^2)$.

Proofs of (i) can be found in [2], [7], [12], [16], those of (ii) in [1], [17], [13], [4], [5], those of (iii) in [9], [10], [8], [18], and those of (iv) in [15]. The common feature of these four cubics is that the curve $y^2 = f(x)$ is simply the most general elliptic curve defined over the rationals with complex multiplication by, respectively, $\sqrt{-1}$, $\sqrt{-2}$, $\sqrt{-3}$, $\sqrt{-7}$. There are five other such elliptic curves and it is conjectured by E. Lehmer and R. J. Evans that in each of these cases Σ_f has an answer similar to the above four cases. Recently H. Stark has developed a method which evaluates these sums systematically. The exact statement of Stark's result (unpublished) is:

$\Sigma_{f_m(x)} = c$ where $f_m(x)$ is the corresponding elliptic curve and where $4p = c^2 + md^2$ with $\left(\frac{c}{m}\right) = 1$ if $m = 7$, $\left(\frac{6}{p}\right)$ if $m = 11$, $\left(\frac{2}{p}\right)$ if $m = 19, 43, 67, 163$.