On Relationships Between Conjugate Algebraic Numbers

Neil Berry

Doctor of Philosophy
University of Edinburgh
2003

To my parents.

Abstract

We study two problems concerning algebraic numbers whose conjugates satisfy a certain relationship. In the first problem, the relationship is geometric: we classify all algebraic numbers that lie with their conjugates on a pair of straight lines in the complex plane. In the second problem, the relationship is algebraic: it concerns the *conjugate dimension* of an algebraic number, namely the dimension of the vector space (over some base field K) spanned by its conjugates. The work on the latter problem is based on collaboration with Arturas Dubickas, Noam Elkies, Bjorn Poonen and Chris Smyth.

We begin by providing some background material, mainly galois theory. In the second chapter, we state the main results that solve the first problem, and quote previous results that classify algebraic numbers whose conjugates all lie on a single straight line, and those whose conjugates all lie on a (nondegenerate) conic. Thus the new results complete the classification of algebraic numbers whose conjugates all lie on any conic.

The proofs of the solutions to the first problem are given in chapters 3-6. Note that the requirement of symmetry in the real axis gives us four cases to consider: a vertical line and the real axis, two parallel horizontal lines, two parallel vertical lines, and two non perpendicular lines that intersect at a single point. The most surprising result concerns the point of intersection of the two non perpendicular lines (chapter 6). It transpires that this point need not be rational, but may also be quadratic.

In the final chapter, we study the second problem. For each $n \in \mathbb{N}$, we find upper and lower bounds for the degree over $\mathbb{Q}$ in relation to the conjugate dimension n, and show that these bounds can be attained. The upper bound is equal to the upper bound on the order of a finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$. From a result by Feit, for all but seven exceptional n the maximal order of a subgroup of $\mathrm{GL}_n(\mathbb{Q})$ is equal to $2^n n!$. We extend these results for base field equal to either a finite extension of $\mathbb{Q}$ or a finite field.

Acknowledgements

I would like to thank the following people and organisation:

My supervisor Chris Smyth, for giving advice and guidance whenever it was asked for or required.

Arturas Dubickas, Noam Elkies, Bjorn Poonen and Chris Smyth (again!) for their work in [1] (see Chapter 7).

My second supervisor Liam O'Carroll, for reading an early draft of a couple of the chapters, and advice on general layout and format.

EPSRC, for funding my research.

My fellow PhD mathematics students at Edinburgh University, for sharing in the whole experience.

Friends outside the department, especially those who took the time to ask how the PhD was going (although this may not have been appreciated at the time!).

My family, and in particular my parents, to whom I owe a tremendous amount of gratitude for all the support they have given me over the years.

Notation

$\mathbb{Q}$	The field of rational numbers.
$\mathbb{Z}$	The ring of integers.
$\mathbb{N}$	The set of natural numbers.
$\mathbb{R}$	The field of real numbers.
$\mathbb{C}$	The field of complex numbers.
α, β, γ	Algebraic numbers.
$\overline{\alpha}$	Complex conjugate of α.
P_α	Minimal polynomial of α.
σ, ϕ, τ	Automorphisms.
K, L, F	A general field.
K^*	The multiplicative group of the non zero elements of K.
$K[x_1, \ldots, x_n]$	The polynomial ring of $x_1, \ldots, x_n$ in K.
$K(x_1, \ldots, x_n)$	The set of rational functions of $x_1, \ldots, x_n$ in K.
$K(x_1, \ldots, x_n)^G$	The G-invariant subfield of $K(x_1, \ldots, x_n)$.
L/K	Extension of K by L.
$\mathrm{Gal}(L/K)$	Galois group of L/K.
$[L : K]$	Degree of extension L/K.
$K(\alpha)$	Field generated by K and α.
$\mathrm{Tr}(\alpha)$	Trace of α.
$\mathrm{GL}_n(K)$	Group of invertible $n \times n$ matrices with coefficients in K.
S_n	Symmetric group on n symbols.
$\deg_K(\alpha)$	Degree of α over K.
$\Re(\alpha)$	Real part of α.
$\Im(\alpha)$	Imaginary part of α.
ω_j	Primitive j^{th} root of unity.
$G_1 \rtimes G_2$	Semidirect product of G_1 by G_2.
$G_1 \wr G_2$	Wreath product of G_1 by G_2.
$S_+(p)$	The lines $\Re(z) = p$ and the real axis.
$S_=(h)$	The lines $\Im(z) = \pm\sqrt{-h}$.
$S_\parallel(p, q)$	The lines $\Re(z) = p$ and $\Re(z) = q$.
$S_\times(C, \sqrt{u})$	The lines $z = C + t\sqrt{u}$ and $z = C + t\sqrt{u^{-1}}$ $(t \in \mathbb{R})$.
$\bigoplus_{i=1}^n U_i$	$U_1 \oplus U_2 \oplus \cdots \oplus U_n$.
$U^{\oplus m}$	$U \oplus U \oplus \cdots \oplus U$ (m times).
$\mathrm{GL}(V)$	General linear group of invertible linear transformations of V.

Table of Contents

Chapter 1

Preliminaries

We provide the background material which is assumed knowledge in subsequent chapters. This comes mainly in the form of galois theory. Unless otherwise stated, the results in Sections 1.1-1.4 below can be found in Stewart [24] and Garling [10].

1.1 Algebraic Numbers

We begin with some definitions:

Definition 1.1.1. An **algebraic number** is any number $\alpha \in \mathbb{C}$ which is a root of a polynomial $P \in \mathbb{Q}[x]$. More generally, α is **algebraic over** K if it is a root of some polynomial $P \in K[x]$ for some field K. If α is not algebraic over K, then it is **transcendental over** K.

The following definitions are given for a general field K, but unless stated otherwise, we shall assume that $K = \mathbb{Q}$.

Definition 1.1.2. Let α be an algebraic number. The **minimal polynomial** P_α of α over K is the gcd of all monic polynomials $P \in K[x]$ for which α is a root.

Definition 1.1.3. An algebraic number α' that is also a root of the minimal polynomial P_α of α over K is defined to be a **conjugate** of α over K. The **conjugate set** of α is the set of all conjugates of α.

Definition 1.1.4. An algebraic number α is **totally real** if the conjugate set of α are all real.

The proof that $\overline{\alpha}$ is a conjugate of α over $\mathbb{Q}$ is well known and straightforward:

Lemma 1.1.5. *Let α be an algebraic number with minimal polynomial $P_\alpha[x]$ over $\mathbb{Q}[x]$. Then $\overline{\alpha}$ also has minimal polynomial $P_\alpha[x]$, and so $\overline{\alpha}$ is a conjugate of α.*

Proof. Let P be the minimal polynomial of α over $\mathbb{Q}$. If $P(\alpha) = 0$ then $\overline{P}(\alpha) = 0$ as P has rational coefficients. Thus

$$\overline{\overline{P}(\alpha)} = P(\overline{\alpha}) = 0,$$

and as P is irreducible, it is the minimal polynomial of $\overline{\alpha}$.

□

Definition 1.1.6. The **degree** of an algebraic number α is defined to be the degree of the minimal polynomial of α.

Definition 1.1.7. The **trace** of α, denoted $\mathrm{Tr}(\alpha)$, is defined as

$$\mathrm{Tr}(\alpha) = \sum_{i=1}^{d} \alpha_i,$$

where $\{\alpha_1, \ldots, \alpha_d\}$ is the conjugate set of α.

Definition 1.1.8. An algebraic number is **unit-circular** if it lies with its conjugate set on the unit circle $|z| = 1$ in the complex plane.

The following result, originally incorporated in [18], is stated in the form below in [4]:

Proposition 1.1.9. *Let β be a totally real algebraic number whose conjugate set $\{\beta_1 = \beta, \ldots, \beta_d\}$ all lie in the interval $[-2, 2]$. Define an algebraic number α by its minimal polynomial*

$$P_\alpha[x] = \prod_{i=1}^{d} (x^2 - \beta_i x + 1) \in \mathbb{Q}[x].$$

Then α is unit-circular.

Conversely, let α be an algebraic unit-circular number. Then either $\alpha = 1$ or -1, or $\beta = \alpha + \alpha^{-1}$ is totally real, with conjugate set in $[-2, 2]$, and α has minimal polynomial

$$P_\alpha[x] = \prod_{i} (x^2 - \beta_i x + 1) \in \mathbb{Q}[x].$$

Proof. ($\Rightarrow$) Let β be a totally real algebraic number of degree d whose conjugate set all lie in $[-2, 2]$. If $\beta = \pm 2$, then $\alpha = 1$ or -1 is unit circular. Otherwise, define

$$\alpha = \frac{\beta + \sqrt{\beta^2 - 4}}{2}.$$

Then $|\alpha| = 1$, and α is a root of

$$P_\alpha[x] = \prod_i (x^2 - \beta_i x + 1).$$

Apply an automorphism to α:

$$\alpha' = \frac{\beta' \pm \sqrt{\beta'^2 - 4}}{2}.$$

Since $\beta' \in [-2, 2]$, $|\alpha'| = 1$, and hence α is unit-circular.

($\Leftarrow$) Let α be a unit-circular algebraic number. If $\alpha = \pm 1$, then α has minimal polynomial $P_\alpha[x] = x \mp 1$. Otherwise, $\overline{\alpha} = \alpha^{-1}$ is a conjugate of α. Define $\beta = \alpha + \alpha^{-1}$. Any automorphism that maps $\alpha \mapsto \hat{\alpha}$ must map $\alpha^{-1} \mapsto \hat{\alpha}^{-1}$, so β is totally real. Also, for all conjugates β' of β,

$$\beta' = 2\Re(\alpha') \tag{1.1}$$

for some conjugate α' of α. Since α is unit circular, $|\Re(\alpha')| \leq 1$ for all conjugates α' of α. Hence β lies with its conjugates in $[-2, 2]$.

Now

$$\Re(\alpha)^2 + \Im(\alpha)^2 = 1.$$

So from Equation (1.1),

$$\Im(\alpha) = \frac{\sqrt{4 - \beta^2}}{2}.$$

Since $|\beta| \leq 2$,

$$\alpha = \frac{\beta + \sqrt{\beta^2 - 4}}{2},$$

and

$$\alpha^{-1} = \frac{\beta - \sqrt{\beta^2 - 4}}{2}.$$

Let $P_\alpha[z]$ be the minimal polynomial of α. Then $(z - \alpha)(z - \alpha^{-1}) = z^2 - \beta z + 1$ is a factor of P_α, and hence

$$P_\alpha[z] = \prod_i (z^2 - \beta_i z + 1)$$

as required. □

1.2 Symmetric Polynomials

Definition 1.2.1. A polynomial in the indeterminates $x_1, \ldots, x_n$ is known as a **symmetric polynomial** if it is invariant under any permutation of $\{x_1, \ldots, x_n\}$.

The trace of an algebraic number α is an example of a symmetric polynomial in its conjugate set.

Definition 1.2.2. Let P be a monic polynomial of degree n, and let P have roots $t_1, t_2, \ldots, t_n$. Then the **elementary symmetric polynomials** $(s_1, \ldots, s_n)$ in $t_1, \ldots, t_n$ are defined by

$$P[x] = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots + (-1)^n s_n.$$

So

$$\begin{gathered} s_1 = t_1 + t_2 + \cdots + t_n \\ s_2 = t_1t_2 + t_1t_3 + \cdots + t_{n-1}t_n \\ \vdots \\ s_n = t_1t_2 \cdots t_n. \end{gathered}$$

Let $q(s_1, \cdots, s_n)$ be a polynomial in the elementary symmetric functions. Let $cs_1^{m_1}s_2^{m_2}\cdots s_n^{m_n}$ be a term in q. Then the **weight** of the term $cs_1^{m_1}s_2^{m_2}\cdots s_n^{m_n}$ is defined to be $m_1 + 2m_2 + \cdots + nm_n$. The largest weight amongst all such terms in q is called the **weight** of q.

Remark. When a polynomial is expressed in terms of the indeterminates $x_1, \ldots, x_n$, we refer to its *degree*, whereas if it is expressed in terms of the elementary symmetric polynomials, we refer to its *weight*.

Theorem 1.2.3. *[25] [Fundamental Theorem of Symmetric Polynomials] Let K be a field. A symmetric polynomial of degree r in $K[x_1, x_2, \ldots, x_n]$ may be written as a polynomial $p(s_1, s_2, \ldots, s_n)$ of weight r.*

Proof. Let $f(x_1, \ldots, x_n)$ be a symmetric polynomial of degree r. The proof is by double induction on n and r. Consider the case $n = 1$. Every polynomial $f(x_1)$ is symmetric in x_1, and $s_1 = x_1$, so $f(x_1) = f(s_1)$.

Assume the theorem is true for polynomials in n variables (for some $n > 0$). Consider polynomials in $n + 1$ variables $x_1, \ldots, x_{n+1}$:

For polynomials in $n + 1$ variables of degree $r = 0$, the theorem is trivial. We make a second assumption, that the theorem is true for all polynomials in $n+1$ variables of degree less than r. Let $f(x_1, \ldots, x_{n+1})$ be a polynomial in $n+1$ variables of degree r. Set $x_{n+1} = 0$. Then $f(x_1, \ldots, x_n, 0)$ is a symmetric polynomial in n variables, so by the first assumption, can be written as a polynomial

$\phi(s_1, \ldots, s_n)$ in the elementary symmetric polynomials of weight at most r. Now define a new polynomial $g(x_1, \ldots, x_{n+1})$ such that

$$g(x_1, \ldots, x_{n+1}) = f(x_1, \ldots, x_{n+1}) - \phi(s_1, \ldots, s_n).$$

Note that $g(x_1, \ldots, x_{n+1})$ is symmetric in the x's, and since f has degree r and ϕ has weight at most r, g has degree at most r. Also, for $x_{n+1} = 0$, $g = 0$, so all terms contain the factor x_{n+1}. Since g is symmetric, all terms must contain the factors $x_1, x_2, \ldots, x_n$ as well. So all terms of g contain the product $x_1 x_2 \cdots x_{n+1}$. Factoring this out of g gives

$$g(x_1, \ldots, x_{n+1}) = s_{n+1} h(x_1, \ldots, x_{n+1}),$$

where h is again a symmetric polynomial of degree at most $r - (n+1)$.

Recall that by the second assumption, every polynomial of degree $n+1$ with weight less than r can be written as a polynomial in the elementary symmetric functions. So

$$h(x_1, \ldots, x_{n+1}) = \xi(s_1, \ldots, s_{n+1}),$$

where ξ has weight at most $r - (n+1)$. Therefore

$$\begin{aligned} f(x_1, \ldots, x_{n+1}) &= g(x_1, \ldots, x_{n+1}) + \phi(s_1, \ldots, s_n) \\ &= s_{n+1}\xi(s_1, \ldots, s_{n+1}) + \phi(s_1, \ldots, s_n). \end{aligned}$$

The right hand side is a polynomial in the s_i of weight at most r. The weight cannot be less than r, since otherwise f would have degree less than r. Therefore the right hand side is exactly of weight r. This completes the proof. □

Theorem 1.2.4. *[25] A symmetric polynomial in $K[x_1, \ldots, x_n]$ can be expessed uniquely as a polynomial in the elementary symmetric polynomials.*

Proof. Let ψ_1 and ψ_2 be two polynomials in the indeterminates $x_1, \ldots, x_n$. Suppose

$$\psi_1(x_1, \ldots, x_n) \neq \psi_2(x_1, \ldots, x_n).$$

Then

$$\psi_1(x_1, \ldots, x_n) - \psi_2(x_1, \ldots, x_n) = \psi(x_1, \ldots, x_n) \neq 0.$$

We have to prove that

$$\psi(s_1, \ldots, s_n) \neq 0.$$

The proof is by induction on n. The theorem is true for $n = 1$, since $s_1 = x_1$, so $\psi(x_1) = \psi(s_1)$.

Now assume the theorem is true for all symmetric polynomials with fewer than n indeterminates, for some $n > 1$. Suppose there exists a polynomial $\psi(x_1, \ldots, x_n) \neq 0$ of minimal degree m with respect to x_n such that $\psi(s_1, \ldots, s_n) = 0$. We arrange the terms of $\psi(x_1, \ldots, x_n)$ in decreasing powers of x_n, then

$$\psi_m(x_1, \ldots, x_{n-1})x_n^m + \psi_{m-1}(x_1, \ldots, x_{n-1})x_n^{m-1} + \cdots + \psi_0(x_1, \ldots, x_{n-1}) \neq 0 \quad (1.2)$$

and

$$\psi_m(s_1, \ldots, s_{n-1})s_n^m + \cdots + \psi_0(s_1, \ldots, s_{n-1}) = 0. \quad (1.3)$$

Now suppose that $\psi_0(x_1, \ldots, x_{n-1}) = 0$. Then x_n could be cancelled from all the terms in Inequality (1.2), and $\psi_0(s_1, \ldots, s_{n-1}) = 0$ by the assumption, so s_n could be cancelled in Equation (1.3). Then we would have

$$\tilde{\psi}(x_1, \ldots, x_n) = \psi_m(x_1, \ldots, x_{n-1})x_n^{m-1} + \cdots + \psi_1(x_1, \ldots, x_{n-1}) \neq 0 \quad (1.4)$$

and

$$\tilde{\psi}(s_1, \ldots, s_n) = \psi_m(s_1, \ldots, s_{n-1})s_n^{m-1} + \cdots + \psi_1(s_1, \ldots, s_{n-1}) = 0 \quad (1.5)$$

where the polynomial $\tilde{\psi}$, viewed as a polynomial in x_n, has degree less than m, contradicting our assumption about the minimality of m. So

$$\psi_0(x_1, \ldots, x_{n-1}) \neq 0.$$

Now let $x_n = 0$ in Equation (1.3):

$$\psi_0(s_1, \ldots, s_{n-1}) = 0$$

and since we have $\psi_0(x_1, \ldots, x_{n-1}) \neq 0$, this gives us the required contradiction. □

1.3 Field Extensions

We now turn our attention to fields. The following results are given for general fields K and L. In the following chapters on the two lines problem, when applying these results we take the base field K to be $\mathbb{Q}$.

Definition 1.3.1. Let L be a field and K be a subfield of L. Then we say L/K is an **extension** of K.

Theorem 1.3.2. *Suppose L/K is an extension. Under the operations*
$+ : L \times L \to L$, $(l_1, l_2) \mapsto l_1 + l_2$, *and*
$\times : K \times L \to L$, $(k, l) \mapsto kl$,
L is a vector space over K.

Definition 1.3.3. The **degree** of a field extension L/K, denoted $[L:K]$, is the dimension of L considered as a vector space over K.

Definition 1.3.4. Let L/K be an extension, and let $\alpha \in L$ be algebraic over K. Then the smallest subfield generated by K and α is denoted $K(\alpha)$. It is the field of all elements of the form $\frac{a(\alpha)}{b(\alpha)}$, where a, b are polynomials in K, with $b(\alpha) \neq 0$. If P_α is the minimal polynomial of α, then

$$K(\alpha) \cong K[x]/\langle P_\alpha(x) \rangle,$$

where $\langle P_\alpha(x) \rangle$ is the ideal of $K[x]$ generated by the minimal polynomial of α.

Definition 1.3.5. An extension L/K is **algebraic** if every element $\alpha \in L$ is algebraic over K. An algebraic extension L/K such that $[L:K] < \infty$ is a **finite** extension. Otherwise L/K is an **infinite** extension.

Theorem 1.3.6. *Suppose L/K is an extension and that $\alpha \in L$. Then α is algebraic over K if and only if $[K(\alpha):K] < \infty$. If $[K(\alpha):K] = n < \infty$, then n is the degree of the minimal polynomial P_α of α.*

Remark. If $[K(\alpha):K] = n < \infty$, then a basis for $K(\alpha)/K$ is furnished by

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}.$$

Definition 1.3.7. The set of all numbers that are algebraic over $\mathbb{Q}$ is a field, usually denoted $\mathbb{A}$. The extension $\mathbb{A}/\mathbb{Q}$ is infinite. Any finite extension of $\mathbb{Q}$ is called a **number field**.

Definition 1.3.8. Let L be an algebraic extension of K. Then L is a **simple** extension of K if $L = K(\beta)$ for some $\beta \in L$.

Proposition 1.3.9. *Any number field is a simple extension of $\mathbb{Q}$.*

The following is known as the tower law:

Theorem 1.3.10. *Let K, L and M be fields such that $K \subseteq L \subseteq M$. Then*

$$[M:K] = [M:L][L:K]. \tag{1.6}$$

Equation (1.6) requires some comment if any of the extensions are infinite. As one would expect, $[M:K] = \infty$ if and only if either $[M:L] = \infty$ or $[L:K] = \infty$.

Theorem 1.3.11. *Suppose M/L and L/K are algebraic extensions. Then M/K is algebraic.*

We now examine different factorisations of the minimal polynomial P_α of α over K. First, we consider fields over which P_α factorises completely.

Theorem 1.3.12. *Let α be an algebraic number with minimal polynomial P_α over K. Then there exists a finite extension L/K such that P_α factorises into linear factors*

$$k(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

where $k \in K$, and $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n \in L$.

Definition 1.3.13. If P_α factorises into linear factors over an extension L/K, we say that P_α **splits over** L. We say that L is a **splitting field** for P_α over K if:

1. P_α splits over K
2. If M/K is an extension such that P_α splits over M, then $L \subseteq M$. L can also be denoted by $K(\alpha_1, \ldots, \alpha_n)$. Such a field is unique up to isomorphism.

An extension L/K is **normal** if any polynomial that is irreducible over $K[x]$ either splits in L or has no roots in L.

Theorem 1.3.14. *Suppose that $f \in K[x]$ is irreducible of degree n. Then there is a simple algebraic extension $K(\alpha)/K$ such that $[K(\alpha):K] = n$ and $f(\alpha) = 0$.*

Theorem 1.3.15. *Suppose that $f \in K[x]$. Then there exists a splitting field extension L/K for f, with $[L:K] \leq n!$.*

Remark. A *separable* extension is one in which every irreducible polynomial has no multiple roots. In the following section, we require our extension to be finite, normal and separable. However, every field with characteristic zero is separable, and all fields in Chapters 2-6 are number fields, so separability can be assumed.

Definition 1.3.16. An extension that is finite, normal and separable is called a **galois extension**.

1.4 Galois Theory

Definition 1.4.1. If L/K is an extension, a **K-automorphism** τ is an automorphism of L such that $\tau(\beta) = \beta$ for all $\beta \in K$.

Definition 1.4.2. Define **Aut(L)** to be the set of K-automorphisms of L. Then $\mathrm{Aut}(L)$ forms a group under composition of maps. This group is called the **galois group** of L/K, and is denoted by $\mathrm{Gal}(L/K)$.

$$\mathrm{Gal}(L/K) = \{\sigma : \sigma \in \mathrm{Aut}(L)\}.$$

Suppose that $f \in K[x]$ and L/K is a splitting field extension for f over K. Then we call $\mathrm{Gal}(L/K)$ the **galois group** of f. We denote it by $\mathrm{Gal}_K(f)$ or $\mathrm{Gal}(f)$.

Theorem 1.4.3. *Suppose that $f \in K[x]$ is irreducible and that L/K is a splitting field extension for f. Let R denote the set of roots of f in L. Each $\sigma \in \mathrm{Gal}(f)$ defines a permutation of R, so that we have a mapping from $\mathrm{Gal}(f)$ into the group S_R of permutations of R. The mapping is a group homomorphism, and is 1-1.*

The following, Proposition 10.2 in Stewart [24], shows that the Galois group of a polynomial f acts transitively on the roots of f:

Proposition 1.4.4. *Suppose L/K is a finite normal extension, and α_1, α_2 are zeros in L of the irreducible polynomial P over K. Then there exists an automorphism $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\alpha_1) = \alpha_2$.*

More generally, if we have algebraic numbers $\beta_1, \ldots, \beta_r$ that are not conjugate over K, we can take an algebraic extension L/K such that the minimal polynomials $P_{\beta_1}, \ldots, P_{\beta_r}$ all split over L. Then for any choice of $\beta'_1, \ldots, \beta'_r$ conjugate to $\beta_1, \ldots, \beta_r$ respectively, there exists $\tau \in \mathrm{Gal}(L/K)$ such that $\tau(\beta_1) = \beta'_1, \ldots, \tau(\beta_r) = \beta'_r$. The smallest such L is known as the **normal closure** of $\beta_1, \ldots, \beta_r$, and is unique up to isomorphism.

Remark. In subsequent chapters, when we apply an automorphism σ, it is understood that $\sigma \in \mathrm{Gal}(L/K)$, where L is the normal closure of the elements we are mapping.

Theorem 1.4.5. *Let L/K be a finite extension. If P_α has splitting field L/K, then*

$$|\mathrm{Gal}(L/K)| = [L : K].$$

The subgroups of $\mathrm{Gal}(L/K)$ have a particular significance:

Definition 1.4.6. Let L be a splitting field for a minimal polynomial P_α of α. We consider fields M such that $K \subseteq M \subseteq L$, and call M an **intermediate field** of L/K.

Let α and P_α be defined as above, and let L be a splitting field for P_α. Associated with every intermediate field M there is a group $\mathrm{Gal}(L/M)$ of all M-automorphisms of L.

Conversely, to each subgroup H of $\mathrm{Gal}(L/K)$ we associate a field L^H containing elements $\beta \in L$ such that $\tau(\beta) = \beta$ for all $\tau \in H$. L^H is an intermediate field of L/K, known as the **fixed field** of H.

The following is taken from Garling [10], Theorem 11.3:

Theorem 1.4.7 (Artin). *Let K be a field, and let G be a finite group of automorphisms of K. Then K is a galois extension of the fixed field*

$$K^G = \{a \in K : \sigma(a) = a \, \forall \sigma \in G\}$$

with galois group $\mathrm{Gal}(K/K^G) = G$.

Theorem 1.4.8 (Fundamental Theorem of Galois Theory). *Let L/K be a galois extension, with galois group* $\mathrm{Gal}(L/K)$, *let M be an intermediate field of L/K and let H be a subgroup of* $\mathrm{Gal}(L/K)$. *Then:*

1. *There is an inclusion reversing bijection between intermediate fields of L/K and subgroups of* $\mathrm{Gal}(L/K)$ *given by*

$$M \to \mathrm{Gal}(L/M)$$

$$H \to L/L^H.$$

Hence the lattice of intermediate fields of L/K is the inverted lattice of subgroups of $\mathrm{Gal}(L/K)$.

2. *The intermediate field M is a normal extension of K if and only if* $\mathrm{Gal}(L/M)$ *is a normal subgroup of* $\mathrm{Gal}(L/K)$.

3. *If M is a normal extension of K then* $\mathrm{Gal}(M/K)$ *is isomorphic to the quotient group* $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$.

Corollary 1.4.9. *Let r be an algebraic number with splitting field L. Suppose that $\sigma(r) = r$ for all $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Then $r \in \mathbb{Q}$.*

Example 1.4.10. Let α be an algebraic number with minimal polynomial

$$P_\alpha = a_0 + a_1 x + \cdots + a_n x^n$$

over $\mathbb{Q}$. Let L be a splitting field for P_α, and let σ be a $\mathbb{Q}$-automorphism over L. Since a_i is the i^{th} symmetric polynomial in the conjugate set of α, $\sigma(a_i) = a_i$ for all i.

It is natural to ask what else is known about the galois group of an algebraic number. The study of which groups form galois groups of some polynomial over a field K is known as *inverse galois theory.* In Chapter 7, the question of whether there exists an α algebraic over K such that the galois group of α is isomorphic to a finite subgroup of $GL_n(K)$ of maximal order for various n and K is addressed. Elsewhere, the following two Theorems (1.4.11) and (1.4.12) are used:

Theorem 1.4.11. *[25, p.192] For every $n \in \mathbb{N}$, there exists an α of degree n whose minimal polynomial has galois group S_n over $\mathbb{Q}$.*

Theorem 1.4.12. *[24, Lemma 14.7] Suppose that $f \in \mathbb{Q}[x]$ is irreducible, of degree p for some prime p, and has exactly two non-real roots. Then the galois group $\operatorname{Gal}(f)$ of f over $\mathbb{Q}$ is the symmetric group S_p.*

Theorem 1.4.13. *[10, Theorem 19.6] [The Normal Basis Theorem] Let K be an infinite field, and let L/K be a galois extension with galois group $G = \{\sigma_1, \ldots, \sigma_n\}$. Then there exists $l \in L$ such that $\{\sigma_1(l), \ldots, \sigma_n(l)\}$ is a basis for L over K.*

1.5 Group Theory

The following is collection of group theory definitions used in Chapter 7:

Definition 1.5.1. Let X be a set, G a finite group that acts on X, and S a subset of X. Then we say that S is **G-stable** if $gS = \{gs : s \in S\}$ is equal to S for all $g \in G$.

Definition 1.5.2. Let G be a group with subgroups N and K such that

1. N is normal,
2. $N \cap K = \{e\}$, and
3. $G = NK$.

Then G is a **semidirect product** of N and K, denoted $G = N \rtimes K$.

Remark. If K is also a normal subgroup of G, then G is a *direct product* $N \times K$.

Example 1.5.3. [12] Let $v = (v_1, \ldots, v_n) \in (\mathbb{Z}/2\mathbb{Z})^n$, let $f \in S_n$, and define

$$\hat{f}(v) = (v_{f^{-1}(1)}, \ldots, v_{f^{-1}(n)}) = P(f^{-1})v^t,$$

where $P(g)$ is an $n \times n$ permutation matrix that permutes $x_1, \ldots, x_n$ in the same manner as $g \in S_n$, and v^t is the transpose of v. We define the semi-direct product

$$(\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$$

by

$$(v, p) * (w, q) = (w + \hat{q}(v), pq),$$

where $v, w \in (\mathbb{Z}/2\mathbb{Z})^n$, $p, q \in S_n$.

More generally, the semidirect product $(\mathbb{Z}/l\mathbb{Z})^n \rtimes S_n$ is defined exactly as above, except for $(\mu, v) \in (\mathbb{Z}/l\mathbb{Z})^n \rtimes S_n$, $v = (v_1, \ldots, v_n)$, with each v_j an element of the multiplicative group generated by $\langle e^{2\pi i/l} \rangle$.

Definition 1.5.4. Let G_1 and G_2 be groups, with G_2 acting on a finite set $X = \{x_1, \ldots, x_n\}$, and let

$$K = \prod_{x \in X} G_x,$$

where $G_x \cong G_1$ for all $x \in X$. The **wreath product** of G_1 and G_2, denoted $G_1 \wr G_2$, is the semidirect product of K by G_2, where G_2 acts on K by $g_2 \circ (g_x) = g_{g_2 x}$ for all $g_2 \in G_2$ and $g_x \in \prod_{x \in X} G_x$. We call the normal subgroup K of $G_1 \wr G_2$ the **base** of the wreath product.

Example 1.5.5. Let G be a group. Consider the wreath product $G \wr S_2$, $s \in S_2$ acts on $(g_1, g_2) \in G^2$ by

$$s(g_1, g_2) = \begin{cases} (g_1, g_2) & \text{if } s \text{ is the identity element in } S_2\text{; or} \\ (g_2, g_1) & \text{if } s \text{ is the nontrivial element in } S_2. \end{cases}$$

In general, $G \wr S_n$, let $g = (g_1, \ldots, g_n) \in G^n$. Then $s \in S_n$ acts on g by

$$s(g) = (g_{s(1)}, \ldots, g_{s(n)}).$$

Example 1.5.6. The semidirect product in Example 1.5.3 $(\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$ can be expressed as a wreath product $(\mathbb{Z}/2\mathbb{Z}) \wr S_n$. The base of $(\mathbb{Z}/2\mathbb{Z}) \wr S_n$ is $(\mathbb{Z}/2\mathbb{Z})^n$.

Definition 1.5.7. Let V be a finite dimensional vector space over a field F. A linear automorphism $S : V \to V$ is called a **pseudo-reflection** if it is of finite order > 1, and leaves a codimension 1 subspace fixed pointwise. A group $G \subset \mathrm{GL}(V)$ is a **pseudo-reflection group** if it is generated by its pseudo-reflections.

Shephard and Todd [20], classified all pseudo-reflection groups (up to isomorphism). The notation (ST_r) that is used in Table 7.3 refers to the numbering of the groups used in the classification- see [20], Table VII, and also Smith [21], Table 7.3.1.

Definition 1.5.8. Let F be an arbitrary field, and let V be a vector space over F. A **reflection** s is a diagonalizable linear automorphism $s : V \to V$, which is not the identity map, but leaves a codimension 1 subspace fixed pointwise. This subspace is often called the reflecting hyperplane of s. A reflection is a diagonalizable pseudo-reflection, i.e. one whose order is relatively prime to the characteristic of F.

All the eigenvalues of a reflection except one are equal to 1. Assuming the reflection s is finite of order n, the exceptional eigenvalue is a primitive n-th root of unity. So in the Euclidean space $F = \mathbb{R}$, as ± 1 are the only roots of unity, a reflection s must have order 2. We can define $s = s_\alpha$ as a map that takes a vector α to its negative and fixes its orthogonal complement pointwise. There is a formula

$$s_\alpha \lambda = \lambda - \frac{2(\lambda, \alpha)}{(\alpha, \alpha)} \alpha,$$

where (,) is the standard inner product on Euclidean space.

Definition 1.5.9. A **root system** is a finite set Φ (called **roots**) that satisfy

1. $\Phi \cap \mathbb{R}\alpha = \{\alpha, -\alpha\}$ for all $\alpha \in \Phi$.

2. $s_\alpha(\Phi) = \Phi$ for all $\alpha \in \Phi$.

There is a group, usually denoted W, generated by the set of reflections s_α ($\alpha \in \Phi$).

Definition 1.5.10. A root system Φ as defined in Definition 1.5.9 above is **crystallographic** if it also satisfies

3. $\frac{2(\alpha,\beta)}{(\beta,\beta)} \in \mathbb{Z}$

for all $\alpha, \beta \in \Phi$.

The group W generated by all reflections s_α, where α is an element of a crystallographic root system Φ, is known as the **Weyl group** of Φ.

See Humphreys [11] for more details.

1.6 Representation Theory

Let K be a field with zero characteristic (this condition is required for Maschke's theorem to hold), and G a finite group. The following definitions and results are taken from Ledermann [14]:

Definition 1.6.1. A **representation** of G on a finite dimensional vector space V over K is a homomorphism

$$\phi : G \to \mathrm{GL}_n(V),$$

from G to the group of automorphisms of V. The representation is **faithful** if it is injective.

Example 1.6.2. A representation of the group $(\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$ is given by the *signed permutation group*, namely the group of $n \times n$ matrices that has exactly one 1 or -1 in every row and column, with zeros elsewhere. Specifically, let $v = (v_1, \ldots, v_n) \in (\mathbb{Z}/2\mathbb{Z})^n$, and let $\mu \in S_n$ be a permutation matrix. For all $j \in 1, \ldots, n$, if v_j is not the identity element in $\mathbb{Z}/2\mathbb{Z}$, change the non zero entry in column j of the permutation matrix of μ to -1. The resulting matrix is a representation of (v, μ).

More generally, $(\mathbb{Z}/l\mathbb{Z})^n \rtimes S_n$ has a representation called the *monomial matrix group*, namely the group of $n \times n$ matrices that have exactly one non-zero entry in each row and column, the entry being an element of $\langle e^{2\pi i/l} \rangle$. Again for an element $(w, \lambda) \in (\mathbb{Z}/l\mathbb{Z})^n \rtimes S_n$, take the permutation matrix that is a representation of λ, let $w = (w_1, \ldots, w_n)$, and for all $j \in 1, \ldots, n$, change the non zero entry in the j^{th} column to w_j.

Definition 1.6.3. A KG**-module** is a vector space V over K with a multiplication

$$V \times G \to V$$

satisfying:

1. $\mathbf{v}(gh) = (\mathbf{v}g)h$

2. $\mathbf{v}1_G = \mathbf{v}$

3. $(\lambda \mathbf{v})g = \lambda(\mathbf{v}g)$

4. $(\mathbf{u} + \mathbf{v})g = \mathbf{u}g + \mathbf{v}g$

for all $\lambda \in K$, $\mathbf{u}, \mathbf{v} \in V$, $g, h \in G$.

Definition 1.6.4. Let V be a KG-module. A KG**-submodule** W of V is a subspace of V such that $\mathbf{w}g \in W$ for all $\mathbf{w} \in W, g \in G$.

A representation of a group G over a field K is equivalent to a KG-module:

Theorem 1.6.5. *If $\phi : G \to GL_n(K)$ is a representation of G over K, and $V = K^n$, then V becomes a KG-module by defining multiplication as*

$$vg = v(\phi(g)),$$

where $v \in V, g \in G$.

Definition 1.6.6. A representation of a group G with no nontrivial proper G-stable subspaces is called **irreducible**. Otherwise it is **reducible**. Let ϕ be a reducible representation of G over a finite dimensional vector space V, and let W be a nontrivial proper G-stable subspace of V. Considering ϕ only on W, we obtain a new representation of G called a **subrepresentation**.

Definition 1.6.7. A representation is **completely reducible** if it can be written as a direct sum of its irreducible subrepresentations.

Theorem 1.6.8 (Cayley). *Any finite group of order n can be represented by permutations acting on n objects.*

Definition 1.6.9. Let $G = \{g_1, \dots, g_r\}$. The **regular KG-module** is defined to be the KG-module with vector space V having basis $\{g_1, \dots, g_r\}$. The **regular representation** of G, denoted KG, is the representation $G \to S_r$ defined mapping $g \in G$ to the permutation

$$\pi(g) = \begin{pmatrix} g_1 & g_2 & \cdots & g_r \\ g_1 g & g_2 g & \cdots & g_r g \end{pmatrix}.$$

Theorem 1.6.10 (Maschke). *Let K and G be as above. Then every KG-module is completely reducible.*

The following result comes from the discussion following Equation (2.24) in [14]:

Lemma 1.6.11. *The regular representation KG of G contains $\dim(\phi)$ copies of any irreducible representation ϕ of G.*

Chapter 2

Introduction and Results

2.1 Earlier Work

Our aim in the following five chapters is to classify all algebraic numbers whose conjugate set lies on a pair of straight lines (but not a single line) in the complex plane. The motivation for studying such numbers comes from previous work on algebraic numbers that lie with their conjugates on various conics, given below. Our classification completes the classification of algebraic numbers whose conjugate set lie on a conic in the complex plane.

In 1969, R.M. Robinson asked which algebraic numbers have all their conjugates lying on a circle in the complex plane (see [18]). This question was answered for circles with rational centre by Robinson himself:

Theorem 2.1.1 (Robinson). *Let α be an algebraic number whose conjugate set lie on a circle centred at the origin with radius R. Then for some $n \in \mathbb{N}$, $R^n = q \in \mathbb{Q}$, and $\alpha^n = qu$, where u is unit-circular.*

Conversely, let $q \in \mathbb{Q}_{>0}$, and let u be unit-circular. Then α, defined as a root of $\alpha^n = uq$, lies with its conjugates on the circle $|z| = q^{\frac{1}{n}}$.

Proof. ($\Rightarrow$) Let α and all its conjugates lie on a circle $|z| = R$. Let α have degree d. Then $\alpha\alpha_2 \dots \alpha_d = \epsilon R^d \in \mathbb{Q}$ for some $\epsilon = \pm 1$. Let $n \in \mathbb{N}$ be the smallest power such that $R^n = q \in \mathbb{Q}$. Then

$$\alpha^n = uq \tag{2.1}$$

for some algebraic u of unit modulus. Apply an automorphism to Equation (2.1):

$$\hat{\alpha}^n = u'q.$$

Since $\hat{\alpha}$ lies on $|z| = q^{\frac{1}{n}}$, $|u'| = 1$. Hence u is unit circular.

($\Leftarrow$) Let $q \in \mathbb{Q}_{>0}$, let u be unit-circular, and let α be a root of $\alpha^n = uq$. Then $|\alpha| = q^{\frac{1}{n}}$. Apply an automorphism that maps $\alpha \mapsto \hat{\alpha}$. We have:

$$\hat{\alpha}^n = u'q,$$

and since u is unit-circular, $|\hat{\alpha}| = q^{\frac{1}{n}}$. Hence α and all its conjugates lie on the circle $|z| = q^{\frac{1}{n}}$.

□

Robinson's question was answered for circles with totally real centre by V. Ennola in [5], and for circles with non totally real centre by V. Ennola and C.J. Smyth in [6] (for centres of degree three or four) and [7] (for centres of degree greater than four). If the centre C of the circle is not totally real, it transpires that C itself lies with all its conjugates on a circle.

The question of finding all algebraic numbers that lie with their conjugates on a vertical line was answered by C.J. Smyth in [23], (see Corollary 2.1.6 below). In [4], C.J. Smyth and A. Dubickas find all algebraic numbers with norm ±1 that lie with their conjugates on a pair of concentric circles with rational centre.

All algebraic numbers that lie with their conjugates on parabolas, ellipses and hyperbolas are also found in [23]. This is a non-degenerate version of the two lines problem, and the results are given below in Theorems 2.1.2, 2.1.3 and 2.1.4.

Notation. 1. **Parabola**

Let $\mathfrak{P}(C, F)$ denote the parabola with equation

$$y^2 = F(x + \frac{1}{4}F - C),$$

or in parametric form,

$$z(t) = \frac{1}{F}(t + \frac{1}{2}iF)^2 + C,$$

where $(C, 0)$ is the focus of the parabola, and $F > 0$.

2. **Ellipse**

Let C be the centre of the ellipse, let $R > 0, \epsilon = \pm 1$ be fixed, and $B > 1$. The equation of the ellipse $\mathfrak{E}(C, R, B, \epsilon)$ is given by

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

or in parametric form,

$$z(t) = C + R(B^{\frac{1}{2}}t + \epsilon(B^{\frac{1}{2}}t)^{-1}),$$

where t takes values on the unit circle.

3. **Hyperbola**

Let C be the centre of the hyperbola, let $R > 0, \epsilon = \pm 1$ be fixed, and $|B| = 1, B \notin \mathbb{R}$. The equation of the hyperbola $\mathfrak{H}(C, R, B, \epsilon)$ is given by

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

or in parametric form,

$$z(t) = C + R(B^{\frac{1}{2}}t + \epsilon(B^{\frac{1}{2}}t)^{-1}),$$

where $t \in \mathbb{R}$.

We also define the following sets of algebraic numbers:

$S_{\mathfrak{P}} = \{F : F > 0$ and all other conjugates of F are $< 0\}$,
$S_{\mathfrak{E}} = \{B : B > 1$ is real, as is B^{-1}, and all other conjugates of B lie on the unit circle $\}$,
$S_{\mathfrak{H}} = \{B : B$ lies on the unit circle, $B^2 \neq 1$, and all conjugates of $B \neq B^{\pm 1}$ are real $\}$.

Let $k(B)$ be the smallest positive integer such that $B^{k(B)}$ has no conjugate of the form $\omega B^{\pm k(B)}$, where $\omega \neq 1$ is a root of unity. T_k denotes the Chebyshev polynomial of degree k, i.e. $T_k(t + t^{-1}) = t^k + t^{-k}$.

Theorem 2.1.2 (Parabolas). *Let α be an algebraic number of degree at least 9 whose conjugate set lies on a parabola $\mathfrak{P}(C, F)$. Then:*

1. *$C \in \mathbb{Q}$, and $F \in S_{\mathfrak{P}}$.*

2. *α has a conjugate of the form*

$$\frac{1}{4}\left(\beta^{\frac{1}{2}} + \sum_{j=1}^{n}(-F_j)^{\frac{1}{2}}\right)^2 + C, \tag{2.2}$$

where $\{F = F_1, \ldots, F_n\}$ is the conjugate set of F, and β is totally real, with all its conjugates non negative.

Conversely, given $C \in \mathbb{Q}$, $F \in S_{\mathfrak{P}}$ and β totally real, with all its conjugates non negative, the algebraic number given by Equation (2.2) lies with its conjugates on $\mathfrak{P}(C, F)$.

It may be possible to reduce the lower bound on $\deg(\alpha)$ in Theorem 2.1.2 to 5, but no further, since there exist algebraic numbers of degree 4 that lie on a parabola with non rational focus.

Theorem 2.1.3 (Ellipses). *Let α be an algebraic number of degree at least 25, whose conjugate set lies on an ellipse $\mathfrak{E}(C, R, B, \epsilon)$. Then*

1. *$C, R^2 \in \mathbb{Q}$, and $B^{k(B)} \in S_{\mathfrak{E}}$.*

2. *Let*
$$\alpha^* = T_{k(B)}\left(\frac{(\alpha - C)\epsilon^{\frac{1}{2}}}{R}\right). \tag{2.3}$$
Then α^* lies with all its conjugates on $\mathfrak{E}(0, 1, B^{k(B)}, 1)$.

3. *In view of (2) above, we need only consider $C = 0, R = 1, k(B) = 1, \epsilon = 1$. Here α has a conjugate of the form $\nu + \nu^{-1}$, where*
$$\nu = \frac{1}{2}(\beta + (\beta^2 - 4)^{\frac{1}{2}})\left(\prod_{j=1}^{n} B_j\right)^{\frac{1}{2}}, \tag{2.4}$$
where $B = B_1$ and either $B \in \mathbb{Q}$ and $n = 1$, or $\{B_1^{\pm 1}, B_2^{\pm 1}, \ldots, B_n^{\pm 1}\}$ is the conjugate set of B. Also β is totally real, with its conjugate set lying in the interval $[-2, 2]$.

   Conversely, let $B \in S_{\mathfrak{E}}$ and β be totally real, with its conjugate set lying in the interval $[-2, 2]$. Then

4. *$\alpha = \nu + \nu^{-1}$, where ν is given by Equation (2.4), and the conjugate set of α lies on $\mathfrak{E}(0, 1, B, 1)$.*

5. *Let $C, R^2 \in \mathbb{Q}$ and $B^{k(B)} \in S_{\mathfrak{E}}$.*

   Use (4) to define α^* on $\mathfrak{E}(0, 1, B^{k(B)}, 1)$. Then if α is a root of Equation (2.3), then α lies with its conjugates on $\mathfrak{E}(C, R, B, \epsilon)$.

Theorem 2.1.4 (Hyperbolas). *Let α be an algebraic number of degree at least 25 whose conjugate set lies on a hyperbola $\mathfrak{H}(C, R, B, \epsilon)$. Then*

1. *$C, R^2 \in \mathbb{Q}, k(B) = 1$ or 2, and $B^{k(B)} \in S_{\mathfrak{H}}$.*

2. *If $B \neq \pm i$ and α^* is defined by Equation (2.3), then α^* and all its conjugates lie on the hyperbola $\mathfrak{H}(0, 1, (\epsilon B)^{k(B)}, 1)$. Furthermore, if $k(B) = 2$ then t is positive.*

3. *If $B \neq \pm i$, then $\alpha^* = (\alpha - C)^2$ and all its conjugates lie on the vertical line $\Re(\alpha^*) = 2\epsilon R^2$, and so*
$$\alpha^* = 2\epsilon R^2 + i\beta \tag{2.5}$$
for some totally real β (cf Corollary 2.1.6).

4. *In view of (2) and (3), we need only consider the case $B \neq \pm i, C = 0, R = 1, k(B) = 1, \epsilon = 1$. Here α has a conjugate of the form $\nu + \nu^{-1}$, where ν is given by Equation (2.4), with $B = B_1$, $\{B_1^{\pm 1}, \ldots, B_n^{\pm 1}\}$ is the conjugate set of B, and β totally real, with conjugate set lying in $(-\infty, -2] \cup [2, \infty)$.*

   Conversely, let $B \in S_{\mathfrak{H}}$ and β be totally real, with conjugate set lying in $(-\infty, -2] \cup [2, \infty)$. Then

5. *$\alpha = \nu + \nu^{-1}$, where ν is given by Equation (2.4), and the conjugate set of α lies on $\mathfrak{H}(0, 1, B, 1)$.*

6. *Let $C, R^2 \in \mathbb{Q}, B \neq \pm i$, $k(B) = 1$ or 2, and $B^{k(B)} \in S_{\mathfrak{H}}$. Use (5) to define α^* on $\mathfrak{H}(0, 1, (\epsilon B)^{k(B)}, 1)$, with the conjugate set of α^* all having positive parameter t. Then if α is a root of Equation (2.3), α lies with its conjugates on $\mathfrak{H}(C, R, B, \epsilon)$.*

7. *Let $C, R^2 \in \mathbb{Q}, B = \pm i$, $k(B) = 1$ or 2, and let β totally real. Then*
$$\alpha = C + (2\epsilon R^2 + i\beta)^{\frac{1}{2}}$$
lies with its conjugates on $\mathfrak{H}(C, R, B, \epsilon)$.

Again the lower bound on $\deg(\alpha)$ may be reduced from 25 to 7, and there exist algebraic numbers of degree 6 that lie on ellipses or hyperbolas with irrational centre.

Notation. For an algebraic number α with conjugate α_j say, it is understood that by $\alpha_{\bar{j}}$ we mean the complex conjugate $\overline{\alpha_j}$ of α_j, and applying an automorphism σ to the conjugates of α will map $\alpha_j \mapsto \alpha_{\sigma(j)}$ and $\alpha_{\bar{j}} \mapsto \alpha_{\sigma(\bar{j})}$ respectively.

The following lemma, taken from [23], is the main result used in classifying all algebraic numbers that lie with their conjugates on a straight line (Corollary 2.1.6). It is also used frequently in the subsequent work on the two lines problem.

Lemma 2.1.5. *Let α, α_1 and α_2 be distinct conjugate algebraic numbers. Then for any choice of signs,*

$$\alpha_1 \pm \alpha_2 \neq \pm 2\alpha.$$

Proof. Suppose that $\alpha_1 \pm \alpha_2 = \pm 2\alpha$ for some distinct conjugates α, α_1 and α_2. Let α_3 be a conjugate of α with maximal absolute value. By Proposition 1.4.4, there exists an automorphism σ that maps $\alpha \mapsto \alpha_3$. Applying σ to

$$\alpha_1 \pm \alpha_2 = \pm 2\alpha$$

gives

$$\alpha_{\sigma(1)} \pm \alpha_{\sigma(2)} = \pm 2\alpha_3.$$

We know that

$$|\alpha_{\sigma(1)} \pm \alpha_{\sigma(2)}| \leq 2|\alpha_3|,$$

so $\alpha_{\sigma(1)} = \pm\alpha_{\sigma(2)}$ and α_3 is equal to at least one of $\alpha_{\sigma(1)}, \alpha_{\sigma(2)}$. Applying σ^{-1} contradicts the distinctness of α, α_1 and α_2. □

The following is also taken from [23]:

Corollary 2.1.6. *Let α be an algebraic number that lies with its conjugates on a single line in the complex plane. Then α is either totally real, or is of the form $p + it$, where $p \in \mathbb{Q}$ and t is totally real.*

Proof. Suppose that α is not totally real, so that it has a conjugate $\alpha_1 = p+it \notin \mathbb{R}$. Then by Lemma 1.1.5, $\alpha_{\overline{1}} = p - it$ is also a conjugate of α. So the conjugate set of α all lie on $\Re(z) = p$. Let F be the normal closure of $\mathbb{Q}(p, t)$. Now apply an automorphism $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ that maps $p \mapsto p'$. Then

$$\sigma(p) = \sigma\left(\frac{1}{2}(\alpha_1 + \alpha_{\overline{1}})\right) = \frac{1}{2}(\alpha_{\sigma(1)} + \alpha_{\sigma(\overline{1})}),$$

so

$$\sigma(p) = p'$$

must lie on $\Re(z) = p$. Suppose $p' \notin \mathbb{R}$. Then p has conjugates $p' = p + ir$ and $\overline{p'} = p - ir$ for some $r \in \mathbb{R}$. But then

$$p' + \overline{p'} = 2p,$$

contradicting Lemma 2.1.5. Hence $p' \in \mathbb{R}$, so $p' = p$. Therefore, p is fixed by all $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, so by Corollary 1.4.9, $p \in \mathbb{Q}$.

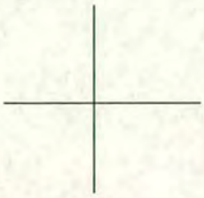
Now suppose t is not totally real, and apply an automorphism τ that maps $t \mapsto t' \notin \mathbb{R}$. Then

$$\tau(p + it) = \tau(p) + \tau(it) = p \pm it'$$

does not lie on $\Re(z) = p$. Hence t is totally real. □

2.2 Classification of Lines

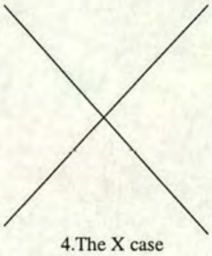
Consider the following four possible pairs of lines:



1.The + Case

2.The = Case

3.The || Case



4.The X case

1. The lines $\Re(z) = p$ and the real axis $\mathbb{R}$. For ease of reference, we will refer to these two lines as the + case. It has one real parameter, p, and α and all its conjugates are contained in the set
$$S_+(p) := \mathbb{R} \cup \{z : \Re(z) = p\}.$$

2. The two horizontal lines $\Im(z) = \sqrt{h}$ and $\Im(z) = -\sqrt{h}$ $(h > 0)$. These two lines will be referred to as the = case. It also has one parameter, h, and α and all its conjugates are contained in the set
$$S_=(-h) := \{z : \Im(z) = \sqrt{h}\} \cup \{z : \Im(z) = -\sqrt{h}\}.$$

3. The two vertical lines $\Re(z) = p$ and $\Re(z) = q$ $(p \neq q)$. This case will be referred to as the || case, and has two real parameters, p and q. Here α and all its conjugates are contained in the set
$$S_{\|}(p,q) := \{z : \Re(z) = p\} \cup \{z : \Re(z) = q\}.$$

4. The two lines $z(t) = C + tu^{\pm\frac{1}{2}}$ $(t \in \mathbb{R}, |u| = 1)$. This case will be referred to as the × case, and has two parameters, C (the point of intersection of the two lines) and u (equal to $e^{2i\theta}$, where $0 < \theta < \frac{\pi}{2}$ is the angle between the positive real axis and the line with positive gradient). Here α and its conjugates are contained in the set
$$S_\times(C, \sqrt{u}) := \{z : z(t) = C + tu^{\pm\frac{1}{2}} | t \in \mathbb{R}, |u| = 1\}.$$

The following proposition shows the significance of these four types of pairs of lines:

Proposition 2.2.1. *Let α be an algebraic number that lies with its conjugates on a pair of straight lines in the complex plane. Then the pair of lines can be taken to be one of the four types given above, i.e. we can replace (if necessary) the pair of lines by one of the four types.*

Proof. Let P_α be the minimal polynomial of α. Any algebraic number α has an even number of non real conjugates, since if $\alpha_i \notin \mathbb{R}$ is a root of P_α, then by Lemma 1.1.5 so is its complex conjugate $\alpha_{\bar{i}}$, and $\overline{\alpha} = \alpha$ if and only if $\alpha \in \mathbb{R}$. Moreover, if α has no non real conjugates, then α and all its conjugates lie on a single line, the real axis $\mathbb{R}$. If α has two non real conjugates, then either α and all its conjugates lie on a single vertical line (if the degree of α is two), or the pair of lines given by case (1) above.

Suppose α has at least four non real conjugates. If all the non real conjugates have the same real part, then α and all its conjugates lie either on a single vertical line, or the pair of lines given by case (1) above. So suppose that there exists non-real conjugates $\alpha_1, \alpha_{\bar{1}}, \alpha_2$ and $\alpha_{\bar{2}}$ of α such that $\Re(\alpha_1) \neq \Re(\alpha_2)$. Thus no three of the above four conjugates are collinear, and there exists three possible pairs of lines on which the conjugates lie:

1. Two vertical lines, one joining α_1 and $\alpha_{\bar{1}}$, the other joining α_2 and $\alpha_{\bar{2}}$. These lines are categorized by case (3).

2. The line joining α_1 and α_2, and the line joining $\alpha_{\bar{1}}$ and $\alpha_{\bar{2}}$. If $\Im(\alpha_1) = \Im(\alpha_2)$, then the pair of lines are horizontal, and are categorized by case (2). If $\Im(\alpha_1) \neq \Im(\alpha_2)$, then the pair of lines intersect, and are symmetric about the real axis, so are categorized by case (4).

3. The line joining α_1 and $\alpha_{\bar{2}}$, and the line joining $\alpha_{\bar{1}}$ and α_2. The choice of calling a particular conjugate α_i or $\alpha_{\bar{i}}$ is arbitrary, so the lines are categorized as in case (2) above.

If $\deg(\alpha) = 4$, then any of the above pairs of lines will suffice. If $\deg(\alpha) > 4$, then the conjugate set of α will lie on exactly one of the pairs of lines considered above. □

2.3 Results

The results of the two lines problem are:

(1) **The + Case**

Theorem 2.3.1. *Let p and a be totally real algebraic numbers such that a is negative, $\mathbb{Q}(p) \subset \mathbb{Q}(a)$, and the minimal polynomial P_a of a factorises over $\mathbb{Q}(p)$ as*

$$P_a(x) = f(p, x)Q_a(x), \tag{2.6}$$

where

$$Q_a(x) = \prod_{p' \neq p} f(p', x) \tag{2.7}$$

does not necessarily factorise, p' is a conjugate of p, $f(p, x)$ is the minimal polynomial of a over $\mathbb{Q}(p)$ and has at least two negative roots, and $f(p', x)$ has all roots positive for $p' \neq p$. Define $\alpha = p + \sqrt{a}$. Then α has more than two non real conjugates, and lies with its conjugates on $S_+(p)$.

Conversely, suppose that α is an algebraic number that has more than two non-real conjugates and lies with its conjugates on $S_+(p)$ for some $p \in \mathbb{R}$. Then p is totally real, α is of the form $\alpha = p' + \sqrt{a'}$, where p' is a conjugate of p, and a' is a conjugate of a, where a is totally real and negative, with $\mathbb{Q}(a) \supset \mathbb{Q}(p)$. The minimal polynomial P_a of a factorises over $\mathbb{Q}(p)$ as in Equation (2.6), where Equation (2.7) does not necessarily factorise, $f(p, x)$, the minimal polynomial of a over $\mathbb{Q}(p)$, has at least two negative roots, and $f(p', x)$ has all roots positive for $p' \neq p$.

Remark. Theorem 2.3.1 only considers algebraic numbers with more than two non real conjugates. Note that any algebraic number with exactly two non real conjugates lies with its conjugates on $S_+(p)$ for some algebraic p.

(2) **The = Case**

Theorem 2.3.2. *Let h be a totally real, negative, algebraic number whose conjugates $h_2, \ldots, h_g$ are all positive. Let r be a totally real algebraic number, and let $\epsilon_j = \pm 1$ for $j = 1, \ldots, g$. Define*

$$\alpha = r + \epsilon_1\sqrt{h} + \epsilon_2\sqrt{h_2} + \cdots + \epsilon_g\sqrt{h_g}.$$

Then α lies with all its conjugates on $S_=(h)$.

Conversely, suppose that for some h, there exists an algebraic number α whose conjugate set lies on $S_=(h)$. Then h is totally real and negative with conjugates $h_2, \ldots, h_g$ all positive, and there exists some totally real number r such that

$$\alpha = r + \epsilon_1\sqrt{h} + \epsilon_2\sqrt{h_2} + \cdots + \epsilon_g\sqrt{h_g},$$

where $\epsilon_j = \pm 1$ for $1 \leq j \leq g$.

(3) **The $\|$ Case**

Theorem 2.3.3. *1. Let p and q be distinct real algebraic numbers such that $p, q \notin \mathbb{Q}$, $p+q \in \mathbb{Q}$ and $h = (\frac{p-q}{2})^2$ is totally real with all other conjugates $h_2, \ldots, h_g$ of h negative. Let r be a totally real algebraic number and let $\epsilon_j = \pm 1$ for $j = 1, \ldots, g$. Define*

$$\alpha = \frac{p+q}{2} + \epsilon_1\sqrt{h} + \epsilon_2\sqrt{h_2} + \cdots + \epsilon_g\sqrt{h_g} + ir.$$

Then α lies with all its conjugates on $S_{\|}(p,q)$.

2. Let p be the real root of a non totally real cubic, with conjugates p_1 and $p_{\bar{1}}$. Let $\Re(p_1) = q$, and let r be totally real. Define $\alpha = p + ir$. Then α lies with all its conjugates on $S_{\|}(p,q)$.

Conversely, suppose that for some distinct real algebraic numbers p and q, there exists an algebraic number α whose conjugate set lies on $S_{\|}(p,q)$. Then either

1. *$p+q \in \mathbb{Q}$, $p, q \notin \mathbb{Q}$ and*

$$\alpha = \frac{p+q}{2} + \epsilon_1\sqrt{h} + \epsilon_2\sqrt{h_2} + \cdots + \epsilon_g\sqrt{h_g} + ir,$$

where $h = \left(\frac{p-q}{2}\right)^2$ is totally real with conjugates $h_2, \ldots, h_g$ all negative, r is totally real, and $\epsilon_j = \pm 1$ for $j = 1, \ldots, g$, or

2. *p is the real root of a non totally real cubic, whose non real roots have real part q, and α can be uniquely defined as $p' + ir$, where p' is a conjugate of p and r is totally real.*

(4) **The × Case**

Theorem 2.3.4. *Let C, u and α be defined in one of the following ways:*

1. *Let $C \in \mathbb{Q}(\sqrt{n})$ be quadratic for some square-free $n \in \mathbb{N}$, with conjugate $C' \neq C$. Let $u = i$, and let r be totally real. Define*

$$\alpha = \frac{C+C'}{2} + i\frac{C'-C}{2} + r\sqrt{\epsilon i(C'-C)},$$

where

$$\epsilon = \begin{cases} 1, & \text{if } C < C'; \\ -1, & \text{if } C' < C. \end{cases}$$

2. Let $C \in \mathbb{Q}(\sqrt{n})$ be quadratic for some square-free $n \in \mathbb{N}$, with conjugate $C' \neq C$. Let $u = \frac{a\sqrt{n}+b\sqrt{-k}}{e}$ be such that $a \in \mathbb{N}_{\geq 0}$, $e \in \mathbb{N}$, $b \in \mathbb{Z}^*$, $k \in \mathbb{N}$ is square-free or equal to 1, and $a^2n + b^2k = e^2$. Let r be totally real. Define
$$\alpha = \frac{C+C'}{2} + u\frac{C'-C}{2} + r\sqrt{u(u+u^{-1})}.$$

3. Let $C \in \mathbb{Q}$, $u = i$, and define
$$\alpha = C + \sqrt{ir}$$
where r is totally real.

4. Let $C \in \mathbb{Q}$, let $u = u_1 = e^{2i\theta}$ have conjugates $u_1^{-1}, \ldots, u_g, u_g^{-1}$ where $u_j \in \mathbb{R}$ for $2 \leq j \leq g$, and let r be totally real. Define
$$\alpha = C + r\sqrt{\delta u_1 u_2 \cdots u_g},$$
where
$$\delta = \begin{cases} 1, & \text{if } u_2 \ldots u_g > 0; \\ -1, & \text{if } u_2 \ldots u_g < 0, \end{cases}$$
and r is totally real.

5. Let $C \in \mathbb{Q}$, let $u = u_1 = e^{2i\theta}$ have conjugates $\pm u_1^{\pm 1}, \ldots, \pm u_g^{\pm 1}$, where $u_j \in \mathbb{R}$ for $2 \leq j \leq g$. Define
$$\alpha = C + r\sqrt{\delta u_1 u_2 \cdots u_g (u_1 + u_1^{-1})(u_2 + u_2^{-1}) \cdots (u_g + u_g^{-1})},$$
where
$$\delta = \begin{cases} 1, & \text{if } (u_1 + u_1^{-1}) > 0; \\ -1, & \text{if } (u_1 + u_1^{-1}) < 0, \end{cases}$$
and r is totally real.

Then α lies with all its conjugates on $S_\times(C, \sqrt{u})$.

Conversely, let α be an algebraic number of degree at least 10 that lies with its conjugates on $S_\times(C, \sqrt{u})$. Then either $C \in \mathbb{Q}(\sqrt{n})$ is quadratic with conjugate $C' \neq C$, $n \in \mathbb{N}$ is square-free, and α can be written in one of the following forms:

1.
$$\alpha = \frac{C+C'}{2} + i\frac{C'-C}{2} + r\sqrt{\epsilon i(C'-C)},$$
where $u = i$, r is totally real and
$$\epsilon = \begin{cases} 1, & \text{if } C' > C; \\ -1, & \text{if } C > C', \text{ or} \end{cases}$$

2.

$$\alpha = \frac{C+C'}{2} + u\frac{C'-C}{2} + r\sqrt{u(u+u^{-1})}$$

where $u = \frac{a\sqrt{n}+b\sqrt{-k}}{e}$, $a \in \mathbb{N}_{\geq 0}$, $e \in \mathbb{N}$, $b \in \mathbb{Z}^*$, $k \in \mathbb{N}$ *is square-free or equal to* 1, *and* r *is totally real,*

or $C \in \mathbb{Q}$, *and* α *can be written in one of the following ways:*

1. $\alpha = C + \sqrt{ir}$, $u = i$ *and* r *is totally real, or*

2.

$$\alpha = C + r\sqrt{\delta u_1 u_2 \cdots u_g},$$

$u = e^{2i\theta}$ *has conjugates* u_1^{-1}, *and* $u_j^{\pm 1} \in \mathbb{R}$ *for* $2 \leq j \leq g$, r *is totally real and*

$$\delta = \begin{cases} 1, & \text{if } u_2 \ldots u_g > 0; \\ -1, & \text{if } u_2 \ldots u_g < 0, \text{ or} \end{cases}$$

3.

$$\alpha = C + r\sqrt{u_1 u_2 \cdots u_g (u_1 + u_1^{-1})(u_2 + u_2^{-1}) \cdots (u_g + u_g^{-1})},$$

$u = u_1 = e^{2i\theta}$ *has conjugates* $\pm u_j^{\pm 1}$ *where* $u_j \in \mathbb{R}$ *for* $2 \leq j \leq g$, r *is totally real and*

$$\delta = \begin{cases} 1, & \text{if } (u_1 + u_1^{-1}) > 0; \\ -1, & \text{if } (u_1 + u_1^{-1}) < 0. \end{cases}$$

Chapter 3

Proof Of The + Case

In this chapter, we prove Theorem 2.3.1, categorizing algebraic numbers whose conjugate set all lie on $S_+(p)$.

3.1 Lemmas Required For The Proof

Lemma 3.1.1. *Let p and a be algebraic numbers, and define*

$$\alpha = p + \sqrt{a}. \tag{3.1}$$

1. *All conjugates of α are of the form $\alpha' = p' \pm \sqrt{a'}$, where p' is a conjugate of p and a' is a conjugate of a.*

2. *For each conjugate p' of p there is a conjugate a'' of a such that at least one of $p' \pm \sqrt{a''}$ is a conjugate of α. Similarly, for each conjugate a' of a there is a conjugate p'' of p such that at least one of $p'' \pm \sqrt{a'}$ is a conjugate of α.*

Proof. Let K be the normal closure of $\mathbb{Q}(\alpha)$, and let σ be an automorphism in $\mathrm{Gal}(K/\mathbb{Q})$ that maps $\alpha \mapsto \alpha'$. Then applying σ to

$$(\alpha - p)^2 - a = 0, \tag{3.2}$$

we get $(\alpha' - p')^2 - a' = 0$, which gives $\alpha' = p' \pm \sqrt{a'}$.

Now for any given conjugate p' of p, apply an automorphism $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ that maps $p \mapsto p'$ to Equation (3.2). This gives

$$\alpha'' = p' \pm \sqrt{a''},$$

where α'' is a conjugate of α and a'' is a conjugate of a. Similarly, applying an automorphism that maps $a \mapsto a'$ to Equation (3.2) will map α to a conjugate $\alpha'' = p'' \pm \sqrt{a'}$. □

Lemma 3.1.2. *Let α be an algebraic number, with more than two non-real conjugates, whose conjugate set lies on $S_+(p)$. Consider a non-real conjugate of α, say α_1, and its complex conjugate $\alpha_{\overline{1}}$. Any automorphism ϕ applied to α_1 and $\alpha_{\overline{1}}$ results in one of the following. Either:*

1. $\alpha_{\phi(1)}, \alpha_{\phi(\overline{1})} \in \mathbb{R}$, *or*

2. $\alpha_{\phi(1)}$ *and* $\alpha_{\phi(\overline{1})}$ *both lie on* $\Re(z) = p$.

Proof. Suppose there exists an automorphism ϕ that maps $\alpha_1 \mapsto \alpha_{\phi(1)} = r \in \mathbb{R}$ and $\alpha_{\overline{1}} \mapsto \alpha_{\phi(\overline{1})} = p + i\lambda \notin \mathbb{R}$. Let $\alpha_2, \alpha_{\overline{2}}$ be two non-real conjugates distinct from α_1 and $\alpha_{\overline{1}}$. Applying ϕ to

$$2p = \alpha_1 + \alpha_{\overline{1}} = \alpha_2 + \alpha_{\overline{2}}$$

gives

$$2p' = (p + r) + i\lambda = \alpha_{\phi(2)} + \alpha_{\phi(\overline{2})}, \tag{3.3}$$

with $\alpha_{\phi(2)}, \alpha_{\phi(\overline{2})}$ distinct from $\alpha_{\phi(1)}, \alpha_{\phi(\overline{1})}$. So

$$\Im(\alpha_{\phi(2)} + \alpha_{\phi(\overline{2})}) = \lambda.$$

If both $\alpha_{\phi(2)}$ and $\alpha_{\phi(\overline{2})}$ lie on $\Re(z) = p$, then equating the real parts of Equation (3.3) gives $\alpha_{\phi(1)} = p$, and so

$$2\alpha_{\phi(1)} = \alpha_1 + \alpha_{\overline{1}},$$

contradicting Lemma 2.1.5.

If exactly one of $\alpha_{\phi(2)}, \alpha_{\phi(\overline{2})}$ lies on $\Re(z) = p$, then on equating real parts of Equation (3.3), we see that one of $\alpha_{\phi(2)}, \alpha_{\phi(\overline{2})}$ is equal to $\alpha_{\phi(\overline{1})}$, contradicting the distinctness of $\alpha_{\overline{1}}, \alpha_2$ and $\alpha_{\overline{2}}$. Thus $\alpha_{\phi(1)}$ and $\alpha_{\phi(\overline{1})}$ are either both real (case 1), or both have real part p (case 2). □

3.2 Proof Of Theorem 2.3.1

Proof. ($\Rightarrow$) Let p, a, α, f, P_a and Q_a be defined as in the theorem. Then $\alpha = p + \sqrt{a}$ lies on the line $\Re(z) = p$. For some index set i, let $\{\tau_i\}$ be the set of automorphisms that map α to any non real conjugate. Since α has more than two non real conjugates, at least four such τ_i exist, by Proposition 1.4.4. Note that $\tau_i(a) < 0$ for all i, as $\tau_i(\alpha) \notin \mathbb{R}$. Recall that P_a factorises over $\mathbb{Q}(p)$ as

$$P_a(x) = f(p, x)Q_a(x),$$

where

$$Q_a(x) = \prod_{p' \neq p} f(p', x)$$

does not necesarily factorise, and all roots $a' < 0$ are roots of $f(p, x)$. So $\tau_i(p) = p$ for all i, and all non real conjugates α' of α are of the form $p \pm \sqrt{a'}$, where a' is a negative conjugate of a. Hence all non real conjugates α' of α lie on $\Re(z) = p$, so α and all its conjugates lie on $S_+(p)$.

($\Leftarrow$) Let α be an algebraic number that has more than two non real conjugates, and whose conjugate set lies on $S_+(p)$. First we show that p is totally real. Let $\alpha_1, \alpha_{\overline{1}}, \alpha_2$ and $\alpha_{\overline{2}}$ be distinct conjugates of α that all lie on $\Re(z) = p$. Applying an automorphism ϕ to

$$\alpha_1 + \alpha_{\overline{1}} = \alpha_2 + \alpha_{\overline{2}} = 2p$$

gives

$$\alpha_{\phi(1)} + \alpha_{\phi(\overline{1})} = \alpha_{\phi(2)} + \alpha_{\phi(\overline{2})} = 2\phi(p) = 2p',$$

where $\alpha_{\phi(1)}, \alpha_{\phi(\overline{1})}, \alpha_{\phi(2)}$ and $\alpha_{\phi(\overline{2})}$ are distinct conjugates of α, and p' is a conjugate of p. By Lemma 3.1.2, either $\alpha_{\phi(1)}$ and $\alpha_{\phi(\overline{1})}$ are both real or both lie on the line $\Re(z) = p$. If they are both real, then p' is real. Suppose they both lie on $\Re(z) = p$. Then either

$$\alpha_{\phi(1)} + \alpha_{\phi(\overline{1})} = 2p,$$

in which case $p' = p$ is real, or

$$\alpha_{\phi(1)} + \alpha_{\phi(\overline{1})} = 2p + i\theta = 2p'$$

for some $\theta \in \mathbb{R}^*$. But then

$$\alpha_{\overline{\phi(1)}} + \alpha_{\overline{\phi(\overline{1})}} = 2p - i\theta = 2\overline{p'},$$

and so $2p = p' + \overline{p'}$, contradicting Lemma 2.1.5. Hence p is totally real.

By Lemma 3.1.1, there exists a non real conjugate $\alpha_1 = p + \sqrt{a}$ of α. We show that a is totally real. Consider

$$\alpha_1 - \alpha_{\overline{1}} = 2\sqrt{a}. \tag{3.4}$$

Squaring Equation (3.4) gives

$$(\alpha_1 - \alpha_{\overline{1}})^2 = 4a. \tag{3.5}$$

Applying an automorphism τ to Equation (3.5) gives

$$(\alpha_{\tau(1)} - \alpha_{\tau(\overline{1})})^2 = 4a'.$$

By Lemma 3.1.2, $\alpha_{\tau(1)}$ and $\alpha_{\tau(\overline{1})}$ are either both real, or both lie on the line $\Re(z) = p$. If $\alpha_{\tau(1)}$ and $\alpha_{\tau(\overline{1})}$ are both real, then clearly $a' \in \mathbb{R}_{>0}$. So suppose that $\alpha_{\tau(1)}$ and $\alpha_{\tau(\overline{1})}$ both lie on $\Re(z) = p$. Let $\alpha_{\tau(1)} = p + i\theta$ and $\alpha_{\tau(\overline{1})} = p + i\lambda$, where $\theta, \lambda \in \mathbb{R}$. Then

$$(\alpha_{\tau(1)} - \alpha_{\tau(\overline{1})})^2 = ((p + i\theta) - (p + i\lambda))^2 = -(\theta - \lambda)^2 \in \mathbb{R}_{<0}.$$

So a' is real, hence a is totally real.

Next we show that $\mathbb{Q}(a) \supset \mathbb{Q}(p)$. Suppose that $p \notin \mathbb{Q}(a)$. There is a tower

$$\begin{tikzcd} K \arrow[d, dash] \\ \mathbb{Q}(a) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

where K is a splitting field for p, a and α, and $\mathbb{Q}(a)$ is an intermediate field of the galois extension $K/\mathbb{Q}$. By the Fundamental Theorem of Galois Theory 1.4.8, K is galois over $\mathbb{Q}(a)$ and there exists an automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(a))$ that maps $p \mapsto p' \neq p$. Thus

$$\alpha_{\sigma(1)} = p' \pm \sqrt{a}.$$

Since p' is real (as p is totally real), and a is real and negative, $\alpha_{\sigma(1)}$ does not lie on $S_+(p)$. So such an automorphism σ does not exist, and therefore $p \in \mathbb{Q}(a)$, i.e. $\mathbb{Q}(p) \subset \mathbb{Q}(a)$.

Thus the minimal polynomial P_a of a must factorise over a splitting field F for p as

$$P_a(x) = f(p, x)Q_a(x),$$

where

$$Q_a(x) = f(p', x)f(p'', x) \cdots,$$

$a = (\alpha - p)^2$ is a root of $f(p, x)$, $a' = (\alpha' - p')^2$ is a root of $f(p', x)$, $a'' = (\alpha'' - p'')^2$ is a root of $f(p'', x)$, and so on. Now $f(p, x)$ is irreducible over $\mathbb{Q}(p)$, as its roots are conjugate over $\mathbb{Q}(p)$. Furthermore, a is a root of $f(p, x)$, so $f(p, x)$ must be the minimal polynomial of a over $\mathbb{Q}(p)$.

If a conjugate a_i of a is negative, then clearly $a_i = (\alpha_i - p)^2$ for some $\alpha_i \notin \mathbb{R}$, and so a_i is a root of $f(p, x)$. Moreover, as α has more than two non real conjugates, there must be at least two such $a_i < 0$. Thus $f(p, x)$ has at least two negative roots, and for every $p' \neq p$, the factor $f(p', x)$ of $P_a(x)$ has all roots positive, a being totally real. □

We can construct a "suitable" a given p as follows:

Proposition 3.2.1. *Let p be a totally real algebraic number. Then there exists a negative totally real algebraic number a such that $p \in \mathbb{Q}(a)$, a has at least one other negative conjugate, and whenever an automorphism maps $p \mapsto p' \neq p$, then $a \mapsto a' > 0$.*

Proof. Let $q \in \mathbb{Q}$ be chosen such that $q < p$ and for all conjugates $p' < p$ of p, $q > p'$. Define $b = \frac{1}{p-q}$. Then $b > 0$, and for all conjugates $b' \neq b$ of b, $b > b'$. Let $r \in \mathbb{Q}$ be such that $r < b$, and $r > b'$ for all $b' \neq b$ conjugate to b. Let $\gamma \notin \mathbb{Q}(b)$ be totally real, and let $\epsilon \in \mathbb{Q}$ be sufficiently small so that

$$\min_{b'} |b' - r| > \epsilon\gamma'$$

for each conjugate γ' of γ. Define

$$a = r - b + \epsilon\gamma.$$

Then a is a negative totally real algebraic number such that $p \in \mathbb{Q}(a)$. Also, a has at least one other negative conjugate, produced for instance by acting on a by an automorphism that fixes $\mathbb{Q}(a)$ and maps $\gamma \mapsto \gamma' \neq \gamma$. Furthermore, whenever an automorphism maps $p \mapsto p' \neq p$, then $b \mapsto b' < r$ and so $a \mapsto a' > 0$. □

3.3 Examples

Example 3.3.1. Let $p = -\sqrt{17}$, and $a = 1 + \sqrt{17} + \sqrt{5}$. Then

$$\mathbb{Q}(p) = \mathbb{Q}(\sqrt{17}) \cap \mathbb{Q}(a) = \mathbb{Q}(\sqrt{17})$$

and

$$P_a(z) = z^4 + 4z^3 - 38z^2 - 84z + 101.$$

Note that p has conjugates $p = -\sqrt{17}$ and $p' = \sqrt{17}$, and P_a factorises over $\mathbb{Q}(\sqrt{17})$ into

$$(z^2 + z(2 + 2\sqrt{17}) + (13 + 2\sqrt{17}))(z^2 + z(2 - 2\sqrt{17}) + (13 - 2\sqrt{17})).$$

Here $Q_a(z) = z^2 + (2 + 2\sqrt{17})z + (13 + 2\sqrt{17})$. The conjugates of a are

$$a = 1 + \sqrt{17} + \sqrt{5}$$

$$a' = 1 + \sqrt{17} - \sqrt{5}$$

$$a'' = 1 - \sqrt{17} + \sqrt{5}$$

$$a''' = 1 - \sqrt{17} - \sqrt{5},$$

and the conjugates of α are

$$\begin{aligned}
\alpha &= p' + \sqrt{a} = \sqrt{17} + \sqrt{1 + \sqrt{17} + \sqrt{5}} \\
\alpha' &= p' - \sqrt{a} = \sqrt{17} - \sqrt{1 + \sqrt{17} + \sqrt{5}} \\
\alpha'' &= p' + \sqrt{a'} = \sqrt{17} + \sqrt{1 + \sqrt{17} - \sqrt{5}} \\
\alpha''' &= p' - \sqrt{a'} = \sqrt{17} - \sqrt{1 + \sqrt{17} - \sqrt{5}} \\
\alpha_2 &= p + \sqrt{a''} = -\sqrt{17} + \sqrt{1 - \sqrt{17} + \sqrt{5}} \\
\alpha_{\bar{2}} &= p - \sqrt{a''} = -\sqrt{17} - \sqrt{1 - \sqrt{17} + \sqrt{5}} \\
\alpha_3 &= p + \sqrt{a'''} = -\sqrt{17} + \sqrt{1 - \sqrt{17} - \sqrt{5}} \\
\alpha_{\bar{3}} &= p - \sqrt{a'''} = -\sqrt{17} - \sqrt{1 - \sqrt{17} - \sqrt{5}}.
\end{aligned}$$

Here α and all its conjugates lie on $S_+(-\sqrt{17})$.

Theorem 2.3.1 describes all algebraic numbers that have more than two non-real conjugates and lie with all their conjugates on $S_+(p)$. However, if only two conjugates lie on the line $\Re(z) = p$, then Theorem 2.3.1 does not apply, and p need not be totally real. For example:

Proposition 3.3.2. *Let α be an algebraic number of degree q, where q is prime, such that α has exactly two non real conjugates. Then p is not totally real.*

Proof. Let G be the galois group of $\mathrm{Gal}(L/\mathbb{Q})$, where L is the normal closure of α, and let $\alpha_1, \alpha_{\bar{1}}$ be the non-real conjugates of α, with real part p. By Theorem 1.4.12, $G = S_q$. Hence $p = \frac{1}{2}(\alpha_1 + \alpha_{\bar{1}})$ has $\binom{q-2}{2} + 1$ real conjugates, and $2q - 4$ non real conjugates. Hence p is not totally real. □

Chapter 4

Proof Of The = Case

In this chapter, we study the case where α and all its conjugates lie on $S_=(h)$, a pair of horizontal lines symmetric in the real axis.

4.1 Results Required For The Proof

Notation. In the following two results, we denote the set of elements of a field K that are squares in K by K^2.

Lemma 4.1.1. *Suppose that $b_1, \ldots, b_g \in K$, a field of characteristic zero, and that $[K(\sqrt{b_1}, \ldots, \sqrt{b_g}) : K] = 2^g$. Then*

$$K(\sqrt{b_1}, \ldots, \sqrt{b_g})^2 \cap K = \bigcup_{\epsilon_i \in \{0,1\}} b_1^{\epsilon_1} \cdots b_g^{\epsilon_g} K^2.$$

Proof. Use induction on g.

The result is trivial for $g = 0$. Suppose $g \geq 1$, and that

$$K(\sqrt{b_1}, \ldots, \sqrt{b_r})^2 \cap K = \bigcup_{\epsilon_i \in \{0,1\}} b_1^{\epsilon_1} \cdots b_r^{\epsilon_r} K^2$$

for all $r \in \{1, \ldots, g-1\}$. Set $K_{g-1} = K(\sqrt{b_1}, \cdots, \sqrt{b_{g-1}})$, and suppose that $(a + c\sqrt{b_g})^2 \in K$, where $a, c \in K_{g-1}$. Then one of a or c must equal zero, since $\sqrt{b_g} \notin K_{g-1}$. Hence

$$K(\sqrt{b_1}, \ldots, \sqrt{b_g})^2 \cap K = \bigcup_{\epsilon_i \in \{0,1\}} b_1^{\epsilon_1} \cdots b_g^{\epsilon_g} K^2.$$

The result follows by induction. □

Theorem 4.1.2. *Let β be a totally real algebraic number with conjugate set $\{\beta_1 = \beta, \beta_2, \ldots, \beta_g\}$ such that*

$$\beta_1 < 0 < \beta_2 < \cdots < \beta_g.$$

Let K be the normal closure of β over $\mathbb{Q}$. Then

1. $[K(\sqrt{\beta_1},\ldots,\sqrt{\beta_g}):K]=2^g$,
and

2. There exists an automorphism $\sigma\in\mathrm{Gal}(K(\sqrt{\beta_1},\ldots,\sqrt{\beta_g})/\mathbb{Q})$ *that maps* $\sqrt{\beta}\mapsto\epsilon_j\sqrt{\beta_j}$ *for all* β_j *conjugate to* β *over* $\mathbb{Q}$ *and all* $\epsilon_j\in\{-1,1\}$.

Proof. 1. Since $K\subset\mathbb{R}$, $\sqrt{\beta_1}\notin K$, as $\sqrt{\beta_1}\notin\mathbb{R}$. Suppose $\sqrt{\beta_j}\in K$ for some $2\le j\le g$. Then

$$\beta_j=P(\beta,\ldots,\beta_j,\ldots,\beta_g)^2\in K^2, \tag{4.1}$$

where P is a polynomial in $\mathbb{Q}(\beta_1,\ldots,\beta_g)$. Applying an automorphism $\phi\in\mathrm{Gal}(K/\mathbb{Q})$ that maps $\beta_j\mapsto\beta$ to Equation (4.1) gives

$$\beta=P(\phi(\beta),\ldots,\beta,\ldots,\phi(\beta_g))^2\in K^2,$$

contradicting $\beta\notin K^2$. Clearly, $[K(\sqrt{\beta}):K]=2$, as $K(\sqrt{\beta})/K$ is non real, and $\sqrt{\beta_2}\notin K(\sqrt{\beta})$, so $[K(\sqrt{\beta},\sqrt{\beta_2}):K(\sqrt{\beta})]=2$. We can show that

$$[K(\sqrt{\beta},\sqrt{\beta_2},\ldots,\sqrt{\beta_g}):K]=2^g$$

by induction on g:

Suppose the result is true for $g-1$, i.e. that

$$[K(\sqrt{\beta},\sqrt{\beta_2},\ldots,\sqrt{\beta_{g-1}}):K]=2^{g-1}.$$

We claim that

$$[K(\sqrt{\beta},\ldots,\sqrt{\beta_g}):K(\sqrt{\beta},\ldots,\sqrt{\beta_{g-1}})]=2.$$

Suppose that $\sqrt{\beta_g}\in K(\sqrt{\beta},\ldots,\sqrt{\beta_{g-1}})$. Then by Lemma 4.1.1,

$$\beta_g\beta_{j_1}\beta_{j_2}\cdots\beta_{j_t}\in K^2$$

for some $t<g$ and some t-element set $S=\{j_1,\ldots,j_t\}\subset\{1,\ldots,g-1\}$. Clearly $\beta\notin\{\beta_{j_1},\ldots,\beta_{j_t}\}$. We choose an automorphism τ that maps $\beta_g\mapsto\beta$. Then

$$\beta\tau(\beta_{j_1})\tau(\beta_{j_2})\cdots\tau(\beta_{j_t})\in K^2.$$

But $\beta\tau(\beta_{j_1})\tau(\beta_{j_2})\cdots\tau(\beta_{j_t})<0$ is not in K^2. So

$$[K(\sqrt{\beta},\ldots,\sqrt{\beta_g}):K(\sqrt{\beta},\ldots,\sqrt{\beta_{g-1}})]=2.$$

Therefore, by Theorem 1.3.10,

$$[K(\sqrt{\beta},\ldots,\sqrt{\beta_g}):K]$$

$$= [K(\sqrt{\beta}, \ldots, \sqrt{\beta_g}) : K(\sqrt{\beta}, \ldots, \sqrt{\beta_{g-1}})][K(\sqrt{\beta}, \sqrt{\beta_2}, \ldots, \sqrt{\beta_{g-1}}) : K],$$

which is equal to $2.2^{g-1} = 2^g$ by the assumption. The result follows.

2. Since $[K(\sqrt{\beta}, \ldots, \sqrt{\beta_g}) : K] = 2^g$, $\epsilon_j \sqrt{\beta_j}$ is a conjugate of $\sqrt{\beta}$ for every β_j conjugate to β and all $\epsilon_j \in \pm 1$. The result follows by galois theory. □

Remark. we have

$$\mathrm{Gal}(K(\sqrt{\beta_1}, \ldots, \sqrt{\beta_g})/K) \cong (\mathbb{Z}/2\mathbb{Z})^g$$

and

$$\mathrm{Gal}(K(\sqrt{\beta_1}, \ldots, \sqrt{\beta_g})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^g \rtimes \mathrm{Gal}(K/\mathbb{Q}).$$

4.2 Proof of Theorem 2.3.2:

Proof. ($\Rightarrow$) Let α, h, r and ϵ_j be defined as in the theorem. By Theorem 4.1.2, any automorphism τ, when applied to α, will permute the h_j's, and change the sign of a number of the ϵ_j's. Since r is totally real, all conjugates α' of α lie on $S_=(h)$.

($\Leftarrow$) Let α be an algebraic number whose conjugate set lies on $S_=(h)$. We begin by proving that all conjugates of h are real. Suppose α lies on $\Im(z) = \sqrt{-h}$. Define $\beta = \alpha - \overline{\alpha} = 2\sqrt{h}$. Now apply an automorphism ϕ to β (using an obvious notation):

$$\phi(\beta) = \beta' = \phi(\alpha - \overline{\alpha}) = \phi(2\sqrt{h})$$
$$\beta' = \phi(\alpha) - \phi(\overline{\alpha}) = \alpha' - \alpha'' = 2\phi(\sqrt{h}). \tag{4.2}$$

Applying complex conjugation to Equation (4.2) gives

$$\overline{\beta'} = \overline{\alpha'} - \overline{\alpha''}.$$

We know that α' and α'' lie on $S_=(h)$, so $\beta' = \gamma$ or $\gamma \pm 2\sqrt{h}$, for some $\gamma \in \mathbb{R}$.

Suppose $\beta' = \eta \pm 2\sqrt{h}$ for some non-zero $\eta \in \mathbb{R}$. Then

$$\beta' - \overline{\beta'} = \pm 4\sqrt{h} = \pm 2\beta,$$

contradicting Lemma 2.1.5. Hence $\eta = 0$. Therefore $2\phi(\sqrt{h}) = \pm 2\sqrt{h'} = \gamma$ or $\pm 2\sqrt{h}$, which means that $\sqrt{h'}$ either has zero real part or zero imaginary part. Hence h is totally real.

Next we show that if $h' \neq h$ is a conjugate of h, then $h' > 0$. Suppose that h has a negative conjugate $h' \neq h$. Apply an automorphism ϕ that maps $h \mapsto h'$. Thus $\sqrt{h} \mapsto \epsilon\sqrt{h'}$ and

$$\phi(\alpha) - \phi(\overline{\alpha}) = \alpha' - \alpha'' = 2\epsilon\sqrt{h'}$$

for some $\epsilon \in \pm 1$. We know that h' is real and negative, so $2\sqrt{h'}$ has zero real part. By the same reasoning as above, $\alpha' - \alpha'' = \gamma$ or $\pm 2\sqrt{h}$, where $\gamma \in \mathbb{R}$. But $\alpha' - \alpha''$ lies on the line $\Re(z) = 0$, so $2\sqrt{h} = 2\sqrt{h'}$, or $h' = h$. So h itself is the only conjugate of h which is negative. Thus all of the h_i are real and positive.

Now fix α, and set

$$\epsilon_1 = \begin{cases} 1, & \text{if } \Im(\alpha) = \sqrt{-h}; \\ -1, & \text{if } \Im(\alpha) = -\sqrt{-h}. \end{cases}$$

Let

$$r = \alpha - \epsilon_1\sqrt{h} + \epsilon_2\sqrt{h_2} + \cdots + \epsilon_g\sqrt{h_g}, \tag{4.3}$$

for some choice of $\epsilon_2, \ldots, \epsilon_g$. We show that there exists a choice of $\epsilon_2, \ldots, \epsilon_g$ such that r is totally real.

Let h^* be any positive conjugate of h, and τ an automorphism that maps $h^* \mapsto h$. By Theorem 4.1.2, τ maps α to:

$$\begin{array}{lcl} \alpha = r + \epsilon_1\sqrt{h} + \epsilon_2\sqrt{h_2} + \cdots & + \epsilon^*\sqrt{h^*} & + \cdots + \epsilon_g\sqrt{h_g} \\ \qquad\quad \downarrow \tau & \downarrow & \\ \alpha' = r' + \cdots & \pm\sqrt{h} & \pm \cdots \end{array}$$

The other conjugates of h are permuted amongst each other, although we do not know what happens to the signs of their square roots. Either $r' \in \mathbb{R}$, which is what we want, or else $r' = \delta' \mp 2\sqrt{h}$, where $\delta' \in \mathbb{R}$. Now substituting $-\epsilon^*$ for ϵ^*, and setting $r' = \delta'$ gives $r' \in \mathbb{R}$.

Repeating the process for each of the h_i ($i = 2, \ldots, g$), i.e. applying an automorphism that takes $\sqrt{h_i} \mapsto \epsilon\sqrt{h}$ and $r \mapsto r'$, we obtain the sign of each of the $\sqrt{h_i}$ in Equation (4.3) in order that $r' \in \mathbb{R}$. So there exists a choice of $r, \epsilon_1, \epsilon_2, \ldots, \epsilon_g$ such that $r \in \mathbb{R}$,

$$\alpha = r + \epsilon_1\sqrt{h} + \epsilon_2\sqrt{h_2} + \cdots + \epsilon_g\sqrt{h_g} \tag{4.4}$$

lies on $S_=(h)$, and for each conjugate h^* of h, there exists an automorphism that maps $r \mapsto r' \in \mathbb{R}$ and $h^* \mapsto h$.

We claim that for any conjugate h_j of h,

$$\alpha_j = r + \epsilon_1\sqrt{h} + \cdots - \epsilon_j\sqrt{h_j} + \cdots + \epsilon_g\sqrt{h_g}$$

is a conjugate of α.

Let τ be an automorphism that maps $h^* \mapsto h$ and $r \mapsto r' \in \mathbb{R}$ (such an automorphism exists by above). Applying τ to Equation (4.4) gives

$$\tau(\alpha) = \alpha' = r' + \delta_1\sqrt{h} + \cdots + \delta_j\sqrt{h_j} + \cdots + \delta_g\sqrt{h_g}.$$

The complex conjugate of α' is

$$\overline{\alpha'} = r' - \delta_1\sqrt{h} + \cdots + \delta_j\sqrt{h_j} + \cdots + \delta_g\sqrt{h_g}. \tag{4.5}$$

Applying τ^{-1} to Equation (4.5) gives

$$\alpha_j = r + \epsilon_1\sqrt{h} + \cdots - \epsilon_j\sqrt{h_j} + \cdots + \epsilon_g\sqrt{h_g},$$

thus proving the claim.

Now suppose there exists a conjugate $\hat{r} \notin \mathbb{R}$ of r. Note that $\Im(\hat{r}) = \pm 2\sqrt{-h}$. Let ϕ be any automorphism that maps $r \mapsto \hat{r}$. Suppose $\phi(h^*) = h$ for some conjugate h^* of h. Recall that

$$\alpha^* = r + \epsilon_1\sqrt{h} + \cdots - \epsilon_*\sqrt{h^*} + \cdots + \epsilon_g\sqrt{h_g}$$

is a conjugate of α. Apply ϕ to α and α^*:

$$\phi(\alpha) = \hat{r} + \delta_1\sqrt{h} + \cdots + \delta_g\sqrt{h_g},$$

$$\phi(\alpha^*) = \hat{r} - \delta_1\sqrt{h} + \cdots + \delta_g\sqrt{h_g}.$$

If $\Im(\hat{r}) = 2\delta_1\sqrt{-h}$, then $\phi(\alpha)$ does not lie on $S_=(h)$, and if $\Im(\hat{r}) = -2\delta_1\sqrt{-h}$, then $\phi(\alpha^*)$ does not lie on $S_=(h)$. Therefore no such ϕ exists, and r is totally real. □

Example 4.2.1. Let $h = 6 - \sqrt{7} - \sqrt{17}$ and $r = \frac{1+\sqrt{5}}{2}$. Define

$$\alpha = r + \sqrt{h} + \sqrt{h_2} + \sqrt{h_3} + \sqrt{h_4},$$

where h_2, h_3 and h_4 are conjugates of h. Then α and all its conjugates lie on $S_=(6 - \sqrt{7} - \sqrt{17})$, and $\deg(\alpha) = 32$.

Chapter 5

Proof Of The $\parallel$ Case

In this chapter we prove Theorem 2.3.3, which categorizes algebraic numbers whose conjugate set lies on $S_{\parallel}(p, q)$, two distinct parallel lines.

5.1 Lemmas Required For The Proof

Lemma 5.1.1. *Let $\beta \notin \mathbb{Q}^2$ be a totally real algebraic number with conjugates $\beta_1 = \beta, \beta_2, \ldots, \beta_g$, where $\beta > 0$ and $\beta_j < 0$ for $j = 2, \ldots, g$. Then $-\sqrt{\beta}$ is a conjugate of $\sqrt{\beta}$.*

Proof. Let K be the normal closure of β over $\mathbb{Q}$. Since $K \subset \mathbb{R}$, $\sqrt{\beta_2}, \ldots, \sqrt{\beta_g} \notin K$. Suppose $\sqrt{\beta} \in K$. Then for some polynomial P in K,

$$\beta = P(\beta, \ldots, \beta_g)^2 \in K^2. \tag{5.1}$$

Apply an automorphism ϕ that maps $\beta \mapsto \beta_j < 0$ to Equation (5.1):

$$\beta_j = P(\beta_j, \ldots, \phi(\beta_g))^2 \in K^2,$$

contradicting $\sqrt{\beta_j} \notin K$. Hence $\sqrt{\beta} \notin K$, so that $x^2 - \beta$ is irreducible over K, and hence over $\mathbb{Q}$. Thus $-\sqrt{\beta}$ is a conjugate of $\sqrt{\beta}$. □

Lemma 5.1.2. *Multiplying an algebraic number by i will halve, double or preserve its degree.*

Proof. First note that $\mathbb{Q}(i, \beta)/\mathbb{Q} = \mathbb{Q}(i, i\beta)/\mathbb{Q}$. By Theorem 1.3.10,

$$[\mathbb{Q}(i, \beta) : \mathbb{Q}] = [\mathbb{Q}(i, \beta) : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}]$$

and

$$[\mathbb{Q}(i, \beta) : \mathbb{Q}] = [\mathbb{Q}(i, \beta) : \mathbb{Q}(i\beta)][\mathbb{Q}(i\beta) : \mathbb{Q}].$$

Now $[\mathbb{Q}(i, \beta) : \mathbb{Q}(\beta)]$ and $[\mathbb{Q}(i, \beta) : \mathbb{Q}(i\beta)]$ have degree either 1 or 2. Consider the cases:

1. $[\mathbb{Q}(i,\beta):\mathbb{Q}(\beta)] = [\mathbb{Q}(i,\beta):\mathbb{Q}(i\beta)]$. Here $\deg(i\beta) = \deg(\beta)$.

2. $[\mathbb{Q}(i,\beta):\mathbb{Q}(\beta)] = 2$ and $[\mathbb{Q}(i,\beta):\mathbb{Q}(i\beta)] = 1$. Here $\deg(i\beta) = 2\deg(\beta)$.

3. $[\mathbb{Q}(i,\beta):\mathbb{Q}(\beta)] = 1$ and $[\mathbb{Q}(i,\beta):\mathbb{Q}(i\beta)] = 2$. Here $\deg(i\beta) = \frac{1}{2}\deg(\beta)$.

Examples with $\beta = 1+i, 1$ and i prove the existence of all three possibilities. □

Let α be an algebraic number whose conjugate set $\{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d\}$ lies on $S_{\|}(p,q)$ for some real p and q ($p \neq q$), which are necessarily algebraic.

Notation. For convenience, the lines $\Re(z) = p$ and $\Re(z) = q$ will be referred to as L_p and L_q, and the number of conjugates which lie on L_p and L_q denoted N_p and N_q. The conjugates of α that lie on L_p and L_q will be called α_{p_i} and α_{q_j} (for i and j in suitable index sets) respectively.

Proposition 5.1.3. *The number of conjugates of α that lie on each line is either one or an even number.*

Proof. Suppose not, say $N_p = 2n+1$ ($n > 0$). Then $\alpha = p, \alpha' = p + i\lambda$ and $\overline{\alpha'} = p - i\lambda$ ($\lambda \in \mathbb{R}^*$) all lie on L_p. Hence $\alpha' + \overline{\alpha'} = 2\alpha$, contradicting Lemma 2.1.5.

□

Lemma 5.1.4. *Let α_{p_1} denote a conjugate of α that lies on L_p, and let ϕ be an automorphism that maps α_{p_1} onto L_q. Then ϕ maps either all or half the conjugates on L_p onto L_q.*

Proof. By Proposition 5.1.3, N_p is equal to one or an even number. If $N_p = 1$, then ϕ maps all conjugates on L_p onto L_q. So suppose $N_p > 1$. Then $\alpha_{p_1}, \alpha_{\overline{p_1}}, \ldots, \alpha_{p_c}, \alpha_{\overline{p_c}}$ all lie on L_p for some $c \geq 1$. All the α_{p_i} (none of which are real) are related by

$$\alpha_{p_1} + \alpha_{\overline{p_1}} = \alpha_{p_2} + \alpha_{\overline{p_2}} = \cdots = \alpha_{p_c} + \alpha_{\overline{p_c}} = 2p. \tag{5.2}$$

Applying ϕ to Equation (5.2) gives

$$\alpha_q + \alpha_{\phi(\overline{p_1})} = \alpha_{\phi(p_2)} + \alpha_{\phi(\overline{p_2})} = \cdots = \alpha_{\phi(p_c)} + \alpha_{\phi(\overline{p_c})} = 2p', \tag{5.3}$$

where α_q lies on L_q. Then

$$\Re(\alpha_q + \alpha_{\phi(\overline{p_1})}) = 2\Re(p')$$
$$q + \Re(\alpha_{\phi(\overline{p_1})}) = 2\Re(p').$$

Thus $\Re(p') = \frac{p+q}{2}$ (if $\alpha_{\phi(\overline{p_1})}$ lies on L_p) or q (if $\alpha_{\phi(\overline{p_1})}$ lies on L_q).

$\Re(p') = \frac{p+q}{2}$ implies that exactly half of $\alpha_q, \alpha_{\phi(\overline{p_1})}, \ldots, \alpha_{\phi(\overline{p_c})}$ lie on L_q, and $\Re(p') = q$ implies that all of $\alpha_q, \alpha_{\phi(\overline{p_1})}, \ldots, \alpha_{\phi(\overline{p_c})}$ lie on L_q. The result follows. □

Lemma 5.1.5. *Either*

1. *The number of conjugates of α that lie on each line are equal (to $\frac{d}{2}$), or*

2. *There are twice as many conjugates of α that lie on one line than on the other (and so $3|2d$ and $3|d$).*

Proof. By Proposition 5.1.3, N_p and N_q are equal to either one or an even number. Consider the possibility of least one of N_p, N_q equal to one first.

$N_p = N_q = 1$ is covered by case 1.

Let $N_p = 1$ and $N_q > 1$. Then N_q is even, so $N_q = 2c$ say, and

$$q = \frac{1}{2}(\alpha_{q_1} + \alpha_{\overline{q_1}}) = \frac{1}{2}(\alpha_{q_2} + \alpha_{\overline{q_2}}) = \cdots = \frac{1}{2}(\alpha_{q_c} + \alpha_{\overline{q_c}}),$$

where none of the α_{q_j} are real. Apply an automorphism τ that maps $\alpha_{q_1} \mapsto \alpha_p$, where α_p is the conjugate on L_p to q. Then

$$\tau(q) = q' = \frac{1}{2}(\alpha_p + \alpha_{\tau(\overline{q_1})}) = \frac{1}{2}(\alpha_{\tau(q_2)} + \alpha_{\tau(\overline{q_2})}) = \cdots, \tag{5.4}$$

where $\alpha_{\tau(\overline{q_1})}, \alpha_{\tau(q_2)}, \alpha_{\tau(\overline{q_2})}, \cdots$ all lie on L_q.

Suppose $c > 1$. Then equating the real parts of Equation (5.4) gives $\frac{p+q}{2} = q$. This contradicts $p \neq q$, so $c = 1$ and there must be exactly two conjugates on L_q. Thus $N_q = 2 = 2N_p$, as in case 2.

Now suppose that N_p and N_q are both even. Let σ be an automorphism that maps some conjugate α_{q_j} that lies on L_q onto L_p. By Lemma 5.1.4, σ must map either all or half the conjugates on L_q onto L_p, and either all or half the conjugates from L_p onto L_q. Consider:

1. σ maps half the conjugates from L_q onto L_p, or

2. σ maps all the conjugates on L_q onto L_p.

1. Suppose σ maps half the conjugates on L_q onto L_p. Then if half the number of conjugates on L_p are mapped onto L_q, $N_p = N_q$. If every conjugate on L_p is mapped onto L_q, then $N_q = 2N_p$.

2. Suppose σ maps all conjugates on L_q onto L_p. Then if half the number of conjugates on L_p are mapped onto L_q, $N_p = 2N_q$. If every conjugate on L_p is mapped onto L_q, then $N_p = N_q$.

Hence $N_p = N_q$, $\frac{1}{2}N_q$ or $2N_q$ as required. □

The following follows immediately from the proof of Lemma 5.1.5:

Corollary 5.1.6. *If N_p (resp. N_q) is equal to $\frac{d}{3}$, then any automorphism either maps all or none of the conjugates on L_p onto L_q (resp. L_q onto L_p).*

Lemma 5.1.7. *Let the conjugate set of α lie on L_p and L_q (and not just one of them). Then $p, q \notin \mathbb{Q}$.*

Proof. Suppose $p \in \mathbb{Q}$. Let N_p denote the number of conjugates on $\Re(z) = p$. If $N_p = 1$, then some conjugate $\alpha_j = p$, and as α has conjugates on $\Re(z) = q$, this contradicts $p \in \mathbb{Q}$. Let $N_p > 1$. By Proposition 5.1.3, $N_p = 2c$ for some $c \in \mathbb{N}$. Label the conjugates of α lying on $\Re(z) = p$ so that

$$\alpha_{p_1} + \alpha_{\overline{p_1}} = \cdots = \alpha_{p_c} + \alpha_{\overline{p_c}} = 2p.$$

Apply an automorphism that maps α_{p_1} to a conjugate α_q that lies on $\Re(z) = q$. Then for some conjugate α' of α,

$$\alpha_q + \alpha' = 2p. \tag{5.5}$$

Equating real parts of Equation (5.5) contradicts $p \neq q$. Thus $p \notin \mathbb{Q}$. Exactly the same argument will show that $q \notin \mathbb{Q}$. □

5.2 Proof Of Theorem 2.3.3:

Proof. ($\Rightarrow$)

1. Let p and q be distinct real algebraic numbers such that $p+q \in \mathbb{Q}$, $p, q \notin \mathbb{Q}$ and $h = \left(\frac{p-q}{2}\right)^2$ is totally real, with all other conjugates $h_2, \ldots, h_g$ of h negative. Let r be totally real, and let $\epsilon_j = \pm 1$ for $j \in \{1, \ldots, g\}$. Define

   $$\alpha = \frac{p+q}{2} + \epsilon\sqrt{h} + \epsilon_2\sqrt{h_2} + \cdots + \epsilon_g\sqrt{h_g} + ir. \tag{5.6}$$

   Clearly $\alpha \in S_{\|}(p, q)$. Let σ be an automorphism in the galois closure of ir and $\sqrt{h}$. Apply σ to Equation (5.6). By Theorem 4.1.2,

   $$\sigma(\alpha) = \alpha' = \frac{p+q}{2} + \delta_1\sqrt{h} + \delta_2\sqrt{h_2} + \cdots + \delta_g\sqrt{h_g} + \delta i r',$$

   where $r' \in \mathbb{R}$ and $\delta, \delta_1, \ldots, \delta_g \in \pm 1$.

   Since $\Re(\alpha') = \frac{p+q}{2} + \delta\sqrt{h}$, α' lies on $S_{\|}(p, q)$.

   Hence the conjugate set of α lies on $S_{\|}(p, q)$. By Lemma 5.1.1, $-\sqrt{h}$ is a conjugate of $\sqrt{h}$, so there exists an automorphism ϕ that maps $\sqrt{h} \mapsto -\sqrt{h}$, and the conjugate set of α lie on not just one of the lines L_p or L_q.

2. Let p be the real root of a non totally real cubic, with conjugates $p_1, p_{\overline{1}}$ such that $\Re(p_1) = q$, and let r be totally real. Define

$$\alpha = p + ir.$$

Then $\Re(\alpha) = p$, so $\alpha \in S_{\|}(p, q)$. Now let σ be an automorphism in the galois closure of p and ir. Then

$$\sigma(p + ir) = p' \pm ir'.$$

If $p' = p$, then $\Re(\alpha) = p$, and if $p' \neq p$ then $\Re(\alpha) = q$, since $\Re(p') = q$ and $r' \in \mathbb{R}$. Hence the conjugate set of α lies on $S_{\|}(p, q)$.

($\Leftarrow$) Let α and all its conjugates lie on $S_{\|}(p, q)$, for some distinct real numbers p and q. Recall N_p (resp. N_q) denotes the number of conjugates of α lying on L_p (resp. L_q). Suppose without loss of generality that $N_p \leq N_q$. Lemma 5.1.5 gives $N_p = N_q$ or $N_p = \frac{1}{2}N_q$.

1. Consider $N_p = N_q$. By Lemma 5.1.7, $p, q \notin \mathbb{Q}$. We can subtract $\frac{p+q}{2} \in \mathbb{Q}$ from the conjugates of α, so that the midpoint of p and q is the origin, and multiplying by i gives us an algebraic number whose conjugate set lies on $S_{=}(\frac{p-q}{2})$ (note that by Lemma 5.1.2, multiplying an algebraic number by i can double, half or preserve its degree).

Inverting this process, any algebraic number that lies with its conjugates on $S_{\|}(p, q)$ (and $N_p = N_q$) can be constructed, by multiplying an algebraic number whose conjugate set lies on $S_{=}(h)$ by i and adding on a rational. Hence, by Theorem 2.3.2,

$$\alpha = \frac{p+q}{2} + \epsilon_1\sqrt{h} + \epsilon_2\sqrt{h_2} + \cdots + \epsilon_g\sqrt{h_g} + ir.$$

2. Now suppose $N_p = \frac{d}{3}$ and $N_q = \frac{2d}{3} = 2N_p$. Consider the relationship

$$p = \frac{1}{2}(\alpha_{p_1} + \alpha_{\overline{p_1}}) = \frac{1}{2}(\alpha_{p_2} + \alpha_{\overline{p_2}}) = \cdots = \frac{1}{2}(\alpha_{p_{\frac{d}{6}}} + \alpha_{\overline{p_{\frac{d}{6}}}}).$$

By Corollary 5.1.6, on applying an automorphism τ to p, either all of the α_{p_i} remain on L_p, or all of the conjugates are mapped onto L_q. So all conjugates p' of p are of the form $p + i\lambda$ or $q + i\theta$. Application of Lemma 2.1.5 to $p \pm i\lambda$ shows that $\lambda = 0$.

If q is a conjugate of p (i.e. $\theta = 0$), then by the relationship

$$2q = (\alpha_{q_1} + \alpha_{\overline{q_1}}) = (\alpha_{q_2} + \alpha_{\overline{q_2}}) = \cdots = (\alpha_{q_{\frac{d}{3}}} + \alpha_{\overline{q_{\frac{d}{3}}}}),$$

applying an automorphism that maps $q \mapsto p$ will map all of the α_{q_j} onto L_p. However, $N_p < N_q$, so no such automorphism exists and $\theta \neq 0$. Now suppose there are at least four conjugates of p lying on L_q. Call four of them

$$p_1 = q + i\theta_1,$$

$$p_{\overline{1}} = q - i\theta_1,$$

$$p_2 = q + i\theta_2,$$

and

$$p_{\overline{2}} = q - i\theta_2.$$

Consider the relationship

$$q = \frac{1}{2}(p_1 + p_{\overline{1}}) = \frac{1}{2}(p_2 + p_{\overline{2}}). \tag{5.7}$$

Applying an automorphism that maps $p_1 \mapsto p$ to Equation (5.7), and equating real parts gives the required contradiction. So p has exactly two conjugates on L_q, hence is cubic.

To show that r is totally real, apply an automorphism σ that maps $r \mapsto r' \neq r$ to $\alpha = p + ir$:

$$\sigma(\alpha) = \sigma(p + ir) = p' + \epsilon i r',$$

where p' is a conjugate of p and $\epsilon = \pm 1$. Suppose that $\Re(p') = p$. If $r' \notin \mathbb{R}$, then $\Re(\epsilon i r') = q - p$, since $\Re(\sigma(\alpha)) \neq p$ in this situation. But then

$$\Re(\sigma(\overline{\alpha})) = p - \Re(\epsilon i r') = 2p - q,$$

which contradicts $\sigma(\overline{\alpha})$ lying on $S_{\|}(p, q)$. The same argument holds for $\Re(p') = q$. Hence r is totally real.

It remains to check that the construction above does not alter the 1:2 ratio of conjugates on L_p to conjugates on L_q, i.e. that there do not exist distinct conjugates of r, r' and r'' say, such that

$$p' \pm ir' = \overline{p'} \pm ir''.$$

This condition is required to satisfy the uniqueness claim in Theorem 2.3.3. Assume such r' and r'' exist. Then

$$p' \pm ir' - \overline{p'} \mp ir'' = 0. \tag{5.8}$$

Applying any automorphism that maps $p' \mapsto p$ will contradict the equality of the real parts of Equation (5.8). □

5.3 Examples

The following example is a good illustration of the case where p is quadratic:

Example 5.3.1. Consider the equation $P(z) = z^4 + z^3 + z^2 + z + 1$. Then the roots of $P(z)$ are

$$\alpha_1 = e^{\frac{\pi i}{5}} = \frac{1}{4}\sqrt{5} - \frac{1}{4} + \frac{1}{4}i\sqrt{2}\sqrt{5+\sqrt{5}},$$

$$\alpha_{\bar{1}} = e^{\frac{-\pi i}{5}} = \frac{1}{4}\sqrt{5} - \frac{1}{4} - \frac{1}{4}i\sqrt{2}\sqrt{5+\sqrt{5}},$$

$$\alpha_2 = e^{\frac{2\pi i}{5}} = \frac{-1}{4}\sqrt{5} - \frac{1}{4} + \frac{1}{4}i\sqrt{2}\sqrt{5-\sqrt{5}},$$

and

$$\alpha_{\bar{2}} = e^{\frac{-2\pi i}{5}} = \frac{-1}{4}\sqrt{5} - \frac{1}{4} - \frac{1}{4}i\sqrt{2}\sqrt{5-\sqrt{5}}.$$

These roots lie on two vertical lines, $\Re(z) = \frac{-1}{4} \pm \frac{1}{4}\sqrt{5}$. Take $p = \frac{-1}{4} + \frac{1}{4}\sqrt{5}$, $q = \frac{-1}{4} - \frac{1}{4}\sqrt{5}, h = \frac{5}{16}$ and $r = \frac{1}{4}\sqrt{2}\sqrt{5+\sqrt{5}}$. Then p is quadratic, $h \in \mathbb{Q}$ and r is totally real. Adding $\frac{1}{4}$ to each conjugate, and multiplying by i gives eight conjugates, all of which lie on $S_{=}(-\frac{5}{16})$.

Chapter 6

The × Case

In this chapter we examine the case where α and all its conjugates lie on the two lines $z = z(t) = C + tu^{\pm\frac{1}{2}}$ $(t \in \mathbb{R}, u = e^{2i\theta}$ for some $\theta \in (0, \frac{\pi}{2}))$.

Notation. For convenience, the line $z(t) = C + tu^{\frac{1}{2}}$ will be referred to as L, and $z(t) = C + tu^{-\frac{1}{2}}$ as $\overline{L}$. A conjugate of α whose position is known and lies on L will be referred to as α with a numerical subscript, for example α_1. As in previous chapters, an automorphism σ will map $\alpha_1 \mapsto \alpha_{\sigma(1)}$ and $\alpha_{\overline{1}} \mapsto \alpha_{\sigma(\overline{1})}$. If a conjugate is not fixed, but is known to lie on L, it will be referred to as α, with a letter as a subscript, and similarly, $\overline{\alpha}$ with a letter subscript refers to some conjugate of α that lies on $\overline{L}$. A conjugate that could lie on L or $\overline{L}$ will be referred to as α with a superscript, usually α'.

In this chapter, when comparing phases, we will work mod π without loss of generality.

Is it possible for a conjugate of α to be the point of intersection of L and $\overline{L}$? A non totally real cubic is one obvious example. In the first section we show that no algebraic number α of degree greater than three lies with its conjugates on $S_\times(\alpha, \sqrt{u})$ for any u. In the second section, we show that for all algebraic numbers α of degree at least ten which lie with their conjugates on $S_\times(C, \sqrt{u})$, C is totally real. In the third section we refine this result, and show that the degree of C for such an α is at most two. The main theorem, regarding the construction of all algebraic numbers α which lie with their conjugates on $S_\times(C, \sqrt{u})$, is proved in the final two sections, firstly for a real quadratic C, and secondly for $C \in \mathbb{Q}$.

Let α be algebraic, and let

$$\{\alpha_1 = \alpha, \alpha_{\overline{1}}, \dots, \alpha_d, \alpha_{\overline{d}}\}$$

be the conjugate set of α, all of which lie on $S_\times(C, \sqrt{u})$. Then u can be described in terms of the α_i as follows:

$$u = \frac{\alpha_1 - \alpha_2}{\alpha_{\overline{1}} - \alpha_{\overline{2}}} = \frac{\alpha_1 - \alpha_3}{\alpha_{\overline{1}} - \alpha_{\overline{3}}} = \cdots = \frac{\alpha_i - \alpha_j}{\alpha_{\overline{i}} - \alpha_{\overline{j}}} = \cdots = \frac{\alpha_{d-1} - \alpha_d}{\alpha_{\overline{d-1}} - \alpha_{\overline{d}}}.$$

Here $i \neq j$. Alternatively, in terms of the α_i and C:

$$u = \frac{\alpha_1 - C}{\alpha_{\overline{1}} - C} = \frac{\alpha_2 - C}{\alpha_{\overline{2}} - C} = \cdots = \frac{\alpha_d - C}{\alpha_{\overline{d}} - C}. \tag{6.1}$$

Furthermore, C can be described in terms of the α_i by rearranging Equation (6.1) as follows:

$$C = \frac{\alpha_1\alpha_{\overline{2}} - \alpha_{\overline{1}}\alpha_2}{\alpha_1 - \alpha_{\overline{1}} - \alpha_2 + \alpha_{\overline{2}}} = \frac{\alpha_1\alpha_{\overline{3}} - \alpha_{\overline{1}}\alpha_3}{\alpha_1 - \alpha_{\overline{1}} - \alpha_3 + \alpha_{\overline{3}}}$$

$$= \cdots = \frac{\alpha_i\alpha_{\overline{j}} - \alpha_{\overline{i}}\alpha_j}{\alpha_i + \alpha_{\overline{j}} - \alpha_{\overline{i}} - \alpha_j} = \cdots = \frac{\alpha_{d-1}\alpha_{\overline{d}} - \alpha_{\overline{d-1}}\alpha_d}{\alpha_{d-1} - \alpha_{\overline{d-1}} - \alpha_d + \alpha_{\overline{d}}}. \tag{6.2}$$

This shows that C is certainly algebraic.

6.1 Proving that α and C are not conjugate

Let α be an algebraic real number whose conjugate set lies on a pair of lines that intersect at α and neither of which are the real axis. We show that no such α exists if $\deg(\alpha) > 3$. We first consider the case where α has degree at least seven:

Lemma 6.1.1. *There is no real algebraic number α of degree greater than five that lies with its conjugates on $S_\times(\alpha, \sqrt{u})$.*

Proof. Suppose such an α does exist, with $\deg(\alpha) = 2d+1, d \geq 3$. Call its non real conjugates $\alpha_1, \alpha_{\overline{1}}, \alpha_2, \alpha_{\overline{2}}, \ldots, \alpha_d, \alpha_{\overline{d}}$. By replacing C with α in Equation (6.1), the $\binom{d}{2}$ equations in α can be written as

$$\begin{gathered}
(\alpha_1 - \alpha)(\alpha_{\overline{2}} - \alpha) = (\alpha_{\overline{1}} - \alpha)(\alpha_2 - \alpha) \\
(\alpha_1 - \alpha)(\alpha_{\overline{3}} - \alpha) = (\alpha_{\overline{1}} - \alpha)(\alpha_3 - \alpha) \\
\vdots \\
(\alpha_{d-1} - \alpha)(\alpha_{\overline{d}} - \alpha) = (\alpha_{\overline{d-1}} - \alpha)(\alpha_d - \alpha).
\end{gathered} \tag{6.3}$$

Apply an automorphism τ that maps $\alpha \mapsto \alpha_1$ to the $\binom{d}{2}$ Equations (6.3). Then by Theorem 1.4.3, $d-1$ of these equations are mapped to

$$
\begin{aligned}
(\alpha-\alpha_1)(\alpha''-\alpha_1) &= (\alpha'-\alpha_1)(\alpha'''-\alpha_1)\\
(\alpha-\alpha_1)(\alpha^{(iv)}-\alpha_1) &= (\alpha'-\alpha_1)(\alpha^{(v)}-\alpha_1)\\
&\vdots\\
(\alpha-\alpha_1)(\alpha^{(2d-2)}-\alpha_1) &= (\alpha'-\alpha_1)(\alpha^{(2d-1)}-\alpha_1) \qquad (6.4)
\end{aligned}
$$

where $\alpha_1, \alpha, \alpha', \alpha'', \ldots, \alpha^{(2d-1)}$ are all distinct and make up the conjugate set of α. Note that $d-1$ of $\alpha', \alpha'', \ldots, \alpha^{(2d-1)}$ lie on L, and d of $\alpha', \alpha'', \ldots, \alpha^{(2d-1)}$ lie on $\overline{L}$, one of which is $\alpha_{\overline{1}}$. The aim is to derive a contradiction by equating the phases of the set of Equations (6.4). There are d factors of the form $(\hat{\alpha}-\alpha_1)$, where $\hat{\alpha} \neq \alpha_1$ lies on L, and each of these factors has phase θ. Consider $(\alpha'-\alpha_1)$, with respect to each of the following three cases:

1. α' lies on L,

2. $\alpha' = \alpha_{\overline{1}}$, and

3. $\alpha' \neq \alpha_{\overline{1}}, \alpha'$ lies on $\overline{L}$.

1. Suppose α' lies on L, so that $(\alpha'-\alpha_1)$ has phase θ. Then one of $\alpha'', \ldots, \alpha^{(2d-1)}$ is $\alpha_{\overline{1}}$. Without loss of generality, suppose one of α'', α''' is equal to $\alpha_{\overline{1}}$.

(1a) Let $\alpha'' = \alpha_{\overline{1}}$. Then $(\alpha''-\alpha_1)$ has phase $\frac{\pi}{2}$, and so, from the first of Equations (6.4), so does $(\alpha'''-\alpha_1)$. This contradicts $\alpha''' \neq \alpha_{\overline{1}}$.

(1b) Let $\alpha''' = \alpha_{\overline{1}}$. Then $(\alpha'''-\alpha_1)$ has phase $\frac{\pi}{2}$, and so, from the first of Equations (6.4), so does $(\alpha''-\alpha_1)$. This contradicts $\alpha'' \neq \alpha_{\overline{1}}$.

Therefore α' must lie on $\overline{L}$.

(2) Suppose $\alpha' = \alpha_{\overline{1}}$, so that $(\alpha'-\alpha_1)$ has phase $\frac{\pi}{2}$. Consider the conjugates $\alpha''', \alpha^{(v)}, \ldots, \alpha^{(2d-1)}$ which appear on the RHS of the set of Equations (6.4).

(2a) Suppose one of these conjugates, say $\alpha^{(v)}$, lies on L. Then $(\alpha^{(v)}-\alpha_1)$ has phase θ, and so $(\alpha^{(iv)}-\alpha_1)$ has phase $\frac{\pi}{2}$, contradicting $\alpha^{(iv)} \neq \alpha_{\overline{1}}$.

(2b) Suppose the conjugates that lie on L are α'', $\alpha^{(iv)}$,$\cdots$, $\alpha^{(2d-2)}$ (so they all appear on the LHS of the set of Equations (6.4)). Then

$$(\alpha''-\alpha_1), (\alpha^{(iv)}-\alpha_1), \ldots, (\alpha^{(2d-2)}-\alpha_1)$$

all have phase θ. Therefore,

$$(\alpha''' - \alpha_1), (\alpha^{(v)} - \alpha_1), \ldots, (\alpha^{(2d-1)} - \alpha_1)$$

all have phase equal to $2\theta + \frac{\pi}{2}$. This implies that α''', α_1 and $\alpha^{(v)}$ are collinear, a contradiction.

(3) Suppose $\alpha' = \alpha_{\overline{j}}$ for some $j \neq 1$. Let $(\alpha' - \alpha_1)$ have phase ϕ, noting that $\phi \neq \pm\theta$ or $\frac{\pi}{2}$. As above, if one of $\alpha''', \alpha^{(v)}, \ldots, \alpha^{(2d-1)}$, say $\alpha^{(v)}$, lies on L, then $(\alpha^{(iv)} - \alpha_1)$ has phase ϕ, contradicting the fact that $\alpha^{(iv)}$, α_1 and α' are non collinear. We use the first two of Equations (6.4), namely

$$\begin{aligned}(\alpha - \alpha_1)(\alpha'' - \alpha_1) &= (\alpha_{\overline{j}} - \alpha_1)(\alpha''' - \alpha_1) \qquad \text{and}\\ (\alpha - \alpha_1)(\alpha^{(iv)} - \alpha_1) &= (\alpha_{\overline{j}} - \alpha_1)(\alpha^{(v)} - \alpha_1).\end{aligned}$$

Therefore, as $(\alpha'' - \alpha_1), (\alpha^{(iv)} - \alpha_1), \ldots, (\alpha^{(2d-2)} - \alpha_1)$ all have phase θ, $(\alpha''' - \alpha_1)$ and $(\alpha^{(v)} - \alpha_1)$ have phase $2\theta - \phi$. This contradicts the non collinearity of $\alpha''', \alpha^{(v)}$ and α_1.

Hence there is no algebraic number α with degree greater than five that lies with its conjugates on $S_\times(\alpha, \sqrt{u})$. □

The degree of α is taken to be at least seven in order that there are at least two equations in the list of Equations (6.4), so as to obtain a contradiction for cases (2b) and (3). In the following lemma, we deal specifically with the case where the degree of α is five.

Lemma 6.1.2. *There is no real algebraic number α of degree five that lies with its conjugates on $S_\times(\alpha, \sqrt{u})$.*

Proof. Suppose such an α exists. Call its non real conjugates α_1, $\alpha_{\overline{1}}$, α_2 and $\alpha_{\overline{2}}$, with $\Re(\alpha_1) < \Re(\alpha_2)$. Apply an automorphism that maps $\alpha \mapsto \alpha_1$. Then

$$(\alpha_1 - \alpha)(\alpha_{\overline{2}} - \alpha) = (\alpha_2 - \alpha)(\alpha_{\overline{1}} - \alpha) \tag{6.5}$$

is mapped to

$$(\alpha - \alpha_1)(\alpha'' - \alpha_1) = (\alpha' - \alpha_1)(\alpha''' - \alpha_1), \tag{6.6}$$

where α', α'' and α''' represent some permutation of $\alpha_{\overline{1}}, \alpha_2$ and $\alpha_{\overline{2}}$. Consider the two cases:

1. $\alpha'' \neq \alpha_2$, and

2. $\alpha'' = \alpha_2$.

1. We can assume that $\alpha' = \alpha_2$. Then

$$(\alpha - \alpha_1)(\alpha'' - \alpha_1) = (\alpha_2 - \alpha_1)(\alpha''' - \alpha_1). \tag{6.7}$$

Let ϕ denote the phase of $(\alpha_{\overline{2}} - \alpha_1)$. If $\alpha'' = \alpha_{\overline{1}}$, then equating phases of Equation (6.7) gives $\phi = \frac{\pi}{2}$, contradicting the fact that $\Re(\alpha_1) \neq \Re(\alpha_2)$.

If $\alpha'' = \alpha_{\overline{2}}$, then equating phases of Equation (6.7) again gives $\phi = \frac{\pi}{2}$, resulting in the same contradiction as above.

2. Let $\alpha'' = \alpha_2$. We know that $(\alpha - \alpha_1)$ and $(\alpha_2 - \alpha_1)$ have phase θ, and $(\alpha_{\overline{1}} - \alpha_1)$ has phase $\frac{\pi}{2}$. Equation (6.7) becomes:

$$(\alpha - \alpha_1)(\alpha_2 - \alpha_1) = (\alpha_{\overline{1}} - \alpha_1)(\alpha_{\overline{2}} - \alpha_1). \tag{6.8}$$

Let ϕ denote the phase of $(\alpha_{\overline{2}} - \alpha_1)$. Recall that Equation (6.8) was derived from an automorphism that mapped $\alpha \mapsto \alpha_1$. By a similar argument applying an automorphism that maps $\alpha \mapsto \alpha_2$ to Equation (6.5) gives

$$(\alpha - \alpha_2)(\alpha_1 - \alpha_2) = (\alpha_{\overline{1}} - \alpha_2)(\alpha_{\overline{2}} - \alpha_2). \tag{6.9}$$

The LHS of Equations (6.8) and (6.9) have phase 2θ. The RHS of Equation (6.8) has phase $\frac{\pi}{2} + \phi$, and the RHS of Equation (6.9) has phase $\frac{\pi}{2} - \phi$. Equating the phases of the right hand sides gives $2\phi = 0$, so $\phi = 0$ or $\frac{\pi}{2}$. If $\phi = \frac{\pi}{2}$, then the four non-real conjugates have equal real part. This contradicts $\Re(\alpha_1) < \Re(\alpha_2)$. If $\theta = 0$, then $\Im(\alpha_1) = \Im(\alpha_{\overline{2}})$, and so $\alpha_1 + \alpha_2 = 2\alpha$, contradicting Lemma 2.1.5. □

We combine Lemmas 6.1.1 and 6.1.2 to give:

Theorem 6.1.3. *There exists no real algebraic number α of degree greater than three that lies with its conjugates on $S_\times(\alpha, \sqrt{u})$.*

Bearing in mind the cubic case, we now assume that α is of even degree and not equal to C.

6.2 Proving that C is totally real

By Theorem 6.1.3, we know that none of the conjugate set of α are real, so α has even degree, say $\deg(\alpha) = 2d$.

Notation. For reasons that will be made clear in Lemma 6.2.2, we will assume that d is at least five. Define Ω and $\overline{\Omega}$ as the sets of conjugates of α that lie on L and $\overline{L}$ respectively. So

$$\begin{aligned} \Omega &= \{\alpha_1, \alpha_2, \ldots, \alpha_d\}, && \text{and} \\ \overline{\Omega} &= \{\alpha_{\overline{1}}, \alpha_{\overline{2}}, \ldots, \alpha_{\overline{d}}\}. \end{aligned}$$

Define the mean of the elements of Ω as

$$\omega = \frac{1}{d} \sum_{\alpha' \in \Omega} \alpha'.$$

Then

$$\overline{\omega} = \frac{1}{d} \sum_{\alpha' \in \overline{\Omega}} \alpha'.$$

On applying an automorphism σ to the conjugates of α, we denote the set of conjugates $\{\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(d)}\}$ by $\sigma(\Omega)$, and the set of conjugates $\{\alpha_{\sigma(\overline{1})}, \ldots, \alpha_{\sigma(\overline{d})}\}$ by $\sigma(\overline{\Omega})$.

In this section, we assume that $C \notin \mathbb{Q}$, apply an automorphism τ in the galois closure of C, u and α that maps $C \mapsto C' \neq C$ and examine what happens to u.

Remark. If $\omega \in \mathbb{R}$, then $\omega = \overline{\omega} = C$, and so $C \in \mathbb{Q}$. We consider this case in Section 6.5.

Lemma 6.2.1. *Let α_1, α_2 and α_3 be three conjugates of α that belong to Ω. Choose an automorphism τ that maps $\alpha_1 \mapsto \alpha_{\tau(1)}$, $\alpha_2 \mapsto \alpha_{\tau(2)}$ and $\alpha_3 \mapsto \alpha_{\tau(3)}$, where $\alpha_{\tau(1)}, \alpha_{\tau(2)}$ and $\alpha_{\tau(3)}$ all lie on the same line, L say. Then the conjugates $\alpha_{\tau(\overline{1})}, \alpha_{\tau(\overline{2})}$ and $\alpha_{\tau(\overline{3})}$ are collinear.*

Proof. τ maps u to

$$u' = \frac{\alpha_{\tau(1)} - \alpha_{\tau(2)}}{\alpha_{\tau(\overline{1})} - \alpha_{\tau(\overline{2})}} = \frac{\alpha_{\tau(1)} - \alpha_{\tau(3)}}{\alpha_{\tau(\overline{1})} - \alpha_{\tau(\overline{3})}} = \frac{\alpha_{\tau(2)} - \alpha_{\tau(3)}}{\alpha_{\tau(\overline{2})} - \alpha_{\tau(\overline{3})}}. \tag{6.10}$$

At least two of $\alpha_{\tau(\overline{1})}, \alpha_{\tau(\overline{2})}$ and $\alpha_{\tau(\overline{3})}$ belong to one of Ω or $\overline{\Omega}$. Let two of $\alpha_{\tau(\overline{1})}, \alpha_{\tau(\overline{2})}, \alpha_{\tau(\overline{3})} \in \Omega$, say $\alpha_{\tau(\overline{1})}$ and $\alpha_{\tau(\overline{2})}$ without loss of generality. Then

$$u' = \frac{\alpha_{\tau(1)} - \alpha_{\tau(2)}}{\alpha_{\tau(\overline{1})} - \alpha_{\tau(\overline{2})}} = \frac{\alpha_{\tau(1)} - \alpha_{\tau(3)}}{\alpha_{\tau(\overline{1})} - \alpha_{\tau(\overline{3})}}. \tag{6.11}$$

The phase of u' is zero. So $(\alpha_{\tau(\overline{1})} - \alpha_{\tau(\overline{3})})$ has phase θ. Hence $\alpha_{\tau(\overline{3})} \in \Omega$.

The other cases, such as $\alpha_{\tau(1)}, \alpha_{\tau(2)}$ and $\alpha_{\tau(3)}$ all belonging to $\overline{\Omega}$, or $\alpha_{\tau(\overline{1})}$ and $\alpha_{\tau(\overline{2})}$ belonging to $\overline{\Omega}$, follow in exactly the same way. □

Lemma 6.2.2. *Let σ be an automorphism that maps a pair of complex conjugates $(\alpha_i, \alpha_{\overline{i}})$ $(i \in 1, \ldots, d)$ to any two elements in Ω or any two elements in $\overline{\Omega}$. Then all pairs $(\alpha_j, \alpha_{\overline{j}})$ $(j \in 1, \ldots, d)$ are mapped either to two elements in Ω or to two elements in $\overline{\Omega}$, and C is fixed by σ.*

Proof. Let σ map a pair of complex conjugates $(\alpha_i, \alpha_{\bar{i}})$ to two elements in Ω. By taking $d > 4$, at least three elements of $\sigma(\Omega)$ must be collinear, by the pigeonhole principle. Suppose without loss of generality that at least three elements of $\sigma(\Omega)$ lie on L and that $\alpha_{\sigma(i)}$ is one of them (for if $\alpha_{\sigma(i)}$ and $\alpha_{\sigma(\bar{i})}$ lie on $\overline{L}$, then there certainly exists an $\alpha_j \in \Omega$ such that $\alpha_{\sigma(j)}$ and $\alpha_{\sigma(\bar{j})}$ lie on L).

Let $\alpha_a, \alpha_b \neq \alpha_i$ be distinct elements in Ω such that $\alpha_{\sigma(a)}, \alpha_{\sigma(b)}$ and $\alpha_{\sigma(i)}$ are also in Ω. Applying σ to the following identity:

$$u = \frac{\alpha_a - \alpha_b}{\alpha_{\bar{a}} - \alpha_{\bar{b}}} = \frac{\alpha_a - \alpha_i}{\alpha_{\bar{a}} - \alpha_{\bar{i}}} = \frac{\alpha_b - \alpha_i}{\alpha_{\bar{b}} - \alpha_{\bar{i}}}$$

gives

$$u' = \frac{\alpha_{\sigma(a)} - \alpha_{\sigma(b)}}{\alpha_{\sigma(\bar{a})} - \alpha_{\sigma(\bar{b})}} = \frac{\alpha_{\sigma(a)} - \alpha_{\sigma(i)}}{\alpha_{\sigma(\bar{a})} - \alpha_{\sigma(\bar{i})}} = \frac{\alpha_{\sigma(b)} - \alpha_{\sigma(i)}}{\alpha_{\sigma(\bar{b})} - \alpha_{\sigma(\bar{i})}}. \tag{6.12}$$

By Lemma 6.2.1, $\alpha_{\sigma(\bar{a})}, \alpha_{\sigma(\bar{b})}$ and $\alpha_{\sigma(\bar{i})}$ must be collinear. From the assumption that $\alpha_{\sigma(\bar{i})} \in \Omega$, it follows that $\alpha_{\sigma(\bar{a})}$ and $\alpha_{\sigma(\bar{b})}$ are also elements in Ω. Hence $u' \in \mathbb{R}$.

Therefore, if some $\alpha_j \in \Omega$ is mapped by σ to an element $\alpha_{\sigma(j)} \in \Omega$, then $\alpha_{\bar{j}}$ is also mapped to an element in Ω. There must exist at least three distinct conjugates $\alpha_k, \alpha_m, \alpha_n \in \Omega$ such that $\alpha_{\sigma(k)}, \alpha_{\sigma(\bar{k})}, \alpha_{\sigma(m)}, \alpha_{\sigma(\bar{m})}, \alpha_{\sigma(n)}$ and $\alpha_{\sigma(\bar{n})} \in \overline{\Omega}$. By Lemma 6.2.1, if $\alpha_{\sigma(p)} \in \overline{\Omega}$ for some p, then $\alpha_{\sigma(\bar{p})} \in \overline{\Omega}$.

Now suppose $\sigma(C) = C'$, and let $\alpha_q, \alpha_r \in \Omega$ and $\alpha_{\bar{s}}, \alpha_{\bar{t}} \in \overline{\Omega}$ be conjugates of α such that

$$u' = \frac{\alpha_q - C'}{\alpha_r - C'} = \frac{\alpha_{\bar{s}} - C'}{\alpha_{\bar{t}} - C'}.$$

Since $u' \in \mathbb{R}$, C' must be collinear with α_q and α_r, so C' lies on L. Similarly, C' is collinear with $\alpha_{\bar{s}}$ and $\alpha_{\bar{t}}$, so C' lies on $\overline{L}$. Hence $\sigma(C) = C$. □

Remark. We show in Lemma 6.3.1 that such an automorphism σ defined as in Lemma 6.2.2 exists only if $C \in \mathbb{Q}$.

Corollary 6.2.3. *Let σ be an automorphism in the galois closure of C, u and α. If $\sigma(C) = C' \neq C$, then $\alpha_{\sigma(j)}$ and $\alpha_{\sigma(\bar{j})}$ do not both belong to Ω or $\overline{\Omega}$ for all $j \in \{1, \dots, d\}$.*

Proposition 6.2.4. *Let τ be an automorphism that maps $C \mapsto C' \neq C$. Suppose $\tau(\Omega) = \Omega'$. Then $\tau(\overline{\Omega}) = \overline{\Omega'}$.*

Proof. Suppose that $\tau(\overline{\Omega}) = \Omega'' \neq \overline{\Omega'}$. Then there exists some pair $\alpha_a, \alpha_{\bar{a}}$ such that $\tau(\alpha_i) = \alpha_a$ and $\tau(\alpha_j) = \alpha_{\bar{a}}$ for some i, j. Applying τ^{-1} to

$$u = \frac{\alpha_a - C}{\alpha_{\bar{a}} - C}$$

gives

$$u'' = \frac{\alpha_i - C''}{\alpha_j - C''}$$

where $C'' \neq C$. By Corollary 6.2.3, no such automorphism τ^{-1} exists. Hence $\tau(\Omega) = \overline{\Omega'}$. □

Lemma 6.2.5. *Any automorphism τ that maps $C \mapsto C' \neq C$ and $\Omega \mapsto \Omega'$ must map $u \mapsto u'$, where $|u'| = 1$.*

Proof. Consider an automorphism σ that maps $C \mapsto C' \neq C$. Apply σ to u:

$$\begin{aligned} \sigma(u) = u' &= \frac{\alpha_{\sigma(1)} - \alpha_{\sigma(2)}}{\alpha_{\sigma(\bar{1})} - \alpha_{\sigma(\bar{2})}} = \frac{\alpha_{\sigma(1)} - \alpha_{\sigma(3)}}{\alpha_{\sigma(\bar{1})} - \alpha_{\sigma(\bar{3})}} = \cdots \\ &= \frac{\alpha_{\sigma(i)} - \alpha_{\sigma(j)}}{\alpha_{\sigma(\bar{i})} - \alpha_{\sigma(\bar{j})}} = \cdots = \frac{\alpha_{\sigma(d-1)} - \alpha_{\sigma(d)}}{\alpha_{\sigma(\overline{d-1})} - \alpha_{\sigma(\bar{d})}}. \end{aligned}$$

By Proposition 6.2.4, $\sigma(\overline{\Omega}) = \overline{\Omega'}$.

Let i and j be such that

$$|\alpha_{\sigma(i)} - \alpha_{\sigma(j)}| = \max_{\alpha', \alpha'' \in \Omega'} |\alpha' - \alpha''|.$$

Then

$$u' = \frac{\alpha_{\sigma(i)} - \alpha_{\sigma(j)}}{\alpha_{\sigma(\bar{i})} - \alpha_{\sigma(\bar{j})}}$$

for some $\alpha_{\sigma(\bar{i})}, \alpha_{\sigma(\bar{j})} \in \overline{\Omega'}$. Since

$$\max_{\alpha', \alpha'' \in \Omega'} |\alpha' - \alpha''| = \max_{\alpha', \alpha'' \in \overline{\Omega'}} |\alpha' - \alpha''|,$$

$|u'| \geq 1$, and a similar argument gives $|u'| \leq 1$. Hence $|u'| = 1$. □

Remark. In fact, if $C \notin \mathbb{Q}$, we show in Lemma 6.3.3 that τ must map 0 or d conjugates from Ω to $\overline{\Omega}$.

Lemma 6.2.6. *The point of intersection C of L and $\overline{L}$ is totally real.*

Proof. Recall that if $C \notin \mathbb{Q}$, then as noted in the remark preceding Lemma 6.2.1, $\omega \neq C$ and $\frac{\omega - C}{\overline{\omega} - C} = u$. Apply an automorphism ϕ that maps $C \mapsto C' \neq C$. Let $\phi(\omega) = \omega'$. By Proposition 6.2.4, $\phi(\omega') = \overline{\omega'}$. So u is mapped to

$$u' = \frac{\omega' - C'}{\overline{\omega'} - C'},$$

and $|u'| = 1$, so C' is real. Hence C is totally real. □

6.3 Proving that C is rational or quadratic

Let $C \notin \mathbb{Q}$ be totally real. Define $\Omega, \overline{\Omega}$ and ω as in Section 6.2, and let α have degree at least 10.

Lemma 6.3.1. *Let ϕ be an automorphism that maps $C \mapsto C' \neq C$. Then ϕ does not map any pair of complex conjugates $(\alpha_i, \alpha_{\overline{i}})$ to an unordered pair $(\alpha_j, \alpha_{\overline{j}})$.*

Proof. Suppose such an automorphism ϕ does exist. By applying complex conjugation if necessary, we can assume that

$$\phi(u) = u' = \frac{\alpha_j - C'}{\alpha_{\overline{j}} - C'} = \frac{\alpha_j - \alpha'}{\alpha_{\overline{j}} - \alpha''} = \cdots .$$

Now suppose $\alpha' \in \Omega$, say $\alpha' = \alpha_k$. Then $\alpha'' \in \overline{\Omega}$, by Corollary 6.2.3. If $\alpha'' = \alpha_{\overline{k}}$, then

$$\frac{\alpha_j - C'}{\alpha_{\overline{j}} - C'} = \frac{\alpha_k - C'}{\alpha_{\overline{k}} - C'},$$

contradicting Equation (6.2) and the fact that $C' \neq C$. So $\alpha'' \neq \alpha_{\overline{k}}$. By Lemma 6.2.5, $|u'| = 1$. So there exists $\alpha_{\overline{m}} \in \overline{\Omega}$ such that

$$|\alpha_j - \alpha_k| = |\alpha_{\overline{j}} - \alpha_{\overline{m}}|.$$

But then $\alpha_k + \alpha_m = 2\alpha_j$, contradicting Lemma 2.1.5.

So for all $r \in \{1, \ldots, i-1, i+1, \ldots, d\}$, $\alpha_{\phi(r)} \in \overline{\Omega}$, and by the pigeonhole principle, $\alpha_{\phi(\overline{r})}$ lies on L. Furthermore, by the same argument as above, $\alpha_{\overline{\phi(r)}} \neq \alpha_{\phi(\overline{r})}$.

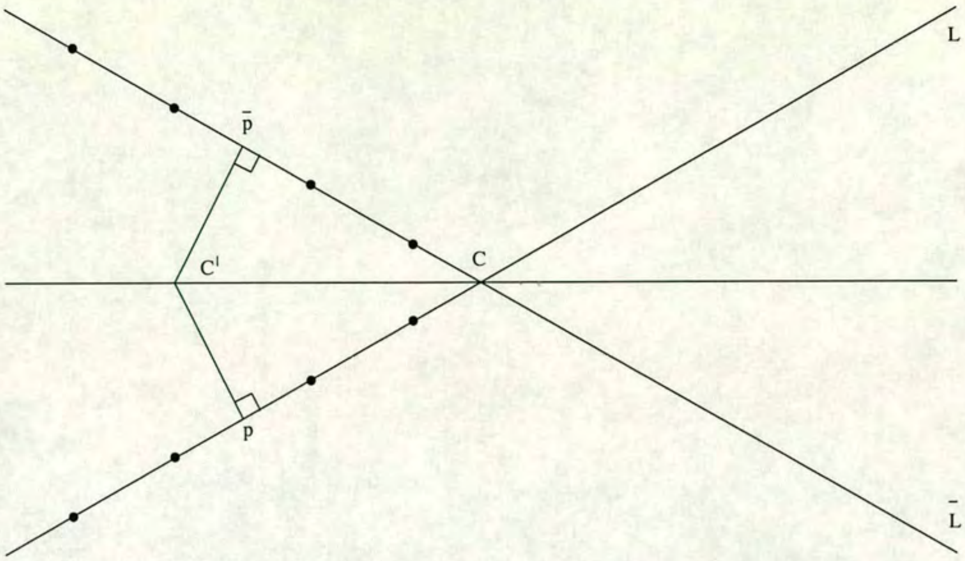
Thus for each conjugate $\alpha' \neq \alpha_j$ or $\alpha_{\overline{j}}$, there exists a conjugate $\alpha'' \neq \alpha'$ or $\overline{\alpha'}$ such that

$$|\alpha' - C'| = |\overline{\alpha'} - C'| = |\alpha'' - C'| = |\overline{\alpha''} - C'|.$$

Relabel the conjugates so that α_j is now α_d, and

$$\alpha_1 + \alpha_{d-1} = \alpha_2 + \alpha_{d-2} = \cdots = \alpha_{\frac{d-1}{2}} + \alpha_{\frac{d+1}{2}} = 2p \qquad (6.13)$$

for some point p lying on L such that $(p - C')$ has phase $\theta + \frac{\pi}{2}$:



Apply a suitable automorphism τ that maps $\alpha_1 \mapsto \alpha_d$. By the fact that there does not exist a conjugate α' of α such that $\alpha_d + \alpha' = 2p$, we have that $\tau(p) = p' \neq p$. Consider the cases (a) $\alpha_{\tau(d-1)} \in \Omega$ and (b) $\alpha_{\tau(d-1)} \in \overline{\Omega}$.

(a) Suppose $\alpha_{\tau(d-1)}$ lies on L. Then p' lies on L, so $\alpha_{\tau(2)}, \alpha_{\tau(3)}, \ldots, \alpha_{\tau(d-2)}$ also lie on L. Hence

$$2p' = \alpha_d + \alpha_{\tau(d-1)} = \alpha_a + \alpha_b = \cdots \tag{6.14}$$

for some $1 \leq a < b \leq d-1$. Also, there exists an α_m $(1 \leq m \leq d-1)$ such that $\alpha_{\tau(m)} = \alpha_{d-a}$ or α_{d-b}, say α_{d-a}. Then

$$2p' = \alpha_{\tau(m)} + \alpha_{\tau(d-m)} = \alpha_{d-a} + \alpha', \tag{6.15}$$

where α' lies on L. Clearly $\alpha_b \neq \alpha_{d-a}$, as $p' \neq p$. So equating (6.14) and (6.15) gives

$$\alpha_a + \alpha_b = \alpha_{d-a} + \alpha'. \tag{6.16}$$

From Equation (6.13),

$$\alpha_a + \alpha_{d-a} = \alpha_{d-b} + \alpha_b. \tag{6.17}$$

Adding Equations (6.16) and (6.17) gives

$$2\alpha_a = \alpha_{d-b} + \alpha'$$

contradicting Lemma 2.1.5.

(b) Suppose $\alpha_{\tau(d-1)}$ lies on $\overline{L}$. Then p' does not lie on L or $\overline{L}$. Exactly one of $\alpha_{\tau(2)}$ and $\alpha_{\tau(d-2)}$ lies on L, say $\alpha_{\tau(2)}$, and so $\alpha_{\tau(d-2)}$ lies on $\overline{L}$. Thus

$$2p' = \alpha_d + \alpha_{\tau(d-1)} = \alpha_{\tau(2)} + \alpha_{\tau(d-2)}.$$

Then

$$\alpha_d - \alpha_{\tau(2)} = \alpha_{\tau(d-2)} - \alpha_{\tau(d-1)}.$$

So the line through α_d and $\alpha_{\tau(2)}$ must be parallel to the line through $\alpha_{\tau(d-1)}$ and $\alpha_{\tau(d-2)}$, contradicting the fact that L and $\overline{L}$ intersect at C. The result follows. □

Corollary 6.3.2. *For all conjugates α_i of α, there exists a conjugate $\alpha_j \neq \alpha_i$ or $\alpha_{\overline{i}}$ such that*

$$|\alpha_i - C'| = |\alpha_{\overline{i}} - C'| = |\alpha_j - C'| = |\alpha_{\overline{j}} - C'|$$

where $C' \neq C$ is a conjugate of C.

Notation. we relabel the conjugates of α so that

$$\Re(\alpha_1) < \Re(\alpha_2) < \cdots < \Re(\alpha_d).$$

Lemma 6.3.3. *The mean ω of the conjugates of α that lie on L is quadratic.*

Proof. By Corollary 6.3.2, for every $\alpha_j \in \Omega$, there exists $\alpha_k \in \Omega$ such that $\alpha_j + \alpha_k = 2\omega$. Therefore

$$2\omega = \alpha_1 + \alpha_d = \alpha_2 + \alpha_{d-1} = \cdots = \alpha_{\frac{d}{2}} + \alpha_{\frac{d}{2}+1}$$

and

$$2\overline{\omega} = \alpha_{\overline{1}} + \alpha_{\overline{d}} = \alpha_{\overline{2}} + \alpha_{\overline{d-1}} = \cdots = \alpha_{\overline{\frac{d}{2}}} + \alpha_{\overline{\frac{d}{2}+1}}.$$

Apply an automorphism τ to ω. Consider the following:

1. $\alpha_{\tau(1)}, \alpha_{\tau(d)} \in \Omega$, in which case $\tau(\omega) = \omega'$ lies on L.

2. $\alpha_{\tau(1)}, \alpha_{\tau(d)} \in \overline{\Omega}$, in which case ω' lies on $\overline{L}$.

3. One of $\alpha_{\tau(1)}, \alpha_{\tau(d)}$ belongs to Ω, and the other belongs to $\overline{\Omega}$, in which case ω' neither lies on L nor $\overline{L}$.

(1) Let $\alpha_{\tau(1)}, \alpha_{\tau(d)} \in \Omega$. Then all the $\alpha_i \in \Omega$ are mapped by τ to a conjugate in Ω. So $\tau(\omega) = \omega$.

(2) Using exactly the same argument as in (1), $\tau(\omega) = \overline{\omega}$.

(3) Let one of $\alpha_{\tau(1)}, \alpha_{\tau(d)}$ belong to Ω and the other to $\overline{\Omega}$. Then exactly one of each of the pairs

$$(\alpha_{\tau(2)}, \alpha_{\tau(d-1)}), \ldots, (\alpha_{\tau(\frac{d}{2})}, \alpha_{\tau(\frac{d}{2}+1)}), (\alpha_{\tau(\overline{1})}, \alpha_{\tau(\overline{d})}), \ldots, (\alpha_{\tau(\overline{\frac{d}{2}})}, \alpha_{\tau(\overline{\frac{d}{2}+1})})$$

belongs to Ω.

Suppose without loss of generality that $\alpha_{\tau(1)}, \alpha_{\tau(2)} \in \Omega$.

Therefore $\alpha_{\tau(d)}, \alpha_{\tau(d-1)} \in \overline{\Omega}$. Hence

$$2\tau(\omega) = 2\omega' = \alpha_{\tau(1)} + \alpha_{\tau(d)} = \alpha_{\tau(2)} + \alpha_{\tau(d-1)}.$$

So

$$\alpha_{\tau(1)} - \alpha_{\tau(2)} = \alpha_{\tau(d-1)} - \alpha_{\tau(d)},$$

which implies that the line through $\alpha_{\tau(1)}$ and $\alpha_{\tau(2)}$ is parallel to the line through $\alpha_{\tau(d)}$ and $\alpha_{\tau(d-1)}$. But L and $\overline{L}$ are not parallel, so no such automorphism exists. Therefore $\tau(\omega) = \omega$ or $\overline{\omega}$. Hence ω is quadratic. □

Corollary 6.3.4. *The set of conjugates $\{\alpha_1, \ldots, \alpha_d\} = \Omega$ are either all mapped to conjugates in Ω, or are all mapped to conjugates in $\overline{\Omega}$.*

Lemma 6.3.5. *The point of intersection C is quadratic, and either $u = i$, or u is quartic with conjugates $\pm u^{\pm 1}$. Any automorphism will map C, u and ω in one of the following ways:*

1. *$C \mapsto C, u \mapsto u$ and $\omega \mapsto \omega$,*

2. *$C \mapsto C, u \mapsto u^{-1}$ and $\omega \mapsto \overline{\omega}$,*

3. *$C \mapsto C', u \mapsto -u$ and $\omega \mapsto \omega$, or*

4. *$C \mapsto C', u \mapsto -u^{-1}$ and $\omega \mapsto \overline{\omega}$.*

Furthermore, all four possibilities occur.

Proof. Apply an automorphism ϕ to Equation (6.1). Consider $\phi(\omega) = \omega$ or $\phi(\omega) = \overline{\omega}$:

(a) Let $\phi(\omega) = \omega$. Apply ϕ to u:

$$\phi(u) = u' = \frac{\alpha_1 - \alpha_d}{\alpha_{\overline{a}} - \alpha_{\overline{b}}} = \frac{\alpha_1 - \phi(C)}{\alpha_{\overline{a}} - \phi(C)} = \frac{\alpha_d - \phi(C)}{\alpha_{\overline{b}} - \phi(C)} = \frac{\omega - \phi(C)}{\overline{\omega} - \phi(C)}.$$

By the relabelling above,

$$\max_{\alpha', \alpha'' \in \Omega} |\alpha' - \alpha''| = |\alpha_1 - \alpha_d|.$$

By the maximality of $|\alpha_1 - \alpha_d|$, either

(a1) $\alpha_{\overline{a}} = \alpha_{\overline{1}}$ and $\alpha_{\overline{b}} = \alpha_{\overline{d}}$, or

(a2) $\alpha_{\overline{a}} = \alpha_{\overline{d}}$ and $\alpha_{\overline{b}} = \alpha_{\overline{1}}$:

(a1) $u' = \frac{\alpha_1 - \alpha_d}{\alpha_{\overline{1}} - \alpha_{\overline{d}}} = u$, and

$$\frac{\alpha_1 - \phi(C)}{\alpha_{\overline{1}} - \phi(C)} = \frac{\alpha_d - \phi(C)}{\alpha_{\overline{d}} - \phi(C)}$$

gives

$$\phi(C) = \frac{\alpha_1 \alpha_{\overline{d}} - \alpha_{\overline{1}} \alpha_d}{\alpha_1 - \alpha_{\overline{1}} - \alpha_d + \alpha_{\overline{d}}} = C.$$

(a2) $u' = \frac{\alpha_1 - \alpha_d}{\alpha_{\overline{d}} - \alpha_{\overline{1}}} = -u$, and

$$\frac{\alpha_1 - \phi(C)}{\alpha_{\overline{d}} - \phi(C)} = \frac{\alpha_d - \phi(C)}{\alpha_{\overline{1}} - \phi(C)}$$

implies that

$$\phi(C) = \frac{\alpha_1 \alpha_{\overline{1}} - \alpha_d \alpha_{\overline{d}}}{\alpha_1 + \alpha_{\overline{1}} - \alpha_d - \alpha_{\overline{d}}}.$$

(b) Let $\phi(\omega) = \overline{\omega}$. Apply ϕ to u: As above,

$$\phi(u) = u' = \frac{\alpha_{\overline{1}} - \alpha_{\overline{d}}}{\alpha_a - \alpha_b} = \frac{\alpha_{\overline{1}} - \phi(C)}{\alpha_a - \phi(C)} = \frac{\alpha_{\overline{d}} - \phi(C)}{\alpha_b - \phi(C)} = \frac{\overline{\omega} - \phi(C)}{\omega - \phi(C)}.$$

By the maximality of $|\alpha_{\overline{1}} - \alpha_{\overline{d}}|$, either
(b1) $\alpha_a = \alpha_1$ and $\alpha_b = \alpha_d$, or
(b2) $\alpha_a = \alpha_d$ and $\alpha_b = \alpha_1$.

Consider

$$\frac{\overline{\omega} - \phi(C)}{\omega - \phi(C)} = e^{-2i\theta}. \tag{6.18}$$

Case (b1) implies that $u' = u^{-1}$, and Equation (6.18) gives $\phi(C) = C$.
Case (b2) implies that $u' = -u^{-1}$, and Equation (6.18) implies that

$$\phi(C) = \frac{\alpha_1 \alpha_{\overline{1}} - \alpha_d \alpha_{\overline{d}}}{\alpha_1 + \alpha_{\overline{1}} - \alpha_d - \alpha_{\overline{d}}}.$$

So for any automorphism σ, $\sigma(C) = C$ or C', where $C' = \frac{\alpha_1 \alpha_{\overline{1}} - \alpha_d \alpha_{\overline{d}}}{\alpha_1 + \alpha_{\overline{1}} - \alpha_d - \alpha_{\overline{d}}}$. Hence C is quadratic.

Now apply an automorphism σ_C that maps $C \mapsto C$. Suppose $\sigma_C(\omega) = \omega$. Then $\sigma_C(u) = u$. This is case 1 above. Applying compex conjugation gives case 2.

Apply an automorphism $\sigma_{C'}$ that maps $C \mapsto C'$. Suppose $\sigma_C(\omega) = \omega$. Then $\sigma_{C'}(u) = -u$. This is case 3 above. Applying compex conjugation gives case 4. □

6.4 Constructing the α_i for quadratic C

Let $C \in \mathbb{Q}(\sqrt{n})$ be quadratic for some square-free $n \in \mathbb{N}$, with conjugate $C' \neq C$. Let $\Omega, \overline{\Omega}$ and ω be defined as in Section 6.2, and let α have degree at least 10.

Lemma 6.4.1. *Either $u = i$, or C and $\omega \in \mathbb{Q}(u)$.*

Proof. Suppose that $u \neq i$. Then $\theta \neq \frac{\pi}{4}$. Recall

$$u = \frac{\alpha_1 - \alpha_d}{\alpha_{\overline{1}} - \alpha_{\overline{d}}}. \tag{6.19}$$

Suppose that $\omega \notin \mathbb{Q}(u)$. Apply an automorphism ϕ to Equation (6.19) that maps $\omega \mapsto \overline{\omega}$ but keeps u fixed. Then $\alpha_1 \mapsto \alpha_{\overline{a}}$ and $\alpha_d \mapsto \alpha_{\overline{b}}$ for some $\alpha_{\overline{a}}, \alpha_{\overline{b}} \in \overline{\Omega}$. But then

$$u = \frac{\alpha_{\overline{a}} - \alpha_{\overline{d-a+1}}}{\alpha_{\phi(\overline{1})} - \alpha_{\phi(\overline{d})}}.$$

This contradicts $u = e^{2i\theta}$, by our assumption $\theta \neq \frac{\pi}{4}$. So $\omega \in \mathbb{Q}(u)$.

Now suppose $C \notin \mathbb{Q}(u)$. Apply an automorphism τ that maps $C \mapsto C' \neq C, u \mapsto u$ and $\omega \mapsto \omega$. Then

$$u = \frac{\omega - C}{\overline{\omega} - C} = \frac{\omega - C'}{\overline{\omega} - C'},$$

contradicting $C' \neq C$. □

Lemma 6.4.2. *We can write ω and $\overline{\omega}$ as follows:*

$$\omega = \frac{1}{d}\sum_{i=1}^{d} \alpha_i = \frac{C + C'}{2} + \frac{C' - C}{2}u$$

and

$$\overline{\omega} = \frac{1}{d}\sum_{i=1}^{d} \alpha_{\overline{i}} = \frac{C + C'}{2} + \frac{C' - C}{2}u^{-1}.$$

Proof. By Lemma 6.3.5, there exists an automorphism τ that maps $C \mapsto C', u \mapsto -u$ and $\omega \mapsto \omega$. Applying τ to

$$\omega = u\overline{\omega} - uC + C \tag{6.20}$$

gives

$$\omega = -u\overline{\omega} + uC' + C'. \tag{6.21}$$

Adding Equations (6.20) and (6.21) gives

$$\omega = \frac{C + C'}{2} + \frac{C' - C}{2}u.$$

Applying complex conjugation will complete the proof. □

Remark. Any real quadratic C can be written in the form $c + d\sqrt{n}$, where $c, d \in \mathbb{Q}, n \in \mathbb{N}$ is squarefree. Where appropriate, we assume that $C = \sqrt{n}$ and $C' = -\sqrt{n}$, noting that the general case can be obtained from this by translating and scaling if necessary.

Lemma 6.4.3. *We can write u in the form $\frac{a\sqrt{n}+b\sqrt{-k}}{e}$, where $a \in \mathbb{N}_{\geq 0}$, $b \in \mathbb{Z}^*$, $e \in \mathbb{N}$, $k \in \mathbb{N}$ is squarefree or equal to 1, and $a^2n + b^2k = e^2$.*

Proof. By the above remark, we can assume that $C = \sqrt{n}$ for some squarefree $n \in \mathbb{N}$. Note that $\Re(u) = \frac{1}{2}(u + u^{-1})$ is quadratic. By Lemma 6.3.5, when C is mapped to itself, u is mapped to $u^{\pm 1}$, and hence $\Re(u) \mapsto \Re(u)$, and when C is mapped to $C' \neq C$, u is mapped to $-u^{\pm 1}$ and $\Re(u) \mapsto -\Re(u)$. So either $\Re(u) = 0$ (if $u = i$), or $\Re(u) = h\sqrt{n}$ for some $h \in \mathbb{Q}$. By Theorem 1.3.10, each of the following extensions has degree two.

$$\begin{tikzcd}
\mathbb{Q}(u) \arrow[d, dash] \\
\mathbb{Q}(\sqrt{n}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

Note that $\mathbb{Q}(u) = \mathbb{Q}(\sqrt{n}, i\Im(u))$. Thus $i\Im(u)$ has degree two. Hence u must be of the form

$$\frac{a\sqrt{n} + b\sqrt{-k}}{e}$$

where $a \in \mathbb{N}_{\geq 0}$, $b \in \mathbb{Z}^*$, $e \in \mathbb{N}$, and $k \in \mathbb{N}$ is squarefree or equal to 1. Finally, $|u| = 1$, so $a^2n + b^2k = e^2$. □

The following result is taken from Niven and Zuckerman [17], Theorem 5.16, with $c = -1$:

Proposition 6.4.4. *Let k and n be given non zero square-free positive integers such that*

$$a^2n + b^2k - e^2 = 0.$$

A necessary and sufficient condition that such an equation has at least one non zero solution (a, b, e) is that n is a quadratic residue mod k, k is a quadratic residue mod n and nk is square-free.

The following is the main theorem for algebraic numbers lying with their conjugates on $S_\times(C, \sqrt{u})$ for quadratic C:

Theorem 6.4.5. *Let $C \in \mathbb{Q}(\sqrt{n})$ be quadratic for some square-free $n \in \mathbb{N}$, with conjugate $C' \neq C$.*

1. *When $u = i$ and r is totally real define*

$$\alpha = \frac{C + C'}{2} + i\frac{C' - C}{2} + r\sqrt{\epsilon i(C' - C)},$$

where

$$\epsilon = \begin{cases} 1, & \textit{if } C < C'; \\ -1, & \textit{if } C' < C. \end{cases}$$

2. *When $u = \frac{a\sqrt{n}+b\sqrt{-k}}{e}$ such that $a \in \mathbb{N}_{\geq 0}$, $b \in \mathbb{Z}^*$, $e \in \mathbb{N}$, $k \in \mathbb{N}$ is square-free or equal to 1 and $a^2n + b^2k = e^2$,and r is totally real define*

$$\alpha = \frac{C + C'}{2} + u\frac{C' - C}{2} + r\sqrt{u(u + u^{-1})}.$$

Then α and all its conjugates lie on $S_\times(C, \sqrt{u})$.

Conversely, suppose α is an algebraic number of degree at least 10 that lies with its conjugates on $S_\times(C, \sqrt{u})$, where $C \notin \mathbb{Q}$. Then $C \in \mathbb{Q}(\sqrt{n})$ has a conjugate $C' \neq C$, $n \in \mathbb{N}$ is square-free, and α can be written in one of the following forms:

1.

$$\alpha = \frac{C + C'}{2} + i\frac{C' - C}{2} + r\sqrt{\epsilon i(C' - C)},$$

where r is totally real and

$$\epsilon = \begin{cases} 1, & \textit{if } C' > C; \\ -1, & \textit{if } C > C', \textit{ or} \end{cases}$$

2.

$$\alpha = \frac{C + C'}{2} + u\frac{C' - C}{2} + r\sqrt{u(u + u^{-1})}$$

where $u = \frac{a\sqrt{n}+b\sqrt{-k}}{e}$, $a \in \mathbb{N}_{\geq 0}$, $b \in \mathbb{Z}^*$, $e \in \mathbb{N}$, $k \in \mathbb{N}$ is square-free or equal to 1 and $a^2n + b^2k = e^2$, and r is totally real.

Proof. ($\Rightarrow$) 1. Let $u = i$, let $C \in \mathbb{Q}(\sqrt{n})$ be quadratic for some square-free $n \in \mathbb{N}$ have a conjugate $C' \neq C$, and let r be totally real. Define

$$\alpha = \frac{C + C'}{2} + i\frac{C' - C}{2} + r\sqrt{\epsilon i(C' - C)},$$

where

$$\epsilon = \begin{cases} 1, & \text{if } C' > C; \\ -1, & \text{if } C > C'. \end{cases}$$

Define $\omega = \frac{C+C'}{2} + i\frac{C'-C}{2}$. Then $(\omega - C)$ has phase $\frac{\pi}{4}$. Hence ω lies on L, and so does

$$\alpha = \omega + r\sqrt{\epsilon i(C' - C)}.$$

Apply an automorphism σ to α. Then C and i are mapped in one of the following ways:

1. $C \mapsto C, i \mapsto i$,

2. $C \mapsto C, i \mapsto -i$,

3. $C \mapsto C', i \mapsto i$, and

4. $C \mapsto C', i \mapsto -i$.

Consider cases 1 and 4. Here $\omega \mapsto \omega$, $i(C' - C) \mapsto i(C' - C)$ and $r \mapsto r' \in \mathbb{R}$. So

$$\sigma(\alpha) = \alpha' = \frac{C + C'}{2} + i\frac{C' - C}{2} \pm r'\sqrt{\epsilon i(C' - C)},$$

lies on L.

Consider cases 2 and 3. Here $\omega \mapsto \overline{\omega}$, $i(C' - C) \mapsto -i(C' - C)$ and $r \mapsto r' \in \mathbb{R}$. So

$$\sigma(\alpha) = \alpha' = \frac{C + C'}{2} - i\frac{C' - C}{2} \pm r'\sqrt{-\epsilon i(C' - C)},$$

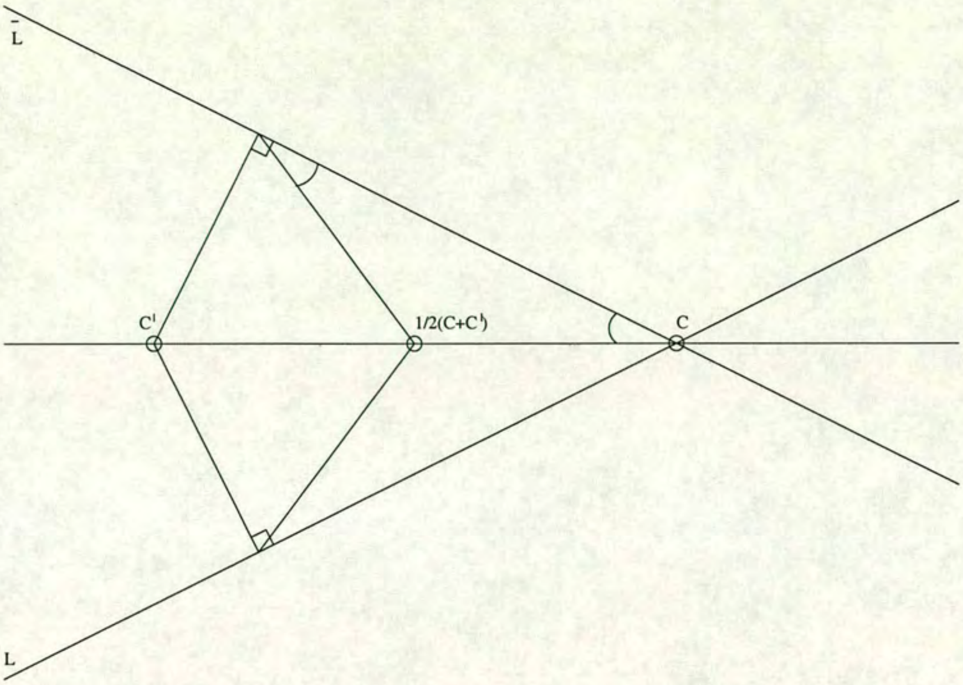
lies on $\overline{L}$.

Hence α and all its conjugates lie on $S_\times(C, \sqrt{i})$.

2. Let $C \in \mathbb{Q}(\sqrt{n})$ for some square-free $n \in \mathbb{N}$ have a conjugate $C' \neq C$. Let $u = \frac{a\sqrt{n}+b\sqrt{-k}}{e}$ be such that $a \in \mathbb{N}_{\geq 0}$, $b \in \mathbb{Z}^*$, $e \in \mathbb{N}$, $k \in \mathbb{N}$ is square-free or equal to 1, and $a^2n + b^2k = e^2$. Let r be totally real.

Define

$$\alpha = \frac{C + C'}{2} - u\frac{C - C'}{2} + r\sqrt{u(u + u^{-1})}.$$



As $\frac{C'-C}{2}(1+u)$ has phase θ, $\frac{C+C'}{2} - u\frac{C-C'}{2}$ lies on L, and so does

$$\alpha = \frac{C+C'}{2} - u\frac{C-C'}{2} + r\sqrt{u(u+u^{-1})}.$$

Now apply an automorphism σ in the galois closure of C, u and r to α. An automorphism will map $\sqrt{n}$ and $\sqrt{-k}$ in one of the following ways:

1. $\sqrt{n} \mapsto \sqrt{n}$ and $\sqrt{-k} \mapsto \sqrt{-k}$.
2. $\sqrt{n} \mapsto \sqrt{n}$ and $\sqrt{-k} \mapsto -\sqrt{-k}$.
3. $\sqrt{n} \mapsto -\sqrt{n}$ and $\sqrt{-k} \mapsto \sqrt{-k}$.
4. $\sqrt{n} \mapsto -\sqrt{n}$ and $\sqrt{-k} \mapsto -\sqrt{-k}$.

Consider case 1:

Here u and C are fixed by σ, and $r\sqrt{u(u+u^{-1})} \mapsto \epsilon r'\sqrt{u(u+u^{-1})}$, where $r' \in \mathbb{R}$ and $\epsilon = \pm 1$, so $\sigma(\alpha)$ lies on L.

Consider case 2:

Here $u \mapsto u^{-1}$, $C \mapsto C$, and $r\sqrt{u(u+u^{-1})} \mapsto \epsilon r'\sqrt{u^{-1}(u+u^{-1})}$, where $r' \in \mathbb{R}$ and $\epsilon = \pm 1$, so $\sigma(\alpha)$ lies on $\overline{L}$.

Consider case 3:

Here $u \mapsto -u^{-1}$, $C \mapsto C'$, and $r\sqrt{u(u+u^{-1})} \mapsto \epsilon r'\sqrt{u^{-1}(u+u^{-1})}$, where $r' \in \mathbb{R}$ and $\epsilon = \pm 1$, so $\sigma(\alpha)$ lies on $\overline{L}$.

Consider case 4:

Here $u \mapsto -u$, $C \mapsto C'$, and $r\sqrt{u(u+u^{-1})} \mapsto \epsilon r'\sqrt{u(u+u^{-1})}$, where $r' \in \mathbb{R}$ and $\epsilon = \pm 1$, so $\sigma(\alpha)$ lies on L.

Hence α and all its conjugates lie on $S_\times(C, \sqrt{u})$.

($\Leftarrow$) Now suppose α and all its conjugates lie on $S_\times(C, \sqrt{u})$, for some $C \notin \mathbb{Q}$. By Lemma 6.3.5, C is a real quadratic, say $C \in \mathbb{Q}(\sqrt{n})$, for some squarefree $n \in \mathbb{N}$, with conjugate $C' \neq C$. By Lemma 6.4.3, $u = \frac{a\sqrt{n}+b\sqrt{-k}}{e}$, where $a \in \mathbb{N}_{\geq 0}, b \in \mathbb{Z}^*, e \in \mathbb{N}, k \in \mathbb{N}$ is squarefree or equal to 1, and $a^2n + b^2k = e^2$. Hence either $u = i$, or u has conjugates $\pm u^{\pm 1}$.

Define

$$\Omega = \{\alpha_1 = \alpha, \ldots, \alpha_d\}$$

as the set of conjugates of α that lie on L, and

$$\overline{\Omega} = \{\alpha_{\overline{1}}, \ldots, \alpha_{\overline{d}}\}$$

as the set of conjugates of α that lie on $\overline{L}$. Define

$$\omega = \frac{1}{d}\sum_{\alpha' \in \Omega} \alpha', \qquad \text{and therefore,}$$

$$\overline{\omega} = \frac{1}{d}\sum_{\alpha' \in \overline{\Omega}} \alpha'.$$

By Lemmas 6.3.5 and 6.4.2, $\omega = \frac{C+C'}{2} + u\frac{C'-C}{2}$ is quadratic.

1. Let $u = i$. Then for some algebraic $r \in \mathbb{R}$,

$$\alpha = \omega + r\sqrt{\epsilon i(C'-C)}, \tag{6.22}$$

where

$$\epsilon = \begin{cases} 1, & \text{if } C' > C; \\ -1, & \text{if } C > C'. \end{cases}$$

We show that r is totally real. Apply an automorphism τ to Equation (6.22). Consider the following:

1. $C \mapsto C, i \mapsto i$ and $\omega \mapsto \omega$,

2. $C \mapsto C, i \mapsto -i$ and $\omega \mapsto \overline{\omega}$,

3. $C \mapsto C', i \mapsto i$ and $\omega \mapsto \overline{\omega}$, and

4. $C \mapsto C', i \mapsto -i$ and $\omega \mapsto \omega$.

Consider cases 1 and 4:
Since $\omega \mapsto \omega$, $\tau(\alpha)$ remains on L, and

$$r' = \delta \frac{\tau(\alpha) - \omega}{\sqrt{\epsilon i(C' - C)}}$$

(for some $\delta = \pm 1$) is real.

Consider cases 2 and 3:
Since $\omega \mapsto \overline{\omega}$, $\tau(\alpha)$ is mapped onto $\overline{L}$, and

$$r' = \delta \frac{\tau(\alpha) - \overline{\omega}}{\sqrt{-\epsilon i(C' - C)}}$$

(for some $\delta = \pm 1$) is real.
Hence r is totally real.

2. Let $u = \frac{a\sqrt{n}+b\sqrt{-k}}{e}$ be such that $a \in \mathbb{N}_{\geq 0}$, $b \in \mathbb{Z}^*$, $e \in \mathbb{N}$, $k \in \mathbb{N}$ is squarefree or equal to 1, and $a^2n + b^2k = e^2$. Then for some algebraic $r \in \mathbb{R}$,

$$\alpha = \omega + r\sqrt{u(u + u^{-1})}. \qquad (6.23)$$

We show that r is totally real. Apply an automorphism τ to Equation (6.23). Consider the following:

1. $C \mapsto C, u \mapsto u$ and $\omega \mapsto \omega$,

2. $C \mapsto C, u \mapsto u^{-1}$ and $\omega \mapsto \overline{\omega}$,

3. $C \mapsto C', u \mapsto -u^{-1}$ and $\omega \mapsto \overline{\omega}$, and

4. $C \mapsto C', u \mapsto -u$ and $\omega \mapsto \omega$.

Consider cases 1 and 4:
Since $\omega \mapsto \omega$, $\tau(\alpha)$ remains on L, and

$$r' = \delta \frac{\tau(\alpha) - \omega}{\sqrt{u(u + u^{-1})}}$$

(for some $\delta = \pm 1$) is real.

Consider cases 2 and 3:

Since $\omega \mapsto \overline{\omega}$, $\tau(\alpha)$ is mapped onto $\overline{L}$, and

$$r' = \delta \frac{\tau(\alpha) - \overline{\omega}}{\sqrt{u^{-1}(u + u^{-1})}}$$

(for some $\delta = \pm 1$) is real.

Hence r is totally real. The result follows. □

Example 6.4.6. Let $u = \frac{2\sqrt{5}+\sqrt{-5}}{5}$ and $C = 2 + \sqrt{5}$. The conjugates of u are $u_1 = u, u_2 = u^{-1}, u_3 = -u$ and $u_4 = -u^{-1}$. Define

$$\alpha = \alpha_1 = -i + (1 + \sqrt{3})\sqrt{\frac{4\sqrt{5}}{5}u}.$$

Then α is an algebraic number of degree 8 with conjugates

$$\begin{aligned}
\alpha_2 &= -i - (1 + \sqrt{3})\sqrt{\frac{4\sqrt{5}}{5}u}, \\
\alpha_3 &= i + (1 + \sqrt{3})\sqrt{\frac{4\sqrt{5}}{5}u^{-1}}, \\
\alpha_4 &= i - (1 + \sqrt{3})\sqrt{\frac{4\sqrt{5}}{5}u^{-1}}, \\
\alpha_5 &= -i + (1 - \sqrt{3})\sqrt{\frac{4\sqrt{5}}{5}u}, \\
\alpha_6 &= -i - (1 - \sqrt{3})\sqrt{\frac{4\sqrt{5}}{5}u}, \\
\alpha_7 &= i + (1 - \sqrt{3})\sqrt{\frac{4\sqrt{5}}{5}u^{-1}}, \\
\alpha_8 &= i - (1 - \sqrt{3})\sqrt{\frac{4\sqrt{5}}{5}u^{-1}}, \qquad (6.24)
\end{aligned}$$

all of which lie on $S_\times\left(2 + \sqrt{5}, \sqrt{\frac{2\sqrt{5}+\sqrt{-5}}{5}}\right)$.

Here $\omega = -i$, and $r = 1 + \sqrt{3}$. The minimal polynomial P_α of α is

$$X^8 - \frac{108}{5}X^6 - \frac{128}{5}X^5 + \frac{5014}{25}X^4 + \frac{768}{25}X^3 + \frac{484}{25}X^2 - \frac{2176}{5}X + \frac{18457}{25}.$$

Example 6.4.7. Let $u = \frac{\sqrt{5}+\sqrt{-11}}{4}$ and $C = \frac{5}{4} + \sqrt{5}$. The conjugates of u are $u_1 = u, u_2 = u^{-1}, u_3 = -u$ and $u_4 = -u^{-1}$. Define

$$\alpha = \alpha_1 = -\frac{\sqrt{-55}}{4} + (1 + \sqrt{3})\sqrt{\frac{\sqrt{5}}{2}u}.$$

Then α is an algebraic number of degree 8 with conjugates

$$\begin{aligned}
\alpha_2 &= -\frac{\sqrt{-55}}{4} - (1+\sqrt{3})\sqrt{\frac{\sqrt{5}}{2}u},\\
\alpha_3 &= \frac{\sqrt{-55}}{4} + (1+\sqrt{3})\sqrt{\frac{\sqrt{5}}{2}u^{-1}},\\
\alpha_4 &= \frac{\sqrt{-55}}{4} - (1+\sqrt{3})\sqrt{\frac{\sqrt{5}}{2}u^{-1}},\\
\alpha_5 &= -\frac{\sqrt{-55}}{4} + (1-\sqrt{3})\sqrt{\frac{\sqrt{5}}{2}u},\\
\alpha_6 &= -\frac{\sqrt{-55}}{4} - (1-\sqrt{3})\sqrt{\frac{\sqrt{5}}{2}u},\\
\alpha_7 &= \frac{\sqrt{-55}}{4} + (1-\sqrt{3})\sqrt{\frac{\sqrt{5}}{2}u^{-1}},\\
\alpha_8 &= \frac{\sqrt{-55}}{4} - (1-\sqrt{3})\sqrt{\frac{\sqrt{5}}{2}u^{-1}},
\end{aligned} \tag{6.25}$$

all of which lie on $S_\times\left(\frac{5}{4}+\sqrt{5}, \sqrt{\frac{\sqrt{5}+\sqrt{-11}}{4}}\right)$.

Here $r = 1+\sqrt{3}$, and the minimal polynomial of α is

$$X^8 - \frac{15}{4}X^6 - \frac{385}{4}X^5 + \frac{32615}{128}X^4 - \frac{20625}{32}X^3 + \frac{2100325}{1024}X^2 - \frac{1348325}{1024}X - \frac{249768025}{65536}.$$

6.5 Constructing α for rational C

Let $C \in \mathbb{Q}$. It can be assumed that $C = 0$ by translating if necessary. We shall state results with general $C \in \mathbb{Q}$, but, in the proofs, assume $C = 0$ (where convenient). Define $\Omega, \overline{\Omega}$ and ω as in Section 6.2.

The Equations (6.1) simplify to:

$$\frac{\alpha_1}{\alpha_{\overline{1}}} = \frac{\alpha_2}{\alpha_{\overline{2}}} = \cdots = \frac{\alpha_d}{\alpha_{\overline{d}}} = e^{2i\theta} = u, \tag{6.26}$$

and applying complex conjugation gives

$$\frac{\alpha_{\overline{1}}}{\alpha_1} = \frac{\alpha_{\overline{2}}}{\alpha_2} = \cdots = \frac{\alpha_{\overline{d}}}{\alpha_d} = e^{-2i\theta} = u^{-1}.$$

Lemma 6.5.1. *Either*

1. *u has four non real conjugates $\pm u^{\pm 1}$, and all other conjugates are real, or*

2. *All conjugates u are real except u and u^{-1}.*

Proof. Consider the two cases:

1. $-\alpha$ is a conjugate of α, and

2. $-\alpha$ is not a conjugate of α.

1. Relabel the conjugates so that

$$\Re(\alpha_1) < \Re(\alpha_2) < \cdots < \Re(\alpha_d).$$

Thus α_1 and α_d will have equal largest modulus of the α_i. Apply an automorphism that maps $u \mapsto u'$. Suppose $|u'| > 1$. There exist conjugates α', α'' such that

$$u' = \frac{\alpha_d}{\alpha'} = \frac{\alpha_{\overline{d}}}{\alpha''}.$$

If u' has phase 2θ, then α'' has phase -3θ. Thus $-3\theta = \theta$. The only solution that satisfies $0 < \theta < \frac{\pi}{2}$ is $\theta = \frac{\pi}{4}$. This gives $u = i$, contradicting $|u'| > 1$.

Similarly, if u' has phase -2θ, then α' has phase 3θ. So again $-3\theta = \theta$, and the only solution that satisfies $0 < \theta < \frac{\pi}{2}$ is $\theta = \frac{\pi}{4}$. This gives $u = i$, contradicting $|u'| > 1$.

Hence if $|u'| > 1$, then u' has phase zero, and so $u' \in \mathbb{R}$. Since u^{-1} is a conjugate of u, it follows immediately that if $|u'| < 1$, then $u' \in \mathbb{R}$.

Now suppose $|u'| = 1$. Then u' has phase $\pm 2\theta$. If u' has phase 2θ, then either $u' = \frac{\alpha_1}{\alpha_{\overline{1}}}$ (in which case $u' = u$), or $u' = \frac{\alpha_1}{\alpha_{\overline{d}}}$ (in which case $u' = -u$).

If u' has phase -2θ, then either $u' = \frac{\alpha_{\overline{1}}}{\alpha_1}$ (in which case $u' = u^{-1}$), or $u' = \frac{\alpha_{\overline{1}}}{\alpha_d}$ (in which case $u' = -u^{-1}$).

2. Suppose that $-\alpha$ is not a conjugate of α. Relabel the $\alpha_i \in \Omega$ such that

$$|\alpha_1| < |\alpha_2| < \cdots < |\alpha_d|.$$

Then for all $\alpha_i, \alpha_j \in \Omega$, $|\alpha_i| \neq |\alpha_j|$. If $|u'| = 1$, then clearly $u' = u$ or u^{-1}. If $|u'| > 1$, then

$$u' = \frac{\alpha_d}{\alpha'} = \frac{\alpha_{\overline{d}}}{\alpha''},$$

and as above, this implies that $u' \in \mathbb{R}$. Since u^{-1} is a conjugate of u, it follows immediately that, if $|u'| < 1$, $u' \in \mathbb{R}$. The result follows. □

Corollary 6.5.2. *Suppose the number of conjugates of α on each line is odd. Then u is quadratic.*

Proof. Let d be odd. Apply an automorphism ϕ to Equation (6.26). Thus

$$\phi(u) = u' = \frac{\alpha_{\phi(1)}}{\alpha_{\phi(\bar{1})}} = \cdots = \frac{\alpha_{\phi(d)}}{\alpha_{\phi(\bar{d})}}.$$

Suppose $u' \in \mathbb{R}$. For all i, if $\alpha_{\phi(i)}$ lies on L, then so does $\alpha_{\phi(\bar{i})}$, and similarly, if $\alpha_{\phi(i)}$ lies on $\overline{L}$, then so does $\alpha_{\phi(\bar{i})}$. But there is an odd number of conjugates on L, so there must be at least one $\alpha_{\phi(j)}$ that contradicts this condition. Hence u has no real conjugates, and any conjugate of u must have phase $\pm 2\theta$. If $-u$ is a conjugate of u, then $-\alpha$ must be a conjugate of α. But if $-\alpha$ is a conjugate of α, then the number of conjugates on L must be even. Hence the only conjugate of u is u^{-1}. □

Lemma 6.5.3. *Let $u_1 = e^{2i\theta}$ be an algebraic number such that either:*

1. *u_1 has conjugates u_1^{-1} and $u_2^{\pm 1}, \ldots, u_g^{\pm 1}$, where $u_j \in \mathbb{R}$ for $2 \le j \le g$.*
2. *u_1 has conjugates $\pm u_1^{-1}$ and $\pm u_2^{\pm 1}, \ldots, \pm u_g^{\pm 1}$, where $u_j \in \mathbb{R}$ for $2 \le j \le g$.*

Then for any $j \in \{1, \ldots, g\}$, any $\epsilon_1, \ldots, \epsilon_g = \pm 1$,

$$\epsilon = \begin{cases} 1, & \textit{in case 1;} \\ \pm 1, & \textit{in case 2,} \end{cases}$$

and any conjugate

$$\epsilon u_1^{\epsilon_1} \cdots u_j^{\epsilon_j} \cdots u_g^{\epsilon_g}$$

of $u_1 u_2 \cdots u_g$, then

$$\epsilon u_1^{\epsilon_1} \cdots u_j^{-\epsilon_j} \cdots u_g^{\epsilon_g}$$

is also a conjugate.

Proof. First, note that, in case 2, if an automorphism σ maps an odd number of the u_i to a negative conjugate $-u_j$, then the same is true of σ^{-1}.

Let $\epsilon u_1^{\epsilon_1} \cdots u_j^{\epsilon_j} \cdots u_g^{\epsilon_g}$ be any conjugate of $u_1 u_2 \cdots u_g$, with $\epsilon = 1$ in case 1, and $\epsilon = \pm 1$ in case 2. Let τ be any automorphism that maps $u_j \mapsto u_1$. Then

$$\tau(u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_g^{\epsilon_g}) = \delta u_1^{\epsilon_j} u_2^{\delta_2} \cdots u_g^{\delta_g} \tag{6.27}$$

for some $\delta_2, \ldots, \delta_g = \pm 1$, $\delta = 1$ in case 1, and $\delta = \pm 1$ in case 2. Apply complex conjugation to $\delta u_1^{\epsilon_j} u_2^{\delta_2} \cdots u_g^{\delta_g}$:

$$\delta u_1^{-\epsilon_j} u_2^{\delta_2} \cdots u_g^{\delta_g}. \tag{6.28}$$

Now apply τ^{-1} to (6.28):

$$\epsilon u_1^{\epsilon_1} \cdots u_j^{-\epsilon_j} \cdots u_g^{\epsilon_g}.$$

The result follows. □

Lemma 6.5.4. *Let $u_1 = e^{2i\theta}$ be an algebraic number that lies on the unit circle, with conjugates $\pm u_j^{\pm 1}$, where $u_j \in \mathbb{R}$ for $j \in \{2, \ldots, g\}$. Define*

$$\gamma = (u_1 + u_1^{-1})(u_2 + u_2^{-1}) \cdots (u_g + u_g^{-1}).$$

Then

$-\gamma$ *is a conjugate of* $\gamma \Leftrightarrow -u_1 u_2 \cdots u_g$ *is a conjugate of* $u_1 u_2 \cdots u_g$.

Proof. ($\Rightarrow$) Suppose $-\gamma$ is a conjugate of γ. Then any automorphism ϕ that maps $\gamma \mapsto -\gamma$ must map an odd number of the pairs

$$\{(u_1, u_1^{-1}), \ldots, (u_g, u_g^{-1})\}$$

to a pair of conjugates $(-u_i, -u_i^{-1})$. Thus

$$\phi(u_1 \cdots u_g) = -u_1^{\epsilon_1} \cdots u_g^{\epsilon_g},$$

where $\epsilon_1, \ldots, \epsilon_g = \pm 1$. By considering each $i \in \{1, \ldots, g\}$ in turn, if $\epsilon_i = -1$, we can apply Lemma 6.5.3 to find a conjugate equal to

$$-u_1 u_2 \cdots u_i u_{i+1}^{\epsilon_{i+1}} \cdots u_g^{\epsilon_g}.$$

This process will yield a conjugate $-u_1 u_2 \cdots u_g$ of $u_1 u_2 \cdots u_g$.

($\Leftarrow$) Suppose $-u_1 u_2 \cdots u_g$ is a conjugate of $u_1 u_2 \cdots u_g$. Then any automorphism ϕ that maps

$$u_1 u_2 \cdots u_g \mapsto -u_1 u_2 \cdots u_g$$

must map an odd number of $u_i \mapsto -u_j^{\pm 1}$ for some $j \in \{1, \ldots, g\}$.

Thus

$$\phi\left((u_1 + u_1^{-1})(u_2 + u_2^{-1}) \cdots (u_g + u_g^{-1})\right) \mapsto -(u_1 + u_1^{-1})(u_2 + u_2^{-1}) \cdots (u_g + u_g^{-1}).$$

□

Remark. The result still holds if $u = i$, although here $\gamma = 0$. This case will be treated separately in Theorem 6.5.5.

The following is the main result for algebraic numbers whose conjugate set lies on $S_\times(C, \sqrt{u})$, where $C \in \mathbb{Q}$:

Theorem 6.5.5. *Let $C \in \mathbb{Q}$, and let u be defined in one of the following ways:*

1. *$u = i$,*

2. *$u = u_1 = e^{2i\theta}$ has conjugates u_1^{-1}, and $u_j^{\pm 1} \in \mathbb{R}$ for $2 \leq j \leq g$, or*

3. *$u = u_1 = e^{2i\theta}$ has conjugates $\pm u_j^{\pm 1}$ where $u_j \in \mathbb{R}$ for $2 \leq j \leq g$.*

In case 1, define

$$\alpha = C + \sqrt{ir}$$

where r is totally real.

In case 2, define

$$\alpha = C + r\sqrt{\delta u_1 u_2 \cdots u_g},$$

where r is totally real, and

$$\delta = \begin{cases} 1, & \text{if } u_2 \ldots u_g > 0; \\ -1, & \text{if } u_2 \ldots u_g < 0. \end{cases}$$

In case 3, define

$$\alpha = C + r\sqrt{\delta u_1 u_2 \cdots u_g (u_1 + u_1^{-1})(u_2 + u_2^{-1}) \cdots (u_g + u_g^{-1})},$$

where r is totally real, and

$$\delta = \begin{cases} 1, & \text{if } (u_1 + u_1^{-1}) > 0; \\ -1, & \text{if } (u_1 + u_1^{-1}) < 0. \end{cases}$$

Then α lies with all its conjugates on $S_\times(C, \sqrt{u})$.

Conversely, suppose that α is an algebraic number of degree at least 10 that lies with its conjugates on $S_\times(C, \sqrt{u})$ for some $C \in \mathbb{Q}$. Then either:

1. *$\alpha = C + \sqrt{ir}$, $u = i$ and r is totally real, or*

2. $$\alpha = C + r\sqrt{\delta u_1 u_2 \cdots u_g},$$

   where $u = e^{2i\theta}$ has conjugates u_1^{-1}, and $u_j^{\pm 1} \in \mathbb{R}$ for $2 \leq j \leq g$, r is totally real and

   $$\delta = \begin{cases} 1, & \text{if } u_2 \cdots u_g > 0; \\ -1, & \text{if } u_2 \cdots u_g < 0, \text{ or} \end{cases}$$

3.

$$\alpha = C + r\sqrt{\delta u_1 u_2 \cdots u_g (u_1 + u_1^{-1})(u_2 + u_2^{-1}) \cdots (u_g + u_g^{-1})},$$

where $u = u_1 = e^{2i\theta}$ *has conjugates* $\pm u_j^{\pm 1}$, *where* $u_j \in \mathbb{R}$ *for* $2 \leq j \leq g$, r *is totally real and*

$$\delta = \begin{cases} 1, & \textit{if } (u_1 + u_1^{-1}) > 0; \\ -1, & \textit{if } (u_1 + u_1^{-1}) < 0. \end{cases}$$

Remark. We include the case where $g = 1$, i.e. u has no real conjugates.

Proof. ($\Rightarrow$) 1. Let $C = 0$, $u = i$ and r be totally real. Define

$$\alpha = \sqrt{ir}.$$

If $r \geq 0$, then $\alpha = \sqrt{r}e^{\frac{i\pi}{2}}$ lies on $S_\times(C, \sqrt{i})$, and if $r < 0$, then again

$$\alpha = i\sqrt{-r}e^{\frac{i\pi}{2}} = \sqrt{-r}e^{\frac{-i\pi}{2}}$$

lies on $S_\times(C, \sqrt{i})$. Now apply an automorphism to α:

$$\alpha' = \epsilon\sqrt{\pm ir'},$$

for some $\epsilon = \pm 1$. Here α' lies on $S_\times(C, \sqrt{i})$, so α and its conjugates all lie on $S_\times(C, \sqrt{i})$.

2. Let $C = 0$, let $u_1 = e^{2i\theta}$ have conjugates u_1^{-1} and $u_2^{\pm 1}, \ldots, u_g^{\pm 1} \in \mathbb{R}$, and let r be totally real. Define

$$\alpha = r\sqrt{\delta u_1 u_2 \cdots u_g},$$

where $\delta = 1$ if $u_2 \ldots u_g > 0$ and $\delta = -1$ if $u_2 \ldots u_g < 0$. Then α lies on $S_\times(C, \sqrt{u})$. Apply an automorphism σ to α:

$$\sigma(\alpha) = \pm r'\sqrt{\delta u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_g^{\epsilon_g}},$$

where $\epsilon_1, \ldots, \epsilon_g = \pm 1$ and $r' \in \mathbb{R}$. If $\epsilon_1 = 1$, then as $\delta u_2^{\epsilon_2} \cdots u_g^{\epsilon_g} > 0$, α' lies on L. If $\epsilon_1 = -1$, then by the same reasoning, α' lies on $\overline{L}$. Hence α and all its conjugates lie on $S_\times(C, \sqrt{u})$.

3. Let $C = 0$, let $u_1 = e^{2i\theta}$ have conjugates $\pm u_1^{\pm 1}$ and $\pm u_2^{\pm 1}, \ldots, \pm u_g^{\pm 1} \in \mathbb{R}$, and let r be totally real. Define

$$\alpha = r\sqrt{\delta u_1 u_2 \cdots u_g (u_1 + u_1^{-1})(u_2 + u_2^{-1}) \cdots (u_g + u_g^{-1})},$$

where $\delta = 1$ if $(u_1 + u_1^{-1}) > 0$ and $\delta = -1$ if $(u_1 + u_1^{-1}) < 0$. Then α lies on $S_\times(C, \sqrt{u})$. We apply an automorphism σ to α:

If σ maps an even number of $u_i \mapsto -u_j^{\epsilon_j}$, then σ maps

$$u_1 u_2 \cdots u_g \mapsto u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_g^{\epsilon_g},$$

for some $\epsilon_1, \ldots, \epsilon_g = \pm 1$, and

$$(u_1 + u_1^{-1})(u_2 + u_2^{-1}) \cdots (u_g + u_g^{-1}) \mapsto (u_1 + u_1^{-1})(u_2 + u_2^{-1}) \cdots (u_g + u_g^{-1}).$$

Thus

$$\sigma(\alpha) = \alpha' = \pm r' \sqrt{\delta u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_g^{\epsilon_g} (u_1 + u_1^{-1})(u_2 + u_2^{-1}) \cdots (u_g + u_g^{-1})},$$

where $r' \in \mathbb{R}$. Hence α' lies on $S_\times(C, \sqrt{u})$.

Now suppose σ maps an odd number of $u_i \mapsto -u_j^{\epsilon_j}$. Then σ maps

$$u_1 u_2 \cdots u_g \mapsto -u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_g^{\epsilon_g},$$

for some $\epsilon_1, \ldots, \epsilon_g = \pm 1$, and

$$(u_1 + u_1^{-1})(u_2 + u_2^{-1}) \cdots (u_g + u_g^{-1}) \mapsto -(u_1 + u_1^{-1})(u_2 + u_2^{-1}) \cdots (u_g + u_g^{-1}).$$

Thus

$$\sigma(\alpha) = \alpha' = \pm r' \sqrt{\delta u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_g^{\epsilon_g} (u_1 + u_1^{-1})(u_2 + u_2^{-1}) \cdots (u_g + u_g^{-1})},$$

where $r \in \mathbb{R}$. Hence α' lies on $S_\times(C, \sqrt{u})$.

Therefore, the conjugate set of α all lie on $S_\times(C, \sqrt{u})$.

($\Leftarrow$) Let α be an algebraic number of degree at least ten whose conjugate set lies on a pair of lines $L = C + t\sqrt{u}$ and $\overline{L} = C + \sqrt{u^{-1}}$ ($t \in \mathbb{R}$), where $C \in \mathbb{Q}$ and $u = e^{2i\theta}$ for some $\theta \in (0, \frac{\pi}{2})$. By Lemma 6.5.1, u either has conjugates $u^{\pm 1}, u_2^{\pm 1}, \ldots, u_g^{\pm 1}$, where $u_j \in \mathbb{R}$ for $2 \le j \le g$, or u has conjugates $\pm u^{\pm 1}, \pm u_2^{\pm 1}, \ldots, \pm u_g^{\pm 1}$, where $u_j \in \mathbb{R}$ for $2 \le j \le g$. Suppose α lies on L:

1. Firstly, suppose $u = i$. Define $r \in \mathbb{R}$ by

$$r = \frac{\alpha^2}{i}. \tag{6.29}$$

Apply an automorphism to Equation (6.29): r is mapped to

$$r' = \frac{\alpha'^2}{\epsilon i},$$

where $\epsilon = \pm 1$. If α' lies on L, then $r' > 0$ if $\epsilon = 1$, and $r' < 0$ if $\epsilon = -1$. Similarly, if α' lies on $\overline{L}$, then $r' > 0$ if $\epsilon = -1$, and $r' < 0$ if $\epsilon = 1$. Hence r is totally real.

2. Let u have conjugates u^{-1}, and $u_2^{\pm 1}, \ldots, u_g^{\pm 1}$, where $u_j^{\pm 1} \in \mathbb{R}$ for $j \geq 2$. Let α lie on L, and so define $\tilde{r} \in \mathbb{R}$ by

$$\alpha = \tilde{r}\sqrt{\delta u_1 u_2 \cdots u_g}, \tag{6.30}$$

where $\delta = 1$ if $u_2 \cdots u_g > 0$ and $\delta = -1$ if $u_2 \cdots u_g < 0$. Let τ be an automorphism that maps $u_j \mapsto u_1^{\epsilon_1}$ for some $u_j \in \{u_2, \ldots, u_g\}, \epsilon_1 = \pm 1$. Then

$$\tau(\alpha) = \alpha' = \tilde{r}'\sqrt{\delta u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_g^{\epsilon_g}}, \tag{6.31}$$

where $\epsilon_2, \ldots, \epsilon_g = \pm 1$. Suppose $\tilde{r}' \notin \mathbb{R}$. Then $\tilde{r}' = s' u^{-\epsilon_1}$ for some $s' \in \mathbb{R}$. So

$$s' = \tilde{r}' u^{\epsilon_1}. \tag{6.32}$$

Substituting Equation (6.32) into Equation (6.31), we have

$$\alpha' = s'\sqrt{\delta u_1^{-\epsilon_1} u_2^{\epsilon_2} \cdots u_g^{\epsilon_g}},$$

and hence

$$\alpha = s\sqrt{\delta u_1 u_2 \cdots u_j^{-1} \cdots u_g},$$

where $s = \tau^{-1}(s')$. Repeating this process for all $u^* \in \{u_2, \ldots, u_g\}$, we obtain an $r \in \mathbb{R}$, $\epsilon_2, \ldots, \epsilon_g = \pm 1$ such that

$$\alpha = r\sqrt{\delta u_1 u_2^{\epsilon_2} \cdots u_g^{\epsilon_g}},$$

and for every $j \in \{1, \ldots, g\}$, there exists at least one automorphism that maps $r \mapsto r' \in \mathbb{R}$ and $u_j \mapsto u_1^{\pm 1}$.

Next, we show that for all $j \in \{1, \ldots, g\}$,

$$\alpha_j = r\sqrt{\delta u_1 u_2^{\epsilon_2} \cdots u_j^{-\epsilon_j} \cdots u_g^{\epsilon_g}} \tag{6.33}$$

is a conjugate of α. Let σ be an automorphism that maps $u_j \mapsto u_1^{\pm 1}$ and $r \mapsto r' \in \mathbb{R}$ (we have just shown that such a σ exists). Applying σ to Equation (6.33) gives

$$\sigma(\alpha) = \alpha' = \epsilon r'\sqrt{\delta u_1^{\delta_1} u_2^{\delta_2} \cdots u_g^{\delta_g}}$$

for some $\epsilon = \pm 1$. Applying complex conjugation gives

$$\overline{\alpha'} = \epsilon r'\sqrt{\delta u_1^{-\delta_1} u_2^{\delta_2} \cdots u_g^{\delta_g}}. \tag{6.34}$$

Now apply σ^{-1} to Equation (6.34):

$$\alpha_j = r\sqrt{\delta u_1 u_2^{\epsilon_2} \cdots u_j^{-\epsilon_j} \cdots u_g^{\epsilon_g}},$$

thus proving the claim.

Now suppose there exists an automorphism ϕ such that $\phi(r) = \hat{r} \notin \mathbb{R}$. Then there exists $u_l \in \{u_1, \ldots, u_g\}$ such that $\phi(u_l) = u_1^{\pm 1}$, say u_1. By the result above,

$$\alpha^* = r\sqrt{\delta u_1 \cdots u_l^{-\epsilon_l} \cdots u_g^{\epsilon_g}} \tag{6.35}$$

is a conjugate of

$$\alpha = r\sqrt{\delta u_1 \cdots u_l^{\epsilon_l} \cdots u_g^{\epsilon_g}}. \tag{6.36}$$

Applying ϕ to Equations (6.36) and (6.35) gives

$$\phi(\alpha) = \hat{r}\sqrt{\delta u_1 u_2^{\delta_2} \cdots u_g^{\delta_g}}$$

and

$$\phi(\alpha^*) = \hat{r}\sqrt{\delta u_1^{-1} u_2^{\delta_2} \cdots u_g^{\delta_g}}.$$

Since $\hat{r} \notin \mathbb{R}$, $\hat{r} = u^{\pm 1}s$ for some $s \in \mathbb{R}$. But if $\hat{r} = u_1 s$ then $\phi(\alpha)$ does not lie on $S_\times(C, \sqrt{u})$, and if $\hat{r} = u_1^{-1}s$ then $\phi(\alpha^*)$ does not lie on $S_\times(C, \sqrt{u})$. Therefore r is totally real.

3. The proof is exactly the same as in 2.

Let $u = u_1$ have conjugates $\pm u_1^{-1}$, and $\pm u_2^{\pm 1}, \ldots, \pm u_g^{\pm 1}$, where $\pm u_j^{\pm 1} \in \mathbb{R}$ for $j \geq 2$. Let α lie on L, and so define $\tilde{r} \in \mathbb{R}$ by

$$\alpha = \tilde{r}\sqrt{\delta u_1 u_2 \cdots u_g (u_1 + u_1^{-1}) \cdots (u_g + u_g^{-1})}, \tag{6.37}$$

where $\delta = 1$ if $(u_1 + u_1^{-1}) > 0$ and $\delta = -1$ if $(u_1 + u_1^{-1}) < 0$. Let τ be an automorphism that maps $u_j \mapsto u_1^{\epsilon_1}$ for some $u_j \in \{u_2, \ldots, u_g\}, \epsilon_1 = \pm 1$. Then

$$\tau(\alpha) = \alpha' = \tilde{r}'\sqrt{\delta u_1^{\epsilon_1} u_2^{\epsilon_2} \cdots u_g^{\epsilon_g} (u_1 + u_1^{-1}) \cdots (u_g + u_g^{-1})}, \tag{6.38}$$

where $\epsilon_2, \ldots, \epsilon_g = \pm 1$. Suppose $\tilde{r}' \notin \mathbb{R}$. Then $\tilde{r}' = s' u^{-\epsilon_1}$ for some $s' \in \mathbb{R}$. So

$$s' = \tilde{r}' u^{\epsilon_1}. \tag{6.39}$$

Substituting Equation (6.39) into Equation (6.38), we have

$$\alpha' = s'\sqrt{\delta u_1^{-\epsilon_1} u_2^{\epsilon_2} \cdots u_g^{\epsilon_g} (u_1 + u_1^{-1}) \cdots (u_g + u_g^{-1})},$$

and hence

$$\alpha = s\sqrt{\delta u_1 u_2 \cdots u_j^{-1} \cdots u_g (u_1 + u_1^{-1}) \cdots (u_g + u_g^{-1})},$$

where $s = \tau^{-1}(s')$. Repeating this process for all $u^* \in \{u_2, \ldots, u_g\}$, we obtain an $r \in \mathbb{R}$, $\epsilon_2, \ldots, \epsilon_g = \pm 1$ such that

$$\alpha = r\sqrt{\delta u_1 u_2^{\epsilon_2} \cdots u_g^{\epsilon_g}(u_1 + u_1^{-1}) \cdots (u_g + u_g^{-1})},$$

and for every $j \in \{1, \ldots, g\}$, there exists at least one automorphism that maps $r \mapsto r' \in \mathbb{R}$ and $u_j \mapsto u^{\pm 1}$.

Next, we show that for all $j \in \{1, \ldots, g\}$,

$$\alpha_j = r\sqrt{\delta u_1 u_2^{\epsilon_2} \cdots u_j^{-\epsilon_j} \cdots u_g^{\epsilon_g}(u_1 + u_1^{-1}) \cdots (u_g + u_g^{-1})} \tag{6.40}$$

is a conjugate of α. Let σ be an automorphism that maps $u_j \mapsto u_1^{\pm 1}$ and $r \mapsto r' \in \mathbb{R}$ (we have just shown that such a σ exists). Applying σ to Equation (6.40) gives

$$\sigma(\alpha) = \alpha' = \epsilon r'\sqrt{\delta u_1^{\delta_1} u_2^{\delta_2} \cdots u_g^{\delta_g}(u_1 + u_1^{-1}) \cdots (u_g + u_g^{-1})},$$

where $\epsilon = \pm 1$. Applying complex conjugation gives

$$\overline{\alpha'} = \epsilon r'\sqrt{\delta u_1^{-\delta_1} u_2^{\delta_2} \cdots u_g^{\delta_g}(u_1 + u_1^{-1}) \cdots (u_g + u_g^{-1})}. \tag{6.41}$$

Now apply σ^{-1} to Equation (6.41):

$$\alpha_j = r\sqrt{\delta u_1 u_2^{\epsilon_2} \cdots u_j^{-\epsilon_j} \cdots u_g^{\epsilon_g}(u_1 + u_1^{-1}) \cdots (u_g + u_g^{-1})},$$

thus proving the claim.

Now suppose there exists an automorphism ϕ such that $\phi(r) = \hat{r} \notin \mathbb{R}$. Then there exists $u_l \in \{u_1, \ldots, u_g\}$ such that $\phi(u_l) = u_1^{\pm 1}$, say u_1. By the result above,

$$\alpha^* = r\sqrt{\delta u_1 \cdots u_l^{-\epsilon_l} \cdots u_g^{\epsilon_g}(u_1 + u_1^{-1}) \cdots (u_g + u_g^{-1})} \tag{6.42}$$

is a conjugate of

$$\alpha = r\sqrt{\delta u_1 \cdots u_l^{\epsilon_l} \cdots u_g^{\epsilon_g}(u_1 + u_1^{-1}) \cdots (u_g + u_g^{-1})}. \tag{6.43}$$

Applying ϕ to Equations (6.43) and (6.42) gives

$$\phi(\alpha) = \hat{r}\sqrt{\delta u_1 u_2^{\delta_2} \cdots u_g^{\delta_g}(u_1 + u_1^{-1}) \cdots (u_g + u_g^{-1})}$$

and

$$\phi(\alpha^*) = \hat{r}\sqrt{\delta u_1^{-1} u_2^{\delta_2} \cdots u_g^{\delta_g}(u_1 + u_1^{-1}) \cdots (u_g + u_g^{-1})}.$$

Since $\hat{r} \notin \mathbb{R}$, $\hat{r} = u_1^{\pm 1}s$ for some $s \in \mathbb{R}$. But if $\hat{r} = u_1 s$ then $\phi(\alpha)$ does not lie on $S_\times(C, \sqrt{u})$, and if $\hat{r} = u_1^{-1}s$ then $\phi(\alpha^*)$ does not lie on $S_\times(C, \sqrt{u})$. Therefore r is totally real. □

Example 6.5.6. Let $C = 0$, $u = i$, $r = \sqrt{2+\sqrt{7}}$ and

$$\alpha = \sqrt{i(2+\sqrt{7})}.$$

Then α has minimal polynomial $X^8 + 22X^4 + 9$, and lies with its conjugates on $S_\times(0, i)$. The algebraic number $\alpha - 2$ has minimal polynomial

$$P_\alpha : X^8 - 16X^7 + 112X^6 - 448X^5 + 1142X^4 - 1968X^3 + 2320X^2 - 1728X + 617,$$

and lies with all its conjugates on $S_\times(2, i)$.

We use a standard method usually used for producing Salem numbers to construct a u of modulus 1 whose conjugates are all real except for $\pm u^{\pm 1}$.

Begin with a totally real number β, with conjugates $\beta_1 = \beta, \beta_2, \ldots, \beta_g$, such that $\beta_1 \in [-2, 2]$ and $\beta_i \notin [-2, 2]$ for $i = 2, \ldots, g$.

Let $\beta = \tau + \frac{1}{\tau}$. Then

$$\tau^2 - \beta\tau + 1 = 0.$$

Solving this for τ gives

$$\tau = \frac{\beta \pm \sqrt{\beta^2 - 4}}{2}.$$

Set

$$\tau_1 = \frac{\beta_1 + \sqrt{\beta_1^2 - 4}}{2}, \tau_1^{-1} = \frac{\beta_1 - \sqrt{\beta_1^2 - 4}}{2},$$
$$\tau_2 = \frac{\beta_2 + \sqrt{\beta_2^2 - 4}}{2}, \cdots, \tau_g^{-1} = \frac{\beta_g - \sqrt{\beta_g^2 - 4}}{2}.$$

Note that τ_1, τ_1^{-1} are non-real and of modulus 1, with phases θ and $-\theta$ respectively, whilst $\tau_2, \tau_2^{-1}, \ldots, \tau_g, \tau_g^{-1} \in \mathbb{R}$. Taking square roots of the conjugates of τ gives the conjugate set of an algebraic number u, whose conjugates are $\pm u_j^{\pm 1}$, where $u_1 = u = e^{2i\theta}$, and $u_j \in \mathbb{R}$ for $2 \leq j \leq g$.

Example 6.5.7. Let $\beta = 3 + \sqrt{5} - \sqrt{17}$. The conjugates of β are:

$$\begin{aligned} \beta = \beta_1 &= 3 + \sqrt{5} - \sqrt{17} \\ \beta_2 &= 3 - \sqrt{5} - \sqrt{17}, \\ \beta_3 &= 3 - \sqrt{5} + \sqrt{17}, \\ \beta_4 &= 3 + \sqrt{5} + \sqrt{17}. \end{aligned}$$

Here $\beta_1 \in [-2, 2]$, $\beta_2 < -2$ and $\beta_3, \beta_4 > 2$. Then

$$\begin{aligned}
u = u_1 &= \frac{\beta_1 + \sqrt{\beta_1^2 - 4}}{2}, \\
u_1^{-1} &= \frac{\beta_1 - \sqrt{\beta_1^2 - 4}}{2}, \\
u_2 &= \frac{\beta_2 + \sqrt{\beta_2^2 - 4}}{2}, \\
u_2^{-1} &= \frac{\beta_2 - \sqrt{\beta_2^2 - 4}}{2}, \\
u_3 &= \frac{\beta_3 + \sqrt{\beta_3^2 - 4}}{2}, \\
u_3^{-1} &= \frac{\beta_3 - \sqrt{\beta_3^2 - 4}}{2}, \\
u_4 &= \frac{\beta_4 + \sqrt{\beta_4^2 - 4}}{2}, \\
u_4^{-1} &= \frac{\beta_4 - \sqrt{\beta_4^2 - 4}}{2},
\end{aligned}$$

Let

$$\alpha = \sqrt{u_1 u_2 u_3 u_4 (u_1 + u_1^{-1})(u_2 + u_2^{-1})(u_3 + u_3^{-1})(u_4 + u_4^{-1})}.$$

Then the conjugates of α are of the form

$$\pm\sqrt{u_1^{\epsilon_1} u_2^{\epsilon_2} u_3^{\epsilon_3} u_4^{\epsilon_4} (u_1 + u_1^{-1})(u_2 + u_2^{-1})(u_3 + u_3^{-1})(u_4 + u_4^{-1})},$$

and the minimal polynomial of α is

$$\begin{aligned}
&Z^{32} + 10201Z^{30} + 10661656Z^{28} + 195321372677Z^{26} + 302936164793957Z^{24} \\
&150786814352570848Z^{22} + 57907565325437379146Z^{20} \\
&11106752943956654777 69Z^{18} + 1634135935836023470039312Z^{16} \\
&113299986781301835872156 9Z^{14} + 6025884468698709174321797546Z^{12} \\
&1600632418801860348804822796 48Z^{10} + 328036457424389457609089991955 7Z^{8} \\
&215756309824701707971126386996 77Z^{6} + 12018902373612578894758111360885 6Z^{4} \\
&117257864492369852051862561201601Z^{2} \\
&+ 117257864492369852051862561201601.
\end{aligned}$$

Chapter 7

The Conjugate Dimension

7.1 Introduction

The following chapter is based on a paper,

(arXiv http://arxiv.org/abs/math.NT/0308069),

written in collaboration with Arturas Dubickas, Noam Elkies, Bjorn Poonen and Chris Smyth [1]. We study the dimension of a vector space over a field K (usually $\mathbb{Q}$) spanned by the conjugates of an algebraic number α.

Definition 7.1.1. Let α be an algebraic number. The **conjugate dimension** of α over a field K, denoted $\dim_K(\alpha)$, is defined to be the dimension n of the K-vector space spanned by the conjugate set of α.

Example 7.1.2. Let α have minimal polynomial $P_\alpha : X^6 - 2$ over $\mathbb{Q}$. What is the conjugate dimension $\dim_{\mathbb{Q}}(\alpha)$ of α?

The conjugate set of α is

$$\alpha = 2^{\frac{1}{6}} \qquad \alpha_2 = \omega 2^{\frac{1}{6}} \qquad \alpha_3 = \omega^2 2^{\frac{1}{6}}$$
$$\alpha_4 = -2^{\frac{1}{6}} \qquad \alpha_5 = -\omega 2^{\frac{1}{6}} \qquad \alpha_6 = -\omega^2 2^{\frac{1}{6}}$$

where $\omega^2 + \omega + 1 = 0$. The conjugates can be expressed as rational linear combinations of α and α_2 as follows:

$$\alpha_3 = -\alpha - \alpha_2 \qquad \alpha_4 = -\alpha \qquad \alpha_5 = -\alpha_2 \qquad \alpha_6 = \alpha_1 + \alpha_2.$$

Since α and α_2 are linearly independent over $\mathbb{Q}$, $\{\alpha, \alpha_2\}$ is a basis for a vector space V over $\mathbb{Q}$ spanned by the conjugate set of α. Hence $\dim_{\mathbb{Q}}(\alpha) = 2$.

Notation. Unless otherwise stated, we set $n = \dim_K(\alpha)$ and $d = \deg_K(\alpha)$.

We fix n and K, and consider what values $\deg_K(\alpha)$ can take. Note that $\deg_K(\alpha)$ is also a measure of dimension, namely the dimension of the vector space over K spanned by the powers of α. In particular we ask what the maximal and minimal values of $\deg_{\mathbb{Q}}(\alpha)$ are.

In the main theorem, we take $K = \mathbb{Q}$, for all n give upper and lower bounds for $\deg_{\mathbb{Q}}(\alpha)$, and prove that these bounds are attained. We extend the results for other base fields, in particular for finite fields and cyclotomic extensions of $\mathbb{Q}$.

7.2 Previous Work And The Main Theorem

Let $K = \mathbb{Q}$, and let L be a splitting field for α over K. There are two previous results to note. If $\mathrm{Tr}(\alpha) \neq 0$ and $\mathrm{Gal}(L/\mathbb{Q}) = S_d$, then $n = d$, by C.J.Smyth [22], Lemma 1:

Lemma 7.2.1. *Let α be an algebraic number with conjugates $\alpha = \alpha_1, \ldots, \alpha_d$, and galois group $\mathrm{Gal}(L/\mathbb{Q}) = S_d$. Then*

$$\sum_{i=1}^{d} \alpha_i v_i \neq 0$$

for any rationals $v_1, \ldots, v_d$ not all equal.

It has also been shown by A.Dubickas [3], Corollary 1 that n can be as small as $\lfloor \log_2 d \rfloor$:

Lemma 7.2.2. *Let K be a number field, and for primes $p_1, \ldots, p_n$, let $L = K(\sqrt{p_1}, \ldots, \sqrt{p_n})$, where*

$$\sqrt{p_1} \notin K, \sqrt{p_2} \notin K(\sqrt{p_1}), \ldots, \sqrt{p_n} \notin K(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}).$$

Then $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/2\mathbb{Z})^n$ and there exists $\alpha \in L$ with $\deg_K(\alpha) = 2^n$ and $\dim_K(\alpha) = \lfloor \log_2 d \rfloor$.

Main Theorem. *Let α be an algebraic number such that $\dim_{\mathbb{Q}}(\alpha) = n$. Then*

1. *We have*

$$\dim_{\mathbb{Q}}(\alpha) \leq \deg_{\mathbb{Q}}(\alpha) \leq d_{\max}(n),$$

where $d_{\max}(n)$ is the order of a maximal subgroup of $\mathrm{GL}_n(\mathbb{Q})$ (unique up to isomorphism) given by Table 7.1 below.

2. *Furthermore, for all integers $n \geq 1$, there exist algebraic numbers α, β with $\dim_{\mathbb{Q}}(\alpha) = n = \dim_{\mathbb{Q}}(\beta)$ such that $\deg_{\mathbb{Q}}(\alpha) = d_{max}(n)$ and $\deg_{\mathbb{Q}}(\beta) = n$.*

The groups $W(\cdot)$ are matrix representations of the Weyl groups (see Section 1.5).

n	$d_{\max}(n)/(2^n n!)$	Maximal order subgroup G	$d_{\max}(n) = \|G\|$
2	3/2	$W(G_2)$	12
4	3	$W(F_4)$	1152
6	9/4	$\langle W(E_6), -I \rangle$	103680
7	9/2	$W(E_7)$	2903040
8	135/2	$W(E_8)$	696729600
9	15/2	$W(E_8) \times W(A_1)$	1393459200
10	9/4	$W(E_8) \times W(G_2)$	8360755200
all other n	1	$W(B_n) = W(C_n) = (\mathbb{Z}/2Z)^n \rtimes S_n$	$2^n n!$

Table 7.1: Maximal order subgroups of $\mathrm{GL}_n(\mathbb{Q})$

7.3 Results used in Proof of the Main Theorem

7.3.1 Finite Subgroups Of $\mathrm{GL}_n(\mathbb{Q})$

Let K be a field. Let α be algebraic over K, with splitting field L. Denote by $\{\alpha_1 = \alpha, \alpha_2, \dots, \alpha_d\}$ the conjugate set of α over K. We give the relationship between $\mathrm{Gal}(L/K)$ and a finite subgroup of $\mathrm{GL}_n(K)$.

Lemma 7.3.1. *Let α be a number, algebraic over a field K, such that $\dim_K(\alpha) = n$ and $\deg_K(\alpha) = d$, and let V be the vector space spanned by the conjugates of α over K. Let $G = \mathrm{Gal}(L/K)$. There is a faithful n-dimensional representation $\rho : G \hookrightarrow \mathrm{GL}_n(K)$ of G.*

Proof. G acts on L by linear substitutions. This action restricts to an action on V, since $\{\alpha_1, \dots, \alpha_d\}$ is G-stable. Let $g \in G$ act on V. If this action is trivial, then all of the α_i are fixed, so g is the identity element. Thus V is a faithful K-representation of G. Clearly $\dim_K V = n$. □

Example 7.3.2. The galois group $\mathrm{Gal}(\mathbb{Q}(\alpha, \alpha_2)/\mathbb{Q})$ with α, α_2 defined as in Example 7.1.2 has a representation

$$\rho : \mathrm{Gal}(\mathbb{Q}(\alpha, \alpha_2)/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{Q}),$$

where $\mathrm{Gal}(\mathbb{Q}(\alpha, \alpha_2)/\mathbb{Q})$ injects into the subgroup of $\mathrm{GL}_2(\mathbb{Q})$ generated by the matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \text{and} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

of order 12.

The maximal finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$ in Table 7.1 are taken from Feit [8], who states the results from some unpublished work by Weisfeiler:

Theorem 7.3.3. *For each $n \in \mathbb{N}$, any maximal finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$ is isomorphic to the one given in Table 7.1.*

7.3.2 More On Representations

Lemma 7.3.4. *Let K be an infinite field, and let V be a variety given by non trivial polynomial equations (with coefficients in K)*

$$p_j(x_1, \ldots, x_n) = 0 \qquad (j = 1, \ldots, N).$$

There exists a choice $(a_1, \ldots, a_n) \in K^n$ that lies outside V.

Proof. Use induction on n. Let $\mathrm{P}(n)$ denote the statement, stronger than that required for the lemma, that there exist $(a_1, \ldots, a_n) \in K^n$ such that $p_j(a_1, \ldots, a_n) \neq 0$ for all $j = 1, \ldots, N$. Consider $\mathrm{P}(1)$:

Let $p_j(x_1) = b_n^{(j)} x_1^n + \cdots + b_0^{(j)}$ be such that $b_n^{(j)} \neq 0$. Then take

$$\sum_{i=1}^{n} \left| \frac{b_i^{(j)}}{b_n^{(j)}} \right| = c_j$$

say, noting that $p_j(a_1) \neq 0$ for $|a_1| > c_j$. Choosing an element of $a \in K$ such that $|a| > \max_j c_j$ will satisfy the hypothesis.

Now assume $\mathrm{P}(n)$ is true for some $n \in \mathbb{N}$. Consider $\mathrm{P}(n+1)$: For all j, write $p_j(x_1, \ldots, x_{n+1})$ as

$$\sum q_{ij}(x_1, \ldots, x_n) x_{n+1}^i,$$

and by the inductive hypothesis, choose $(a_1, \ldots, a_n) \in K^n$ such that $q_{ij}(a_1, \ldots, a_n) \neq 0$ for all i, j. Again choose a_{n+1} such that $|a_{n+1}| > \max_j c_j$. The result follows by induction. □

Lemma 7.3.5. *Let K be an infinite field, and let $V_1, \ldots, V_r$ be r varieties each given by non trivial polynomial equations (with coefficients in K)*

$$p_{(l,j)}(x_1, \ldots, x_n) = 0 \qquad (j = 1, \ldots, N_r, l = 1, \ldots, r).$$

There exists a choice $(a_1, \ldots, a_n) \in K^n$ that lies outside all of the V_i.

Proof. We define each variety by the same number of equations, N say, by repeating some equations if necessary. The union variety is contained in the variety given by

$$W = \{\prod_{l=1}^{r} p_{(l,j)} = 0 \quad (j = 1, \ldots, N)\}.$$

By Lemma 7.3.4, we can choose a point outside W, and so certainly outside the union variety. □

Lemma 7.3.6. *Let K be a field where $\mathrm{Char}(K) = 0$, and let G be a finite group. Let M be a KG-submodule of the regular representation KG. Suppose G acts faithfully on M. Then $M = (KG)\alpha$ for some $\alpha \in M$ that has trivial stabilizer.*

Proof. By Maschke's Theorem 1.6.10 and Lemma 1.6.11,

$$KG = \bigoplus_{i=1}^{r} U_i^{\oplus m_i},$$

and so $M = \bigoplus_i U_i^{\oplus l_i}$, where for some $l_i \leq m_i$ for all $i \in \{1, \ldots, r\}$. We aim to show that the KG-module M can be generated by one element.

An element $\alpha \in M$ fails to generate M as a KG-module if and only if $\{g\alpha : g \in G\}$ fails to span M. Let M be n-dimensional, $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for M over K, and let

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n,$$

where $a_i \in K$ for $i = 1, \ldots, n$. Then for all $g \in G$, g acts on α as follows:

$$g\alpha = \alpha_g = a_{g(1)}\alpha_1 + \cdots + a_{g(n)}\alpha_n. \tag{7.1}$$

Suppose that the multiset $\{g\alpha : g \in G\}$ fails to span M. For each of the $\binom{|G|}{n}$ choices of n of the Equations (7.1), the $n \times n$ matrix whose rows are the row vectors of the coordinates of distinct α_g is singular.

These matrices are all dependent on the choice of $(a_1, \ldots, a_n)$, so their determinants can be expressed as $\binom{|G|}{n}= r$ equations

$$\begin{aligned} p_1(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ p_r(x_1, \ldots, x_n) &= 0, \end{aligned} \tag{7.2}$$

such that $(a_1, \ldots, a_n) \in K^n$ satisfies all of the Equations (7.2). This gives us a variety $W(p_1, \ldots, p_r)$.

Also, for every $g \neq e$ in G, the set

$$M^g := \{\beta \in M : g\beta = \beta\}$$

is a proper subspace of M, since M is faithful.

Let $\beta = b_1\alpha_1 + \cdots + b_n\alpha_n$. Then

$$\begin{aligned} g\beta &= b_1 g(\alpha_1) + \cdots + b_n g(\alpha_n) && (7.3) \\ &= b_{g(1)}\alpha_1 + \cdots + b_{g(n)}\alpha_n, && (7.4) \end{aligned}$$

and so M^g is a variety.

By Lemma 7.3.5, we can choose α outside of $W(p_1, \dots, p_r)$, and outside M^g for each $g \neq e$. This gives an $\alpha \in M$ that has trivial stabilizer and generates M. □

The following is a partial converse of Lemma 7.3.1, i.e. starting with a finite group G, and a faithful n-dimensional representation of G over a field K, given certain conditions there exists an α, algebraic over K, satisfying $\dim_K(\alpha) = n$ and $\deg_K(\alpha) = |G|$:

Lemma 7.3.7. *Let K be a field with $\mathrm{Char}(K) = 0$, and let G be a finite group. Suppose that L is a galois extension of K, with $\mathrm{Gal}(L/K) = G$, and that there exists a faithful n-dimensional subrepresentation M of the regular representation of G over K. Then there exists $\alpha \in L$ such that $\dim_K(\alpha) = n$ and $\deg_K(\alpha) = |G|$.*

Proof. Let $\sigma_1, \dots, \sigma_{|G|}$ be the elements of $\mathrm{Gal}(L/K)$. By the Normal Basis Theorem 1.4.13, there exists $l \in L$ such that

$$\{\sigma_1(l), \dots, \sigma_{|G|}(l)\}$$

is a basis for L over K. G acts on this set by permuting its elements, so the extension L/K, viewed as a representation of G, is isomorphic to the regular representation. Thus M is a subrepresentation of L. From Lemma 7.3.6, we have an element $\alpha \in M$ such that $\dim_K(\alpha) = n$ and $\deg_K(\alpha) = |G|$. □

Remark. If $|G| > d_{\max}(n)$, then by the main theorem, there is no suitable faithful n-dimensional subrepresentation of the regular representation of G.

Lemma 7.3.8. *Let ϕ_k be a faithful n-dimensional representation of G over $\mathbb{Q}$, where G is one of the groups given in Table 7.1. Then ϕ_k is a subrepresentation of the regular representation of dimension $|G|$.*

Proof. By Theorem 1.6.10 and Lemma 1.6.11, we can write the regular representation as

$$KG := \bigoplus_{i=1}^{r} U_i^{\oplus m_i},$$

where the U_i are irreducible and not isomorphic to each other, and $m_i = \dim(U_i)$ for all $i \in \{1, \dots, r\}$. Suppose that ϕ_k is a representation of G but not a subrepresentation of the regular representation. Then by Lemma 1.6.11, it must contain more copies of some irreducible representation than are in the regular representation. Without loss of generality, let

$$\phi_k := \bigoplus_{i=1}^{r} U_i^{\oplus k_i},$$

where $k_i \geq 0$ for all i, and in particular, $k_1 > m_1 \geq 1$. So an element of $g \in G$ is mapped by ϕ_k to

$$(u_1, \ldots, u_1, u_2, \ldots, u_2, \ldots),$$

where $u_i \in \mathrm{GL}(U_i)$, and there are k_i copies of each u_i. Removing a single copy of U_1 produces a subrepresentation $\phi_{k'}$ on a lower dimensional subspace. We show that such a subrepresentation $\phi_{k'}$ is faithful.

Let $g \in \mathrm{Ker}(\phi_{k'})$. Then

$$\phi_{k'}(g) = (I_{m_1}, \ldots, I_{m_1}, I_{m_2}, \ldots, I_{m_2}, \ldots),$$

with $k_1 - 1 \geq 1$ copies of I_{m_1} and k_i copies of I_{m_i} for $i \geq 2$. Thus $\phi_{k'}$ maps $g_i \mapsto I_{m_i}$ for each i, so

$$\phi_k(g) = (I_{m_1}, \ldots, I_{m_1}, I_{m_2}, \ldots, I_{m_2}, \ldots),$$

with k_i copies of $I_{m_i} \in \mathrm{GL}(U_i)$ for each i. Since ϕ_k is faithful, $g = 1_G$. Thus

$$g \in \mathrm{Ker}(\phi_{k'}) \Rightarrow g = 1_G,$$

so $\phi_{k'}$ is a faithful representation on a lower dimensional subspace. Thus G has a faithful representation of degree less than n. This contradicts the fact that $d_{\max}(n)$, the order of the maximal order subgroup of $\mathrm{GL}_n(\mathbb{Q})$, is a strictly increasing function. Therefore ϕ_k is a subrepresentation of the regular representation KG. □

7.3.3 Fields Of Invariants

The following result was discovered by Chevalley [2], and can also be found in Humphreys [11]:

Theorem 7.3.9 (Chevalley). *Let G be a finite reflection group, and let R be the subalgebra of $\mathbb{R}[x_1, \ldots, x_n]$ consisting of G-invariant polynomials. Then R is generated as an R-algebra by n homogeneous, algebraically independent polynomials of distinct degree, i.e.*

$$\mathbb{R}[x_1, \ldots, x_n]^G = \mathbb{R}[f_1, \ldots, f_n].$$

Note that all groups given in Table 7.1 are finite reflection groups, apart from $\langle W(E_6), -I \rangle$, which has a finite reflection group as a subgroup of index 2. The following proposition, from Humphreys [11], combined with Lemma 7.3.15, shows that $-I \notin W(E_6)$:

Proposition 7.3.10. *The scalar transformation $-I \in \mathrm{GL}_n(\mathbb{Q})$ lies in G if and only if all the degrees of the polynomial generators of G have even degrees.*

Definition 7.3.11. Let L/K be an extension, and let $\alpha_1, \ldots, \alpha_n$ be a set of algebraically independent elements over K that generate L. Then the α_i form a **transcendence basis** and n is the **transcendence degree** of L/K.

The following definition comes from Garling [10]:

Definition 7.3.12. Suppose L/K is a finitely generated extension with transcendence degree n. If we can find a transcendence basis $f_1, \ldots, f_n$ for L over K such that $L = K(f_1, \ldots, f_n)$, then we say that L is **purely transcendental** over K.

Lemma 7.3.13. *The G-invariant subfield of $\mathbb{Q}(x_1, \ldots, x_n)$ is $\mathbb{Q}(x_1, \ldots, x_n)^G$.*

Proof. Let $f = \frac{P}{Q} \in \mathbb{Q}(x_1, \ldots, x_n)^G$. We want to show that $P, Q \in \mathbb{Q}[x_1, \ldots, x_n]^G$, the G-invariant subring of $\mathbb{Q}[x_1, \ldots, x_n]$. Let $g \in G$ have order N. Now

$$f = gf = \frac{gP}{gQ} = \frac{P}{Q}.$$

So $gP = RP$ and $gQ = RQ$ for some $R \in \mathbb{Q}[x_1, \ldots, x_n]$. Now g acts on P by linear substitutions, so

$$\deg(gP) \leq \deg(P),$$

and $R \in \mathbb{Q}$. Now

$$g^N P = R^N P = P.$$

Therefore $R^N = 1$, hence $R = \pm 1$. If $R = 1$, then $P, Q \in \mathbb{Q}[x_1, \ldots, x_n]^G$, and if $R = -1$, then $\frac{P}{Q} = \frac{PQ}{Q^2}$, and $PQ, Q^2 \in \mathbb{Q}[x_1, \ldots, x_n]^G$ as required. □

Proposition 7.3.14. *Let G be one of the groups in Table 7.1, considered as a finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$. Then the invariant subfield $\mathbb{Q}(x_1, \ldots, x_n)^G$ is purely transcendental over $\mathbb{Q}$.*

Proof. By Theorem 7.3.9, if G is a finite reflection group, then

$$\mathbb{Q}[x_1, \ldots, x_n]^G = \mathbb{Q}[f_1, \ldots, f_n],$$

where the f_i are homogeneous polynomials of distinct degrees. By Lemma 7.3.13,

$$\mathbb{Q}(x_1, \ldots, x_n)^G = \mathbb{Q}(f_1, \ldots, f_n).$$

For the case $G = \langle W(E_6), -I \rangle$,

$$\mathbb{Q}(x_1, \ldots, x_6)^{W(E_6)} = \mathbb{Q}(I_2, I_5, I_6, I_8, I_9, I_{12}),$$

where I_k is a homogeneous polynomial of degree k in $x_1, \ldots, x_6$.

Thc element $-I \in G$ acts on $\mathbb{Q}(x_1, \ldots, x_6)^{W(E_6)}$ by mapping

$$I_j \mapsto (-1)^j I_j.$$

The ring $\mathbb{Q}[x_1, \ldots, x_6]^G$ of polynomial invariants of G, namely

$$\mathbb{Q}[I_2, I_6, I_8, I_{12}, I_5^2, I_5 I_9, I_9^2],$$

is not generated by 6 algebraically independent polynomials. However, the invariant subfield $\mathbb{Q}(x_1, \ldots, x_6)^G$ is, since in this subfield, the identity

$$(I_5 I_9)^2 = I_5^2 I_9^2$$

can be written as

$$I_9^2 = (I_5 I_9)^2 / I_5^2,$$

giving

$$\mathbb{Q}(x_1, \ldots, x_6)^G = \mathbb{Q}(I_2, I_6, I_8, I_{12}, I_5^2, I_5 I_9).$$

□

The generators of the rings of invariants of the groups given in Table 7.1 are known. See for example Mehta [16].

Lemma 7.3.15. *Let G be one of the groups described in Table 7.1, and let G act on $x_1, \ldots, x_n$ by linear transformations. The generators of the G-invariant subfield of $\mathbb{Q}(x_1, \ldots, x_n)$ are homogeneous polynomials in $x_1, \ldots, x_n$ with degrees given given in Table 7.2 below:*

n	Max. order subgp G	Degs of generators of G-invariant subfield
2	$W(G_2)$	$2, 6$
4	$W(F_4)$	$2, 6, 8, 12$
6	$\langle W(E_6), -I \rangle$	$2, 6, 8, 10, 12, 14$
7	$W(E_7)$	$2, 6, 8, 10, 12, 14, 18$
8	$W(E_8)$	$2, 8, 12, 14, 18, 20, 24, 30$
9	$W(E_8) \times W(A_1)$	$2, 8, 12, 14, 18, 20, 24, 30, 2$
10	$W(E_8) \times W(G_2)$	$2, 8, 12, 14, 18, 20, 24, 30, 2, 6$
all other n	$W(B_n) = W(C_n)$	$2, 4, \ldots, 2n$

Table 7.2: Invariant subfields of maximal subgroups of $\mathrm{GL}_n(\mathbb{Q})$

7.3.4 Hilbert Irreducibility

The following section is taken from the relevant parts of Völklein [26]:

Proposition 7.3.16. *The following are equivalent conditions on a field K:*

1. *For every irreducible polynomial $f(x, y)$ in two variables over K, of degree at least one in y, there are infinitely many $b \in K$ such that the polynomial $f(b, y)$ is irreducible (in y).*

2. *Let L/K be a finite extension, and let $h_1(x, y), \ldots, h_m(x, y) \in L[x][y]$ be polynomials that are irreducible in y over $L(x)$. There exist infinitely many $b \in K$ such that the polynomials $h_1(b, y), \ldots, h_m(b, y)$ are irreducible in y.*

3. *For any $p_1(x, y), \ldots, p_t(x, y) \in K[x][y]$ that are irreducible and of degree 1 when viewed as polynomials in y with coefficients in $K(x)$, there exist infinitely many $b \in K$ such that none of the polynomials $p_1(b, y), \ldots, p_t(b, y) \in K[y]$ have a root in K.*

Definition 7.3.17. A field K is **hilbertian** if it satisfies (one of) the conditions given in Proposition 7.3.16.

Proposition 7.3.18. *The field $\mathbb{Q}$ and any finite extension of $\mathbb{Q}$ are hilbertian.*

Lemma 7.3.19 on Hilbert Irreducibility states that given a purely transcendental extension $\mathbb{Q}(x_1, \ldots, x_n)/\mathbb{Q}(x_1, \ldots, x_n)^G$ with galois group isomorphic to G, there exists $b_1, \ldots, b_n \in \mathbb{Q}$ such that on setting the generators of the invariant subfield $f_i(x_1, \ldots, x_n)$ equal to b_i for $1 \leq i \leq n$, we obtain a galois extension $L/\mathbb{Q}$, where $\mathrm{Gal}(L/\mathbb{Q}) \cong G$.

Lemma 7.3.19 (Hilbert's Irreducibility Theorem). *Let $x_1, \ldots, x_n$ be indeterminates, $K = \mathbb{Q}(x_1, \ldots, x_n)$, and let L be a galois extension of K with galois group $G = \mathrm{Gal}(L/K)$. Suppose that $L = K(\theta)$, where θ is a root of the polynomial (irreducible in y) $p(x_1, \ldots, x_n, y) \in K[y]$ of degree d. Then there exist $x_1^*, \ldots, x_n^* \in \mathbb{Q}$ such that:*

1. *the specialised polynomial*

$$p^*(y) := p(x_1^*, \ldots, x_n^*, y) \in \mathbb{Q}[y]$$

is irreducible over $\mathbb{Q}$.

2. *The map*

$$\mathrm{Gal}(K(\theta)/K) \to \mathrm{Gal}(\mathbb{Q}(\theta^*)/\mathbb{Q})$$
$$\sigma \mapsto \sigma^*,$$

defined by $x_i \mapsto x_i^*$ for $i \in 1, \ldots, n$, is an isomorphism.

Proof. (of (2); (1) follows immediately from Lemma 1.10, [26]).

The proof is adapted from Lemmas 1.5 and 1.7 from [26]. Let A be a finite subset of $K(\theta)$ containing θ and invariant under G. Note that every $a \in A$ can be written in the form

$$a = \sum_{i=0}^{d-1} b_i \theta^i$$

with $b_i \in K$.

Let

$$\omega : K \to \mathbb{Q}$$

be the evaluation homomorphism defined by substituting $x_1^*, \ldots, x_n^* \in \mathbb{Q}$ for $x_1, \ldots, x_n$ respectively, with $x_1^*, \ldots, x_n^*$ chosen such that $b_i(x_1^*, \ldots, x_n^*)$ is well defined for $i = 1, \ldots, n$ and

$$p^*(y) = p(x_1^*, \ldots, x_n^*, y)$$

is irreducible over $\mathbb{Q}$ (such a choice is possible by Lemma 1.10, [26]).

Let $h \in K[y]$ have θ as a root. We show that p is a factor of h:

By polynomial division,

$$h = pq + r \tag{7.5}$$

for some $q, r \in K[y]$, with $\deg r < \deg p$. Now $h(\theta) = p(\theta)q(\theta) + r(\theta) = 0$, so $r(\theta) = 0$ and, since p is the minimal polynomial of θ over K, $r \equiv 0$. Hence h has p as a factor, and so belongs to the ideal of $K[y]$ generated by p, namely the kernel of the natural map

$$\rho : K[y] \to K[\theta], h(y) \mapsto h(\theta).$$

Factoring out the kernel of ρ, we have an isomorphism

$$\phi : K[y]/(p) \to K[\theta].$$

Let θ^* be a root of $p^*(y)$. Extend ω to a map $K[y] \to \mathbb{Q}[y]$ that fixes y. This maps $p \mapsto p^*$, hence induces a homomorphism

$$\tau : K[y]/(p) \to \mathbb{Q}[y]/(p^*)$$

Let ξ be the map obtained by composing ϕ^{-1} with τ. So

$$\xi := \tau \circ \phi^{-1} : K[\theta] \to \mathbb{Q}[y]/(p^*).$$

Hence $\mathbb{Q}[y]/(p^*)$ is a finite extension of $\mathbb{Q}$.

We can assume that our extension $\mathbb{Q}[y]/(p^*)$ is generated by θ^*, so $\mathbb{Q}(\theta^*) = \mathbb{Q}[y]/(p^*)$. The conjugate set of θ over K all lie in A. Call them $\theta_1 = \theta, \ldots, \theta_d$. Let their ξ-images be $\theta_1^* = \theta^*, \ldots, \theta_d^*$. Applying ξ to the coefficients of

$$p(y) = (y - \theta_1) \cdots (y - \theta_d)$$

gives

$$p^*(y) = (y - \theta_1^*) \cdots (y - \theta_d^*).$$

Thus $(\mathbb{Q}[y]/(p^*))/\mathbb{Q}$ is normal, and hence galois.

As θ is a generator of L over K, for each $i \in 1, \ldots, d$, there is a unique $\sigma_i \in G$ such that $\sigma_i(\theta) = \theta_i$. Similarly, there is a unique $\sigma_i^* \in \mathrm{Gal}(\mathbb{Q}(\theta^*)/\mathbb{Q})$ such that $\sigma_i^*(\theta^*) = \theta_i^*$. Hence $\sigma_i \mapsto \sigma_i^*$ is a bijection from $\mathrm{Gal}(K(\theta)/K)$ to $\mathrm{Gal}(\mathbb{Q}(\theta^*)/\mathbb{Q})$. Now let $r \in K[\theta]$ be fixed. Write $r = f(\theta)$, with $f(y) \in K[y]$. Let $f^*(y) \in \mathbb{Q}[y]$ be obtained by applying ω to the coefficients of f. Then

$$\begin{aligned}\sigma_i^*(\xi(r)) = \sigma_i^*(\xi(f(\theta))) = \sigma_i^*(f^*(\theta^*)) = f^*(\theta_i^*)\\ = \xi(f(\theta_i)) = \xi(\sigma_i(f(\theta))) = \xi(\sigma_i(r)).\end{aligned}$$

Hence

$$\sigma^*(\xi(r)) = \xi(\sigma(r))$$

for all $r \in K[\theta]$ and all $\sigma \in G$. In particular,

$$(\sigma\tau)^*(\theta^*) = (\sigma\tau)^*(\xi(\theta))$$

$$= \xi(\sigma\tau(\theta)) = \sigma^*(\xi(\tau(\theta))) = \sigma^*\tau^*(\theta^*).$$

Hence the map $\sigma \mapsto \sigma^*$ is an isomorphism. □

7.3.5 Conditions To Construct An Extension With Galois Group G

Proposition 7.3.20. *Let K be a Hilbertian field. Let G be a finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$ that acts on $K[x_1, \ldots, x_n]$ by linear substitutions. If the invariant subfield $K(x_1, \ldots, x_n)^G$ is purely transcendental over K, then there exists a finite galois extension L/K with galois group G.*

Proof. Suppose

$$K(x_1, \ldots, x_n)^G = K(f_1, \ldots, f_n)$$

for some algebraically independent polynomials $f_1, \ldots, f_n$ in $x_1, \ldots, x_n$. By Artin's Theorem 1.4.7, $K(x_1, \ldots, x_n)$ is a galois extension of $K(f_1, \ldots, f_n)$ with galois group G. Let $\alpha \in K(x_1, \ldots, x_n)$ be such that

$$K(x_1, \ldots, x_n) = K(f_1, \ldots, f_n, \alpha).$$

Let α have minimal polynomial $P_\alpha(f_1, \ldots, f_n)$ over $K(f_1, \ldots, f_n)$. Applying Hilbert Irreducibility (Lemma 7.3.19), we obtain an extension L of K, with galois group G, generated by α^*, a root of $P_\alpha(f_1^*, \ldots, f_n^*)$. □

7.4 Proof Of The Main Theorem

Proof. (1) We have $\dim_K(\alpha) \leq \deg_K(\alpha)$, from linear algebra. It follows from Lemma 7.3.1 that

$$\dim_K(\alpha) \leq d \leq d_{\max}(n), \tag{7.6}$$

since if G is the galois group of α over K, then G has a representation over $GL_n(K)$.

(2) The lower bound is attained for all n by applying Lemma 7.3.7 with $K = \mathbb{Q}$ and $G = S_n$ (an extension $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \cong S_n$ exists for all n, by Theorem 1.4.11).

For any given $n \in \mathbb{N}$, let G be the finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$ of maximal order given in Table 7.1. By Lemma 7.3.8, the given n-dimensional representation is a subrepresentation of the regular representation. Let $x_1, \ldots, x_n$ be indeterminates, and let G act on $\{x_1, \ldots, x_n\}$ by linear substitutions. Then the fixed field $\mathbb{Q}(x_1, \ldots, x_n)^G$ is purely transcendental over $\mathbb{Q}$ by Proposition 7.3.14.

By Proposition 7.3.20, there exists a finite galois extension L of $\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$.

From Lemma 7.3.7, there exists $\alpha \in L$ such that $\deg_{\mathbb{Q}}(\alpha) = |G|$ and $\dim_{\mathbb{Q}}(\alpha) = n$ as required. □

7.5 Attaining The Upper Bound In The Main Theorem

7.5.1 Applying the Theory

To attain $d = d_{\max}(n)$, we will use α for which the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois with Galois group isomorphic to the maximal finite subgroup G of $\mathrm{GL}_n(\mathbb{Q})$ given in Table 7.1.

First of all, we need the generators of the invariant subring $\mathbb{Q}(f_1, \dots, f_n)$ of $\mathbb{Q}(x_1, \dots, x_n)$. These are known, but can be calculated as follows:

Let G act on $\{x_1, \dots, x_n\}$ by linear substitutions. Then calculate

$$P[T] := \prod_{g \in G} (T - g(x_1)).$$

First suppose $n \neq 9$ or 10. Then as G acts transitively on the x_i, the orbit of x_1 contains all of the x_i. Equate $f_1(x_1, \dots, x_n)$ to the coefficient of the highest power of T in $P[T]$ that contains nontrivial homogeneous monomials in $x_1, \dots, x_n$. Then for the next highest power of T, if the coefficient is algebraically independent of f_1, set it equal to f_2. Continue the process, at each stage checking that the coefficient of the power of T is not a polynomial over K in the f_i already defined.

$P[T]$ is an auxiliary polynomial in $(T, f_1, \dots, f_n)$, that has roots (including) $\alpha_1, \dots, \alpha_n$ $\mathbb{Q}$-independent such that the extension

$$\mathbb{Q}(\alpha_1, \dots, \alpha_n, f_1, \dots, f_n)/\mathbb{Q}(f_1, \dots, f_n)$$

is galois with galois group G. Next we choose $b_1, \dots, b_n \in \mathbb{Q}$ such that, taking

$$\alpha = b_1\alpha_1 + \cdots + b_n\alpha_n,$$

we have $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$. Such a choice of $b_1, \dots, b_n$ is possible by Proposition 1.3.9. An alternative way to produce the same α is to define

$$\alpha^* = b_1x_1 + \cdots + b_nx_n,$$

and calculate as before

$$P_\alpha := \prod_{g \in G} (T - g(\alpha^*)).$$

This gives a polynomial of degree $|G|$ in $T, f_1, \dots, f_n$.

In either case, we can (theoretically) write our polynomial in terms of generators $f_1, \dots, f_n$ of the invariant subfield. By Hilbert's Irreducibility Theorem 7.3.19, there exists $c_1, \dots, c_n \in \mathbb{Q}$ such that setting

$$f_i(x_1, \dots, x_n) = c_i$$

for $1 \leq i \leq n$, P_α (resp. P) will be an irreducible polynomial in $\mathbb{Q}[T]$ whose roots are the conjugate set of α (resp. α_1). Finally, if $n = 9$ or 10, G is a direct product of groups acting transitively, so the invariants of G can be found by calculating separately the invariants for each direct factor.

Unfortunately, it is difficult to check that any given choice of $c_1, \dots, c_n$ is "suitable" if $|G|$ is large — even for $n = 4, G = W(F_4)$, such checks have proved difficult for Maple to handle.

7.5.2 The 2-Dimensional Example of Degree 12

Example 7.5.1. An example of an algebraic number α satisfying $\deg_{\mathbb{Q}}(\alpha) = 12$ and $\dim_{\mathbb{Q}}(\alpha) = 2$ is

$$\alpha = 2^{\frac{1}{6}}(1 + 3\omega),$$

where $\omega^2 + \omega + 1 = 0$. The conjugate set of α is $\{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_{12}\}$, where

$$\begin{aligned}
\alpha_2 &= \omega 2^{\frac{1}{6}}(1 + 3\omega), \\
\alpha_3 &= \omega^2 2^{\frac{1}{6}}(1 + 3\omega) = -\alpha - \alpha_2, \\
\alpha_4 &= 2^{\frac{1}{6}}(3 + 3\omega) = \frac{-5}{7}\alpha_1 + \frac{3}{7}\alpha_2, \\
\alpha_5 &= 2^{\frac{1}{6}}(3 + \omega) = \frac{-3}{7}\alpha_1 - \frac{8}{7}\alpha_2, \\
\alpha_6 &= 2^{\frac{1}{6}}(-1 + 2\omega) = \frac{8}{7}\alpha_1 + \frac{5}{7}\alpha_2,
\end{aligned}$$

and $\{\alpha_7, \ldots, \alpha_{12}\} = \{-\alpha_1, \ldots, -\alpha_6\}$.

The minimal polynomial of α is $P_\alpha : X^{12} + 572X^6 + 470596$.

Note that the corresponding finite subgroup of $\mathrm{GL}_2(\mathbb{Q})$ is a faithful representation of $W(G_2)$, has order twelve, and is generated by the matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} \frac{-5}{7} & \frac{8}{7} \\ \frac{3}{7} & \frac{5}{7} \end{pmatrix}.$$

7.5.3 An Example Where $G = W(B_3)$

Corollary 7.5.2. *If $G = W(B_n)$ in Lemma 7.3.7, then choosing $b_1, \ldots, b_n \in \mathbb{Q}^*$ all having different moduli will give an $\alpha = b_1\alpha_1 + \cdots + b_n\alpha_n$ that satisfies $\dim_{\mathbb{Q}}(\alpha) = n$ and $\deg_{\mathbb{Q}}(\alpha) = 2^n n!$.*

Proof. $W(B_n)$ is the *signed permutation group*, i.e. the group of $n \times n$ matrices with entries in $\{1, 0, -1\}$ having exactly one non zero entry in each row and each column. The action of $W(B_n)$ on $\{\alpha_1, \ldots, \alpha_n\}$ by linear substitutions permutes the α_i and alternates some of their signs, so if the b_i are non zero and distinct, then $\deg_{\mathbb{Q}}(\alpha) = 2^n n!$. □

Example 7.5.3. Consider $n = 3$: From Lemma 7.3.15, the generators of the B_3-invariant subfield are $f_1 = x_1^2 + x_2^2 + x_3^2, f_2 = x_1^4 + x_2^4 + x_3^4$ and $f_3 = x_1^6 + x_2^6 + x_3^6$. Setting $f_1 = 3, f_2 = -5, f_3 = 20$ and $y = x_1 + 2x_2 + 3x_3$ (the coefficients of x_1, x_2, x_3 are chosen in accordance with Corollary 7.5.2) and eliminating x_1, x_2, x_3

from the system of equations

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= 3 \\ x_1^4 + x_2^4 + x_3^4 &= -5 \\ x_1^6 + x_2^6 + x_3^6 &= 20 \\ y &= x_1 + 2x_2 + 3x_3 \end{aligned} \tag{7.7}$$

gives a polynomial $P_2[y]$:

$$\begin{aligned} &y^{48} - 720y^{46} + 250368y^{44} - 55808760y^{42} + 8977940832y^{40} \\ &- 1115334443040y^{38} + 111935136044684y^{36} - 9369930116421360y^{34} \\ &+ 669474635847318240y^{32} - 41498928789239602600y^{30} \\ &+ 2256031043775588868224y^{28} - 108243353189287557369120y^{26} \\ &+ 4598892825483080298681270y^{24} - 173073180203566336237521840y^{22} \\ &+ 5744886485254097336805480768y^{20} \\ &- 166330156298436333598058893960y^{18} \\ &+ 4128375688235990189108415172320y^{16} \\ &- 85686863133757840437626064038880y^{14} \\ &+ 1406724125150620160480427076102380y^{12} \\ &- 16502478280402427926342131451877520y^{10} \\ &+ 129901904593279344971655552454976376y^{8} \\ &- 521706752963137888850543724025412440y^{6} \\ &+ 719905927757187016456723151771657376 0y^{4} \\ &- 14636118259595977154253380875644518880y^{2} \\ &+ 3053666927721443582598733583288076 1681 \end{aligned} \tag{7.8}$$

whose conjugates span a 3-dimensional vector space over $\mathbb{Q}$.

7.6 Fields Other Than $\mathbb{Q}$

We examine the effect on the degree of α if we change the base field of the vector space V from $\mathbb{Q}$ to either a finite extension of $\mathbb{Q}$, or a finite field.

Definition 7.6.1. Let K be an arbitrary field and $n \in \mathbb{N}$ be fixed. We denote the maximal degree of the set of numbers α, algebraic over K, with $\dim_K(\alpha) = n$ as $D_K(n)$.

For example, $D_{\mathbb{Q}}(n) = d_{\max}(n)$.

7.6.1 Number Fields

Theorem 7.6.2. *If K is a number field of degree m over $\mathbb{Q}$, then the degree of an algebraic number α where $dim_K(\alpha) = n$ is bounded above by $D_{\mathbb{Q}}(mn) = d_{\max}(mn)$.*

Proof. Let $[K : \mathbb{Q}] = m$, and let α be algebraic over K such that $\deg_K(\alpha) = d$, $\dim_K(\alpha) = n$. Then by Proposition 7.3.1, there exists a subgroup of $\mathrm{GL}_n(K)$ of order d. An n-dimensional vector space over K can be considered as an mn-dimensional vector space over $\mathbb{Q}$, so we have an injection

$$\mathrm{GL}_n(K) \hookrightarrow \mathrm{GL}_{mn}(\mathbb{Q}).$$

Thus d, the degree over K of α is bounded above by mn. □

7.6.2 Cyclotomic Extensions Of $\mathbb{Q}$

Let K be an extension of $\mathbb{Q}$, and let l denote the number of roots of unity in K. Clearly l is even. The roots of unity in K are ω_l^i $(i = 0, \dots, l-1)$, where ω_l is the primitive l^{th} root of 1. The $n \times n$ matrix $M_n(K)$ is defined to be the group of all monomial matrices whose non zero entries are roots of 1 in K.

The following result again comes from Feit [8], with a correction in the case $l = 4, n = 2$:

Theorem 7.6.3. *Let $l \in \mathbb{N}$ be even. Then $M_n(\mathbb{Q}(\omega_l))$ is a finite subgroup of $\mathrm{GL}_n(\mathbb{Q}(\omega_l))$ of maximal order, $l^n n!$, except in the cases given in Table 7.3 where the maximal order is achieved by the listed group:*

l	n	G	$\lvert G\rvert$
4	2	$\langle \mathrm{GL}_2(\mathbb{F}_3), \omega_4 I\rangle = \mathrm{ST}_8$	96
4	4	ST_{31}	46080
4	5	$\mathrm{ST}_{31} \times \langle \omega_4 I\rangle$	184320
4	8	$\mathrm{ST}_{31} \wr S_2$	4246732800
6	4	ST_{32}	155520
6	6	ST_{34}	39191040
8	2	$\langle \mathrm{GL}_2(\mathbb{F}_3), \omega_8 I\rangle = \mathrm{ST}_9$	192
10	2	$\langle \omega_5 I\rangle \times SL_2(\mathbb{F}_5) = \mathrm{ST}_{16}$	600
10	4	$\mathrm{ST}_{16} \wr S_2$	720000
10	6	$\mathrm{ST}_{16} \wr S_3$	1296000000
20	2	$\langle \mathrm{SL}_2(\mathbb{F}_5), \omega_{20} I\rangle = ST_{17}$	1200
a	b	$(\mathbb{Z}/a\mathbb{Z})^b \rtimes S_b$	$a^b b!$

Table 7.3: Maximal Subgroups for $M_n(\mathbb{Q}(\omega_l))$ for exceptional n

The pair (a, b) in the last row of Table 7.3 refers to all $a \in 2\mathbb{N}, b \in \mathbb{N}$ that have not previously occurred as a pair.

As noted in Section 1.5, the notation ST_r refers to the numbering of the classification of pseudo-reflection groups by Shephard and Todd [20].

Theorem 7.6.4. *Let K be a field containing l roots of unity. Then:*

1. *If K is hilbertian, then for all $n \geq 0$, there exists an α, algebraic over K, such that $\dim_K(\alpha) = n$ and $\deg_K(\alpha) = l^n n!$. Hence $l^n n!$ is a lower bound for $D_K(n)$.*
2. *If $K = M_n(\mathbb{Q}(\omega_l))$ as given in Theorem 7.6.3, then $D_K(n)$ is bounded above by the order of the group given in Table 7.3.*

Proof. (1) We know that $\mathrm{GL}_n(K)$ contains the group of order $l^n n!$, consisting of the permutation matrices with powers of the ω_i as its non zero entries. The invariant ring of this group is generated by the elementary symmetric polynomials of the l^{th} powers of the coordinates. Therefore, by Lemmas 7.3.1 and 7.3.7, there exists an α such that $\dim_K(\alpha) = n$ and $\deg_K(\alpha) = l^n n!$

(2) The result follows from Lemma 7.3.1 and Theorem 7.6.3. □

7.6.3 Attaining $D_K(n)$ for $K = M_n(l)$?

Let $K = M_n(l)$ defined as above. For non-exceptional values of l and n, $D_K(n) = l^n n!$. Moreover, $D_K(n) \geq l^n n!$ for the exceptional cases. The upper bound is attained iff the invariant subfield of $K(x_1, \ldots, x_n)$ is purely transcendental over K.

Example 7.6.5. Let $n = 2$, and $K = \mathbb{Q}(i)$. Does there exist an $\alpha \in \overline{K}$ such that $\dim_{\mathbb{Q}(i)}(\alpha) = 2$ and $\deg_{\mathbb{Q}(i)}(\alpha) = 96$?

The 2-dimensional matrix representation G of the group $Z_4\mathrm{GL}_2(\mathbb{F}_3)$ of order 96 is generated by the matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & i \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ -i & 0 \end{pmatrix}.$$

Let G act on $\{x_1, x_2\}$ by linear transformations. Let σ be an element of the representation that sends $x_1 \mapsto x_{\sigma(1)}$ and $x_2 \mapsto x_{\sigma(2)}$. Let S be the image of x_1 and x_2 under such a mapping. Now let

$$P = \prod_{x \in S} (T - x).$$

We obtain a polynomial $P \in \mathbb{Q}(i)(x, y, T)$ of degree 24. The G-invariant subfield $\mathbb{Q}(i)(x_1, x_2)^G$ is generated by

$$\begin{aligned} t_1(x_1, x_2) =&(x_1^2 + x_2^2 - x_1x_2)(x_1^2 - x_2^2 + ix_1x_2) \\ &(x_1^2 - ix_2^2 + (i-2)x_1x_2)(x_1^2 - ix_2^2 + (2i-1)x_1x_2) \end{aligned} \tag{7.9}$$

and

$$\begin{aligned} t_2(x_1, x_2) =&\frac{1}{2}(x_1^2 + ix_2^2)(x_1^2 - ix_2^2 + (2i-2)x_1x_2) \\ &(x_1^2 - (i+1)x_2^2 + 2ix_1x_2)(2x_1^2 - (1+i)x_2^2 + (2i-2)x_1x_2) \\ &(x_1^2 + (1-i)x_2^2 - 2x_1x_2)(2x_1^2 + (1-i)x_2^2 + (2i-2)x_1x_2) \end{aligned} \tag{7.10}$$

We can construct our α_1, α_2 as follows: By Hilbert's Irreducibility Theorem 7.3.19, there exist $c_1, c_2 \in \mathbb{Q}(i)$ such that on making the substitutions $t_1(x_1, x_2) = c_1$ and $t_2(x_1, x_2) = c_2$, we obtain a galois extension $\mathbb{Q}(i)(\alpha_1, \alpha_2)$ of $\mathbb{Q}(i)$ with galois group G. The choice of $t_1 = 1 + i, t_2 = 1$ is suitable, and gives

$$P := 27T^{24} - 270(1+i)T^{16} + 270T^{12} - 810iT^8 + 54(1+i)T^4 - 9 + 8i.$$

In the usual way, $b_1, b_2 \in \mathbb{Q}(i)$ can be chosen such that $\alpha = b_1\alpha_1 + b_2\alpha_2$ is a generator of this extension, and $\dim_{\mathbb{Q}(i)}(\alpha) = 2, \deg_{\mathbb{Q}(i)}(\alpha) = 96$ (a suitable choice is $b_1 = 1$ and $b_2 = 2$).

Example 7.6.6. Let $K = \mathbb{Q}(i, \sqrt{2})$, so K contains 8 roots of unity. Does there exist an α such that $\dim_K(\alpha) = 2$ and $\deg_K(\alpha) = 192$?

By Table 7.3, the finite 2-dimensional matrix group with entries in K of maximal order is the group $G = \langle \mathrm{GL}_2(\mathbb{F}_3), \omega_8 I\rangle$ of order 192. It can be found by multiplying the matrix group in Example 7.6.5 by the elements $\frac{1 \pm i}{\sqrt{2}} \in K$. The generators of G are:

$$\begin{pmatrix} 0 & \frac{1+i}{\sqrt{2}} \\ \frac{1+i}{\sqrt{2}} & \frac{i-1}{\sqrt{2}} \end{pmatrix} \text{ and } \begin{pmatrix} 0 & \frac{1+i}{\sqrt{2}} \\ \frac{1-i}{\sqrt{2}} & 0 \end{pmatrix}.$$

The generators of the G-invariant subfield are:

$$\begin{aligned} t_1 =& -21x^4y^4 + 14x^5y^3 - 14ix^3y^5 - 4iyx^7 + x^8 \\ &- 4xy^7 - 14ix^6y^2 + 14x^3y^5 + 14iy^3x^5 + y^8 \end{aligned} \tag{7.11}$$

and

$$\begin{aligned}
t_2 = {} & 310771850x^{24} + 310771850y^{24} + 6541213522480ix^{18}y^6 \\
& + 157250556100ix^{21}y^3 + 1789302684540iy^{19}x^5 + 86046736052640ix^{10}y^{14} \\
& + 42886515300ix^2y^{22} + 3729262200ix^{23}y + 39483086501720ix^{15}y^9 \\
& + 79194568238520ix^{13}y^{11} + 10660358869740ix^7y^{17} - 79194568238520ix^{11}y^{13} \\
& - 39483086501720ix^{15}y^9 - 10660358869740ix^{17}y^7 - 6541213522480ix^6y^{18} \\
& - 157250556100ix^3y^{21} - 1789302684540ix^{19}y^5 - 86046736052640ix^{14}y^{10} \\
& - 3729262200iy^{23} - 42886515300ix^{22}y^2 - 3729262200x^{23}y \\
& - 839382604074y^{20}x^4 + 157250556100y^{21}x^3 + 157250556100x^{21}y^3 \\
& + 3102220045771y^{16}x^8 - 10660358869740y^{17}x^7 + 1789302684540y^{19}x^5 \\
& + 79194568238520y^{13}x^{11} - 39483086501720y^{15}x^9 - 839382604074x^{20}y^4 \\
& + 1789302684540x^{19}y^5 - 10660358869740x^{17}y^7 - 122353879346244y^{12}x^{12} \\
& + 31022220045771x^{16}y^8 - 39483086501720x^{15}y^9 \\
& + 79194568238520x^{13}y^{11} - 3729262200y^{23}x.
\end{aligned} \tag{7.12}$$

7.6.4 Finite Fields

The following results on finite fields are taken from Lidl and Neddereiter [15]:

Lemma 7.6.7. *Let K be a finite field, and L/K a finite algebraic extension. The galois group of L/K is cyclic.*

Definition 7.6.8. Let $K = F_q$ be a finite field. A generator of the cyclic group F_q^* is called a **primitive element**.

Definition 7.6.9. Let $f \in \mathbb{F}_q[x]$ be a nonzero polynomial. If $f(0) \neq 0$, then the least positive integer e for which $f(x)$ divides $x^e - 1$ is defined to be the **order** of f, denoted $\operatorname{ord}(f(x))$. If $f(0) = 0$, then for some (unique) $h \in \mathbb{N}$ and $g \in \mathbb{F}_q[x]$ such that $g(0) \neq 0$, we have $f(x) = x^h g(x)$, and we define $\operatorname{ord}(f(x)) = \operatorname{ord}(g(x))$.

Lemma 7.6.10. *[15] Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree m and with $f(0) \neq 0$. Then $\operatorname{ord}(f(x))$ is equal to the order of any root of f in the multiplicative group $\mathbb{F}_{q^m}^*$.*

Definition 7.6.11. The polynomials

$$l(x) = \sum_{i=0}^{n} \alpha_i x^i$$

and

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$$

are called **q-associates** of each other. In particular, $l(x)$ is the **conventional q-associate** of $L(x)$, and $L(x)$ is the **linearized q-associate** of $l(x)$.

Lemma 7.6.12. *[15] Let $f(x)$ be irreducible in $\mathbb{F}_q[x]$, and let $F(x)$ be its linearized q-associate. Then the degree of every irreducible factor of $F(x)/x$ in $\mathbb{F}_q[x]$ is equal to* $\operatorname{ord}(f(x))$.

Using these preliminary results, we give the main result for K a finite field.

Theorem 7.6.13. *Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements, for some prime p and $n \in \mathbb{N}$. Then $D_{\mathbb{F}_q}(n) = q^n - 1$.*

Proof. As usual let α be algebraic over $\mathbb{F}_q$ with $\dim_{\mathbb{F}_q}(\alpha) = n$ and $\deg_{\mathbb{F}_q}(\alpha) = d$. Lemma 7.3.1 still holds for a finite field, so the galois group of α over $\mathbb{F}_q$ must be a finite subgroup of $GL_n(\mathbb{F}_q)$, and it must be cyclic, by Lemma 7.6.7. The characteristic equation of an invertible matrix in $\mathrm{GL}_n(\mathbb{F}_q)$ is of the form $X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, where the $a_i \in \mathbb{F}_q$ and $a_0 \neq 0$ is the determinant of the matrix. This equation splits over $\mathbb{F}_{q^n}$ and so its roots are nonzero elements of $\mathbb{F}_{q^n}$, therefore have order at most $q^n - 1$. Hence $|G| \leq q^n - 1$.

Next, we show that the upper bound for $D_{\mathbb{F}_q}(n)$ can be attained. Let g be a generator of the multiplicative group $\mathbb{F}_{q^n}^*$, and let its minimal equation be

$$g(x) = \sum_{i=0}^{n} c_i X^i,$$

with $c_i \in \mathbb{F}_q$ for $i \in \{0 \cdots n\}$. Then by Lemma 7.6.10, $\operatorname{ord}(g(x)) = q^n - 1$. Consider the polynomial

$$G(x)/x = \sum_{i=0}^{n} c_i X^{q^i - 1},$$

so that G is the linearized q-associate of g. Then by Lemma 7.6.12, $G(x)/x$ is irreducible of degree $q^n - 1$. Now let β and γ be roots of $G(x)$ in $\mathbb{F}_{q^n}$, and $c \in \mathbb{F}_q$. Then $\beta + \gamma$ and $c\beta$ are roots of G, since $(\beta + \gamma)^{p^i} = \beta^{p^i} + \gamma^{p^i}$ and $c^{q^i} = c$, for all $i \geq 0$. Hence the roots of $G(x)/x$ are the non zero elements of an n-dimensional vector space over $\mathbb{F}_q$, so $\dim_{\mathbb{F}_q}(G(x)/x) = n$ and $\deg_{\mathbb{F}_q}(G(x)/x) = q^n - 1$. □

Example 7.6.14. Let $K = \mathbb{F}_3$ and $n = 2$. There is a cyclic group of $\mathrm{GL}_2(\mathbb{F}_3)$ generated by the matrix

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}.$$

A primitive element of the multiplicative group $\mathbb{F}_{3^2}^*$ is given by a root of the characteristic polynomial of A, namely

$$X^2 + X + 2 = \sum_{j=0}^{2} c_j X^j \in \mathbb{F}_3[X].$$

We consider the polynomial

$$P[X] := \sum_{i=0}^{2} c_i X^{q^i - 1} = X^8 + X^2 + 2.$$

Let α be a root of $P[X]$. Then α is a primitive element of the field of $3^{3^2-1} = 6561$ elements. Furthermore, the conjugates of α are the non-zero elements of a 2-dimensional $\mathbb{F}_3$-vector space:

$$\alpha, 2\alpha, \alpha^3, 2\alpha^3, \alpha^3 + \alpha, \alpha^3 + 2\alpha, 2\alpha^3 + \alpha, 2\alpha^3 + 2\alpha,$$

giving $\dim_{\mathbb{F}_3}(\alpha) = 2$ and $\deg_{\mathbb{F}_3}(\alpha) = 3^2 - 1 = 8$.

Example 7.6.15. Let $K = \mathbb{F}_2$, and $n = 3$. Then the cyclic group of maximal order over $\mathbb{F}_2$ is of order $2^3 - 1 = 7$. One such generator is

$$B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

B has characteristic equation $P_B[X] : X^3 + X + 1 = \sum_{j=0}^{3} c_j X^j$. P_B is irreducible over $\mathbb{F}_2$. Let β be a root of $P_\beta[X] : \sum_{j=0}^{3} c_j X^{q^j - 1} = X^7 + X + 1$. Then β is a primitive element of the field containing $2^{2^3-1} = 128$ elements. Furthermore, the conjugates of β are

$$\beta, \beta^2, \beta^2 + \beta, \beta^4, \beta^4 + \beta^2, \beta^4 + \beta, \beta^4 + \beta^2 + \beta.$$

So the $7 = 2^3 - 1$ conjugates of β are the non zero elements of a 3-dimensional $\mathbb{F}_2$-vector space.