On a Special Class of Reduced Algebraic Numbers

Thesis by

John Charles Wolfskill

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1982

(Submitted May 18, 1982)

ACKNOWLEDGEMENTS

During my tenure as a graduate student, I have been blessed with help from many sources. The Mathematics Department here has been generous in providing financial support; I am especially thankful for the Bohnenblust travel money I received. The secretarial staff here is excellent. I am grateful to Lillian Chappelle for her thoroughly professional typing of this manuscript.

I thank Marshall Hall, Jr. for starting and encouraging me in mathematical research. I had several valuable discussions with David Cantor. Most of all, I am deeply grateful to Pat Morton for his guidance, teaching, and great patience in spite of my numerous blunders.

My family and friends have been a great blessing to me, concerning matters both mathematical and otherwise. Among my colleagues I am particularly grateful to Igor Mikolič-Torreira, Mike Lewy, and Joel Fowler. Finally, I owe many thanks to my fiancée, Linda. It is no accident that this research came to fruition only after she gave me the peace of mind which was necessary.

ABSTRACT

The notion of a reduced real quadratic number goes back to Gauss, who defined such a number to be reduced if it is greater than one, and its conjugate between negative one and zero. An equivalent characterization is that the continued fraction of a reduced quadratic number is purely periodic. Zassenhaus generalized this by defining a real algebraic number α to be reduced if $\alpha > 1$ and $-1 < \mathrm{Re}\,\alpha' < 0$ for the conjugates α' of α distinct from α. In this thesis, several properties of these reduced numbers are developed. In particular it is shown that there exist reduced numbers α with the property that α has no reduced immediate predecessor, that is, $u + \frac{1}{\alpha}$ is not reduced for any choice of the rational integer u. We call such a number α an ancestor. These ancestors have the property that every real algebraic number of degree at least three is equivalent to exactly one of them. Here, equivalence is in the sense of continued fractions; $\alpha \sim \beta$ means that there exist integers a, b, c, and d such that $ad - bc = \pm 1$ and $\alpha = \frac{a\beta + b}{c\beta + d}$. This is equivalent to α and β having identical continued fractions after a certain point. This property of ancestors gives rise to an application to the problem of determining whether or not two given integral binary homogeneous forms are equivalent, assuming that each form has a real root. If the forms are equivalent, so are the roots of the forms; this can be checked by comparing the ancestors. This method is computationally effective.

In another direction, there is a connection between the reduced numbers defined above and the Pisot-Vijayaraghavan (PV) numbers (a PV number is a real algebraic integer greater than one all of whose other conjugates have absolute value less than one). It turns out that any

reduced algebraic integer which is not an ancestor is a PV number; integral ancestors may or may not be. Part of the thesis is devoted to a more detailed comparison of PV numbers and integral ancestors. On one side, there is the theorem of Salem that the PV numbers are closed. On the other, it is proved here that if K is a field of degree at least three over the rationals, real but not totally real, then no integral ancestor in K is isolated (that is, there are other integral ancestors arbitrarily close). Much more is true; one can show in many cases that the integral ancestors in such a field lie in a set of non-trivial intervals in which they are dense. This decomposition is studied in more detail. For example, in $Q(\alpha)$, where $\alpha^3 = \alpha + 1$, the integral ancestors are actually dense in $[1,\infty)$. In contrast, in $Q(\sqrt[3]{2})$, the integral ancestors are dense in $[1,2] \cup [3,5] \cup [6,8] \cup [9,11] \cup \ldots$ and none of them occur in the gaps. It is proved that all cubic fields which are not totally real are like one of these two fields in the way the integral ancestors are distributed. Similar results hold for fields of higher degree, although the situation is somewhat more complicated.

NOTATION

Throughout this thesis, we will use the following notation:

Z is the ring of rational integers.

Q is the field of rational numbers.

R is the field of real numbers.

R^n is n-dimensional real space.

For a complex number α, $\operatorname{Re}\alpha$ is the real part of α and $\operatorname{Im}\alpha$ is the imaginary part.

For two sets S and T, the difference $S-T$ is the set of things in S but not in T.

We use the notation (a,b) both for the greatest common divisor of a and b, and for the open interval. It will be clear from context which is meant.

If α is an algebraic number of degree n over Q, we denote its conjugates by $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$.

$\operatorname{Tr}\alpha$ is the trace of α; that is, the sum of its conjugates.

$N_{K/Q}(\alpha)$ is the norm of α; that is, the product of the images of α under the automorphisms of K over Q. When the field K is clear, we write simply $N(\alpha)$.

$[x]$ is the greatest integer $\leq x$.

$\|x\|$ is the distance from x to the nearest integer.

Finally, the continued fraction notation $[u_0,u_1,u_2,\ldots]$ means

$$u_0 + \cfrac{1}{u_1 + \cfrac{1}{u_2 + \cdots}}$$

CONTENTS

INTRODUCTION

Let α be a real algebraic number of degree at least three over Q, and let $\alpha = [u_0, u_1, \ldots]$ be its regular continued fraction expansion. Let $\alpha_1, \alpha_2, \ldots,$ be the complete quotients; that is, $\alpha = [u_0, u_0, \ldots, u_{m-1}, \alpha_m]$. Zassenhaus [1] defined the "reduced state" of the continued fraction of α as a point at which $\alpha_k > 1$ and $0 < -\mathrm{Re}\,\alpha_k' \leq |\alpha_k'| < 1$ for each conjugate α_k' of α_k distinct from α_k. The reduced state is important for computational purposes; when this state is achieved, it is easy to discriminate between α_k and its real conjugates (this may not be true of α). This is important in calculating the continued fraction of α. Zassenhaus and Cantor [1] each showed that the reduced state is achieved after finitely many steps, and that if the condition of being reduced holds for α_k, it holds for α_j if $j \geq k$. We will modify Zassenhaus' definition slightly and say that a real algebraic number α is reduced if $\alpha > 1$ and $-1 < \mathrm{Re}\,\alpha' < 0$ for each conjugate α' of α distinct from α. This is a generalization of the existing notion of reduced real quadratic numbers (which goes back to Gauss).

In the continued fraction notation above, we call α_k a successor of α_j if $k > j$; we say it is an immediate successor if $k = j + 1$. Similarly, α_k is a predecessor of α_j if $k < j$, and an immediate predecessor if $k = j - 1$. It is easy to show that a successor of a reduced number is reduced. It is natural, then, to ask the same question about an immediate predecessor of a reduced number. It is proved here that any reduced number α has at most one reduced immediate predecessor; that is, there is at most one integer u such that $u + \frac{1}{\alpha}$ is reduced. Further, by going backwards in this manner one arrives after finitely many steps at a reduced number with no reduced immediate predecessor. We call such a number an ancestor. This thesis is devoted to studying these ancestors. One important property which follows from the facts above is that every real algebraic number of degree at least three is equivalent to exactly one ancestor.

One interesting feature of ancestors derives from the following observation: If α is a reduced algebraic integer and not an ancestor, then α is a PV number; that is, $|\alpha'| < 1$ for the conjugates α' of α distinct from α. Integral ancestors are in general not PV numbers. Because of the rather remarkable properties of PV numbers, in particular the fact that the PV numbers are a closed set (see [2] or [9]), it is natural to investigate the distribution of integral ancestors. One can show by using Minkowski's theorem on homogeneous linear forms that no integral ancestor in a real but not totally real number field K is isolated; that is, there are other integral ancestors in K arbitrarily close. More generally, the same is true for the ancestors within a particular ideal of K. However, this is far from the whole story. Given an ideal A of K, let $L(A) = \{\theta \geq 1 \mid \theta \text{ is a limit of ancestors in } A\}$. If K is a non-totally real cubic field, L(A) consists of non-trivial intervals; further, the intervals are completely determined by the least positive trace of a number in A. As a special case, $L(\frac{1}{\delta})$ is all of $[1,\infty)$, where δ is the different of K. Another special case of interest is the case A = (1) = the ideal of all algebraic integers in K. In this case, $L(A) = [1,\infty)$ if and only if $27 \nmid \Delta$, the discriminant of K; if

$27 | \Delta$, then $L(A) = [1,2] \cup \bigcup_{k=1}^{\infty} [3k, 3k+2]$.

For higher degree fields we were not able to prove that L(A) is a union of non-trivial intervals in general, although this is true under fairly general conditions. However, the decomposition of L(A) is somewhat more chaotic. For example, in $Q(\sqrt[4]{2})$, the integral ancestors are dense in intervals of the form $[2a + 2m\sqrt{2}, 2a + 2m\sqrt{2} + 1]$, where $a = [m\sqrt{2}]$, and no integral ancestor occurs outside these intervals. A similar result holds for $Q(\sqrt[4]{N})$ where $N = 2p$, p prime in Z. By taking N large enough, we can force every integral ancestor in $Q(\sqrt[4]{N})$ to be larger than a given bound. This contrasts sharply with the cubic case above, where the integral ancestors are always dense in [1,2].

This thesis is divided into four chapters. In the first we prove basic facts about reduced numbers, and in particular, the existence of ancestors. The second chapter contains various results which serve to characterize ancestors, in a sense. These results culminate in the theorem that the set of all ancestors in a fixed real number field of degree at least three is dense in $[1,\infty)$. It is in the third chapter that the sets L(A) defined above are studied. Most of the results require the restriction that the field not be totally real. For totally real fields, the corresponding theory is completely different -- in a fixed ideal there are infinitely many ancestors, all of which are isolated. In chapter four we give an application of ancestors to the problem of determining whether or not two given binary homogeneous forms are equivalent. Our method applies to forms which are irreducible and have at least one real root. The method we describe here is effective, and appears in general to be superior to existing methods.

For cubic and quartic forms, there are fairly simple algorithms which are based essentially on undetermined coefficients, such as is given in Delone and Faddeev [3]. However, this is not a promising method if the degree is any larger. The principal general method, due to Hermite and Julia, while theoretically useful, is impractical computationally (see ch. 18 of [6]). We comment on these methods in more detail in chapter four.

We conclude this thesis with a brief description of some unsolved problems which arise from this work.

Chapter 1. General Properties of Reduced Numbers

Throughout this chapter we will use the following notation:

α is a real algebraic number of degree $n \geq 3$.

The conjugates of α are $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$.

Let $\alpha = [u_0, u_1, \ldots, u_k, \ldots]$ be the continued fraction representation of α.

Define α_m for $m \geq 1$ by $\alpha = [u_0, u_1, \ldots, u_{m-1}, \alpha_m]$. These are the complete quotients in the continued fraction of α. Note that the conjugates $\alpha_m^{(k)}$ of α_m are defined by $\alpha^{(k)} = [u_0, u_1, \ldots, u_{m-1}, \alpha_m^{(k)}]$.

Of fundamental importance is the concept of equivalence of two numbers:

Definition. Let x and y be two real numbers. We say x is equivalent to y, denoted $x \sim y$, if $x = \frac{ay+b}{cy+d}$ where a, b, c, and $d \in Z$ and $ad - bc = \pm 1$.

This is an equivalence relation. A basic theorem from the theory of continued fractions states that $x \sim y$ if and only if x and y have identical continued fractions after a certain point (see, for example, [7], p. 65).

We also will use the following terminology:

Definition. In the continued fraction notation above, we say α_j is a successor of α_k if $j > k$; we say it is an immediate successor if $j = k + 1$. Similarly, α_j is a predecessor of α_k if $j < k$, and an immediate predecessor if $j = k - 1$.

It is important to note that all successors and predecessors of a given number are equivalent to each other.

The following definition, essentially due to Zassenhaus, is the starting point for this thesis.

Definition. Let α be a real algebraic number, as above. We say α is reduced if $\alpha > 1$ and $-1 < \mathrm{Re}\, \alpha^{(k)} < 0$ for $k = 2, \ldots, n$.

Note that this agrees with the reduction of quadratic numbers, due to Gauss.

Let α' be a real conjugate of α, and $\beta \pm i\gamma$ a pair of complex conjugates. From the defining equations $\alpha'_k = u_k + \frac{1}{\alpha'_{k+1}}$ and $\beta_k + i\gamma_k = u_k + \frac{1}{\beta_{k+1} + i\gamma_{k+1}}$ we may solve for α'_{k+1}, β_{k+1}, and γ_{k+1} to obtain

$$(1)\quad \begin{cases} \alpha'_{k+1} = \dfrac{1}{\alpha'_k - u_k} \\[2ex] \beta_{k+1} = \dfrac{\beta_k - u_k}{(\beta_k - u_k)^2 + \gamma_k^2} \\[2ex] \gamma_{k+1} = \dfrac{-\gamma_k}{(\beta_k - u_k)^2 + \gamma_k^2} \end{cases}$$

Lemma 1.1. Assume $\alpha_k > 1$. Then if $-1 < \alpha'_k < 0$, the same is true for α'_{k+1}. Also, if $-1 < \beta_k < 0$, the same is true for β_{k+1}. Consequently, the immediate successor of a reduced number is reduced, and so all successors are reduced by induction.

Proof. We have $u_k > 1$. Thus $\alpha'_k - u_k < -1$, and $(\beta_k - u_k)^2 > |\beta_k - u_k|$. The lemma follows immediately.

We are prepared now to prove the principal result of this chapter:

Theorem 1.2. In the notation fixed above,

1. α has a reduced successor.

2. If α has a reduced immediate predecessor, it is unique.

3. α has only finitely many reduced predecessors.

Proof. In view of the lemma, we need only show that each conjugate $\neq \alpha$ eventually drops into the appropriate range. For real conjugates, this is trivial -- if $\alpha^{(k)}$ is real, its continued fraction must differ from the one for α, since $\alpha \neq \alpha^{(k)}$. So at some point we will have

$$\alpha_m^{(k)} = u_m + \frac{1}{\alpha_{m+1}^{(k)}} \quad \text{where} \quad \alpha_{m+1}^{(k)} < 1.$$

From this it follows that $\alpha_{m+2}^{(k)} = \dfrac{1}{\alpha_{m+1}^{(k)} - u_{m+1}} < 0$, and then $-1 < \alpha_{m+3}^{(k)} < 0$.

Consider now a pair of complex conjugates $\beta \pm i\gamma$.

If $\beta_m \leq 0$ then $0 > \dfrac{\beta_m - u_m}{(\beta_m - u_m)^2 + \gamma_m^2} > \dfrac{\beta_m - u_m}{(\beta_m - u_m)^2} = \dfrac{1}{\beta_m - u_m} \geq -1$,

so $-1 < \beta_{m+1} < 0$.

If $\beta_m - u_m \geq 1$ then $\beta_{m+1} = \dfrac{\beta_m - u_m}{(\beta_m - u_m)^2 + \gamma_m^2} < \dfrac{\beta_m - u_m}{(\beta_m - u_m)^2} = \dfrac{1}{\beta_m - u_m} \leq 1$,

and so $\beta_{m+1} < 1$, $\beta_{m+2} < 0$, and $-1 < \beta_{m+3} < 0$.

If $\beta_m - u_m \leq 0$ then $\beta_{m+1} \leq 0$ and $-1 < \beta_{m+2} < 0$.

If $|\gamma_m| \geq 1$ and $0 < \beta_m - u_m < 1$ then $\beta_{m+1} < \beta_m - u_m < 1$, and so $-1 < \beta_{m+3} < 0$.

Thus we will have $-1 < \beta_s < 0$ for some s unless it happens that

$$0 < \beta_m - u_m < 1 \quad \text{and} \quad |\gamma_m| < 1 \quad \forall m.$$

Suppose this happens. Then, since $\beta_{m+1} > u_{m+1} \geq 1$, we have $\beta_m - u_m > (\beta_m - u_m)^2 + \gamma_m^2$.

This implies that

$$|\gamma_{m+1}| = \frac{|\gamma_m|}{(\beta_m - u_m)^2 + \gamma_m^2} > \frac{|\gamma_m|}{\beta_m - u_m}.$$

Now $(\beta_m - u_m)\ \beta_{m+1} = \dfrac{(\beta_m - u_m)^2}{(\beta_m - u_m)^2 + \gamma_m^2} < 1$, so $\dfrac{1}{\beta_m - u_m} > \beta_{m+1} > u_{m+1}$.

Thus $|\gamma_{m+1}| > u_{m+1}|\gamma_m|$. Eventually, we will have $|\gamma_s| > 1$ for some s, unless all but finitely many of the partial quotients $u_k = 1$. But this would imply $\alpha \sim [1,1,1,\ldots] = \frac{1+\sqrt{5}}{2}$, which contradicts the assumption that α is not a quadratic number. This proves the first assertion.

Let α_1 be a reduced number. Any immediate predecessor α to α_1 has the form $\alpha = u + \dfrac{1}{\alpha_1}$ for some integer u. We assert that there is at most one choice for u such that α is reduced. In fact, any conjugate of α_1 will determine u. Consider a real conjugate, say, $\alpha_1^{(2)}$. The corresponding conjugate of α is $\alpha^{(2)} = u + \dfrac{1}{\alpha_1^{(2)}}$. If α is reduced, then $-1 < \alpha^{(2)} < 0$ which implies that

$u < \dfrac{-1}{\alpha_1^{(2)}} < u + 1$ and so $\dfrac{-1}{\alpha_1^{(2)}} = [u, \dfrac{-1}{\alpha^{(2)}}]$, i.e., u is the first partial quotient in the continued fraction of $\dfrac{-1}{\alpha_1^{(2)}}$, and $\dfrac{-1}{\alpha^{(2)}}$ is the complete quotient. As $u = [\dfrac{-1}{\alpha_1^{(2)}}]$, u is determined uniquely.

Consider now a complex conjugate of α_1, say, $\beta_1 + i\gamma_1$. We have

$$\beta + i\gamma = u + \frac{1}{\beta_1 + i\gamma_1} = u + \frac{\beta_1 - i\gamma_1}{\beta_1^2 + \gamma_1^2}, \quad \text{so} \quad \beta = u + \frac{\beta_1}{\beta_1^2 + \gamma_1^2}.$$

If α is reduced, then $-1 < \beta < 0$, which implies that $u < \frac{-\beta_1}{\beta_1^2+\gamma_1^2} < u+1$. Again, there is at most one choice for u. This establishes the second assertion. For future reference, let us label the formulas for u:

$$(2) \begin{cases} u < \dfrac{-1}{\alpha_1^{(2)}} < u+1 & (\alpha_1^{(2)} \text{ real}) \\ u < \dfrac{-\beta_1}{\beta_1^2+\gamma_1^2} < u+1 & \end{cases}$$

Finally, let α_0 be reduced, and consider a chain of reduced predecessors $\alpha_{-k} = [u_{-k}, u_{-k+1}, \ldots, u_{-1}, \alpha_0]$. We assert that k cannot be arbitrarily large.

If α_0 has two real conjugates, say, $\alpha_0^{(2)}$ and $\alpha_0^{(3)}$, then we have the continued fraction expansions (by (2) above)

$$\frac{-1}{\alpha_0^{(j)}} = [u_{-1}, u_{-2}, \ldots, u_{-k}, \frac{-1}{\alpha_{-k}^{(j)}}] \qquad (j = 2,3)$$

Since $\frac{-1}{\alpha_0^{(2)}} \neq \frac{-1}{\alpha_0^{(3)}}$, their continued fractions can agree only to a finite number of places, so this bounds k.

If α_0 does not have two real conjugates, then it must have a pair of complex conjugates $\beta_0 \pm i\gamma_0$. Assuming α_0 has a reduced predecessor, we have from (2)

$$\frac{\beta_0}{\beta_0^2+\gamma_0^2} < -u_{-1} \leq -1.$$

Thus $\gamma_0^2 < -\beta_0 - \beta_0^2$. For $-1 \leq x \leq 0$, the function $-x - x^2$ has maximum value $\frac{1}{4}$, so $|\gamma_0| < \frac{1}{2}$. This is a necessary condition for α_{-1}

to be reduced. Further,

$$\left|\frac{\gamma_{-1}}{\gamma_0}\right| = \frac{1}{\beta_0^2+\gamma_0^2} = \frac{\beta_{-1}-u_{-1}}{\beta_0} = \frac{u_{-1}-\beta_{-1}}{-\beta_0} > u_{-1} - \beta_{-1} > u_{-1}.$$

Hence $|\gamma_{-1}| > 2|\gamma_0|$ if $u_{-1} \geq 2$, and we may conclude that $|\gamma_{-2}| > 2|\gamma_0|$ unless both u_{-1} and $u_{-2} = 1$. In this case we can get a similar inequality as follows:

$$-\beta_{-1} = \frac{u_{-2}-\beta_{-2}}{(u_{-2}-\beta_{-2})^2+\gamma_{-2}^2} > \frac{u_{-2}-\beta_{-2}}{(u_{-2}-\beta_{-2})^2+(u_{-2}-\beta_{-2})} \quad \text{since } \gamma_{-2}^2 < \frac{1}{4} < u_{-2} - \beta_{-2}.$$

Thus $-\beta_{-1} > \frac{1}{u_{-2}-\beta_{-2}+1} > \frac{1}{3}$, and so $\left|\frac{\gamma_{-1}}{\gamma_0}\right| > u_{-1} - \beta_{-1} > \frac{4}{3}$. Since $|\gamma_{-2}| > |\gamma_{-1}|$, we have $|\gamma_{-2}| > \frac{4}{3}|\gamma_0|$. Eventually, $|\gamma_{-m}| > \frac{1}{2}$ for some m, and at that point there are no more reduced predecessors. This completes the proof of the theorem.

Part three of Theorem 1.2 shows that there exist numbers which are reduced, but have no reduced predecessor. These numbers are of central importance in everything that follows.

Definition. Let $\bar{\alpha}$ be a real algebraic number of degree at least three. We say $\bar{\alpha}$ is an ancestor if $\bar{\alpha}$ is reduced but has no reduced predecessor.

Corollary 1.3. Let α be a real algebraic number of degree at least three. Then α is equivalent to exactly one ancestor.

Proof. From Theorem 1.2, we know $\alpha \sim \alpha_k$ with α_k reduced. Let η_{k-1} be the reduced immediate predecessor of α_k (if there is one), and η_{k-2} the reduced immediate predecessor of η_{k-1}, and so on. We know by part three of Theorem 1.2 that this process will stop after finitely many steps and so we will arrive at an ancestor $\bar{\alpha}$ which is equivalent to α. Suppose that $\alpha \sim \bar{\bar{\alpha}}$ also, where $\bar{\bar{\alpha}}$ is a different ancestor. Then $\bar{\alpha} \sim \bar{\bar{\alpha}}$, so their continued fractions have the form $\bar{\alpha} = [u_0, u_1, \ldots, u, \zeta]$ and $\bar{\bar{\alpha}} = [v_0, v_1, \ldots, v, \zeta]$ where $u \neq v$ and ζ is reduced. This implies that $u + \frac{1}{\zeta}$ and $v + \frac{1}{\zeta}$ both are reduced immediate predecessors of ζ, in contradiction to part two of Theorem 1.2.

Example. Let $\alpha = \sqrt[3]{r}$ where $r \in Q$ and $1 < r < 8$. The conjugates of α are $\beta \pm i\gamma$, where $\beta = -\frac{1}{2}\alpha$. α is reduced exactly when $-1 < \beta < 0$, i.e, $1 < \alpha < 2$, which is satisfied. Further, $|\gamma| = \frac{\sqrt{3}}{2}\alpha > \frac{\sqrt{3}}{2} > \frac{1}{2}$, so α is in fact an ancestor.

The lemma which follows allows for a relatively easy determination of the partial quotients of reduced immediate predecessors. It is superior to (2) in that a precise knowledge of the conjugates is not required.

Lemma 1.4. Let α_1 be a reduced number, and let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be its minimal polynomial over Z. If $\alpha = u + \frac{1}{\alpha_1}$ is reduced, then

$$u < \frac{1}{n-1}\left(\frac{a_1}{a_0} + \frac{1}{\alpha_1}\right) < u + 1.$$

Proof. From the formulas which relate the coefficients of f to its roots we have

$$\frac{-a_1}{a_0} = \frac{1}{\alpha_1} + \frac{1}{\alpha_1^{(2)}} + \cdots + \frac{1}{\alpha_1^{(n)}} .$$

If α is reduced, then from (2) $u < \frac{-1}{\alpha_1^{(k)}} < u + 1$ for each real conjugate of α_1, and for a pair of complex conjugates $\beta \pm i\gamma$ we have $2u < \frac{-2\beta}{\beta^2+\gamma^2} < 2(u+1)$. Since $\frac{-2\beta}{\beta^2+\gamma^2} = \frac{-1}{\beta+i\gamma} + \frac{-1}{\beta-i\gamma}$, we have

$$(n-1)u < \frac{-1}{\alpha_1^{(2)}} + \cdots + \frac{-1}{\alpha_1^{(n)}} < (n-1)(u+1).$$

The result follows.

Example 1. Let η_0 be the real root of $f_0(x) = x^3 + 3x + 2$; the other two roots are complex. We will find the ancestor equivalent to η_0. As $-1 < \eta_0 < 0$, $u_0 = -1$ and η_0 is not reduced. Setting $\eta_0 = -1 + \frac{1}{\eta_1}$, we have that η_1 is the real root of $f_1(x) = 2x^3 - 6x^2 + 3x - 1$. Now $2 < \eta_1 < 3$ and $\eta_1 + 2\beta_1 = 3$, so $\beta_1 > 0$, and η_1 is not reduced. $\eta_1 = 2 + \frac{1}{\eta_2}$ where η_2 is a root of $f_2(x) = 3x^3 - 3x^3 - 6x - 2$. Now $2 < \eta_2 < 3$ and $\eta_2 + 2\beta_2 = 1$, so $-1 < \beta_2 < -\frac{1}{2}$, and thus η_2 is reduced. We need to see if η_2 has a reduced immediate predecessor. According to Lemma 1.4, if $u + \frac{1}{\eta_2}$ is reduced, then $u = [\frac{1}{2}(3+\frac{1}{\eta_2})] = 1$. Let $\alpha_1 = 1 + \frac{1}{\eta_2}$; it is a root of $2x^3 - 3x - 2$. $\alpha_1 + 2\beta_1 = 0$ and $1 < \alpha_1 < 2$, so α_1 is reduced (actually, the condition in Lemma 1.4 is both necessary and sufficient, if $u \geq 1$, in the case of cubic non-totally real numbers). Applying the lemma again, if $u + \frac{1}{\alpha_1}$ is reduced then $u = [\frac{1}{2}(\frac{3}{2}+\frac{1}{\alpha_1})] = 1$. Let $\alpha_0 = 1 + \frac{1}{\alpha_1}$; it is a root of $2x^3 - 3x^2 - 1$. As $\alpha_0 + 2\beta_0 = \frac{3}{2}$ and $\alpha_0 = [1,1,\eta_2]$ we have $\frac{3}{2} < \alpha_0 < 2$ and thus α_0 is reduced. Finally, if $u + \frac{1}{\alpha_0}$ is reduced then $u = [\frac{1}{2}(0+\frac{1}{\alpha_0})] = 0$, but a reduced number must be greater than one. So α_0 is an ancestor, and is the ancestor equivalent to η_0. We have $\eta_0 = [-1,2,\eta_2]$ and $\alpha_0 = [1,1,\eta_2]$, so the relationship between η_0 and its ancestor α_0 is $\eta_0 = \frac{-1}{\alpha_0}$.

Example 2. Let $\zeta = \sqrt[3]{6}$ and let α_0 be the real root of $2x^3 + 12x^2 + 24x + 13$; we want to determine whether or not $\alpha_0 \sim \zeta$. The discriminants of the polynomials satisfied by α_0 and ζ both are -972, so this by itself is inconclusive. We will resolve the question by finding the ancestors equivalent to α_0 and ζ. Now ζ already is an ancestor, as verified in an earlier example. For α_0, we follow the same procedure as in example 1 above. First, $-1 < \alpha_0 < 0$, so α_0 is not reduced. Setting $\alpha_0 = -1 + \frac{1}{\alpha_1}$, we find that α_1 is a root of $x^3 - 6x^2 - 6x - 2$, and $6 < \alpha_1 < 7$. Since $\alpha_1 + 2\beta_1 = 6$, we have $-\frac{1}{2} < \beta_1 < 0$, and α_1 is reduced. By Lemma 1.4, if $u + \frac{1}{\alpha_1}$ is reduced, then $u = [\frac{1}{2}(3+\frac{1}{\alpha_1})] = 1$. Let $\overline{\alpha} = 1 + \frac{1}{\alpha_1}$; we find that $\overline{\alpha}$ satisfies $2x^3 - 3$, i.e., $\overline{\alpha} = \sqrt[3]{\frac{3}{2}}$, which not only is reduced, but is an ancestor, according to an earlier example. As $\overline{\alpha} \neq \zeta$, we see that $\alpha_0 \not\sim \zeta$.

We conclude this chapter with some brief comments as to the effectiveness of this method of determining whether or not two real algebraic numbers are equivalent (that is, by comparing their ancestors.) Theorem 1.2 shows that we arrive at the ancestor of a given number α after finitely many steps -- forward to the first reduced successor α_k, and backwards to the ancestor $\overline{\alpha}$. However, the theorem does not give an explicit bound on the number of steps involved, although this is to some extent implicit in the proof. It is clear that in general arbitrarily many steps may be required; for example let $\overline{\alpha}$ be an ancestor, and let $\alpha = [u_{-m}, u_{-m+1}, \ldots, u_{-1}, \bar{\alpha}]$ where each u_j is a positive integer. In general the number of steps required depends on how close the conjugates of α are to each other and to α. Before we give precise bounds on the number of steps, it is helpful first to prove the following lemma:

Lemma 1.5. Let x and y be two distinct real irrational numbers. Then the number of places their continued fractions can agree is bounded by $\frac{-2\log|x-y|}{\log\frac{9}{4}} + 1$.

Proof. Let $x = [u_0, u_1, u_2, \ldots]$ and $y = [v_0, v_1, v_2, \ldots]$, and assume the continued fractions agree to several places. Then

$$|x_1 - y_1| = \left|\frac{1}{x-u_0} - \frac{1}{y-u_0}\right| = \frac{|x-y|}{|x-u_0||y-u_0|} = |x_1 y_1||x-y| > \left(u_1 + \frac{1}{u_2+1}\right)^2 |x-y|.$$

In particular, $|x_1-y_1| > |x-y|$. Similarly,

$|x_2-y_2| > (u_1 + \frac{1}{u_2+1})^2 (u_2 + \frac{1}{u_3+1})^2 |x-y|$. Thus $|x_2-y_2| > 4|x-y|$ unless $u_1 = u_2 = 1$. But then we have $|x_2-y_2| > \frac{9}{4}|x-y|$, so this inequality holds in any event. By induction, $|x_{2n}-y_{2n}| > (\frac{9}{4})^n |x-y|$, as long as the continued fractions of x and y agree to this point. We know that if $|x_k - y_k| > 1$ for some k, then $u_k \neq v_k$. This will be guaranteed if k is large enough -- specifically, if $k > \frac{-2\log|x-y|}{\log\frac{9}{4}}$, as asserted.

This is certainly not the most precise result possible, but it is enough for our purposes. Let us consider now the number of steps needed to go from α_k, the first reduced successor of α, to $\bar{\alpha}$, its ancestor. If α_k has a complex conjugate $\beta_k + i\gamma_k$, then we have $|\gamma_{k-2}| > \frac{4}{3}|\gamma_k|$, from the proof of Theorem 1.2. When $|\gamma_j| > \frac{1}{2}$ the chain stops, so this gives an explicit bound on the number of steps in terms of $|\gamma_k|$. Specifically, the number of steps is bounded by $\frac{-2\log 2|\gamma_k|}{\log\frac{4}{3}}+1$. If α_k has two real conjugates $\alpha_k^{(2)}$ and $\alpha_k^{(3)}$ then reduced immediate predecessors continue only as long as $\frac{-1}{\alpha_k^{(2)}}$ and $\frac{-1}{\alpha_k^{(3)}}$ have the same continued fractions. Thus, by virtue of Lemma 1.5, one may bound the number of steps in terms of $\left|\frac{1}{\alpha_k^{(2)}}-\frac{1}{\alpha_k^{(3)}}\right|$.

The problem of how many steps are required to reduce α to α_k is more difficult. For a real conjugate, say, $\alpha^{(2)}$, this depends on $|\alpha-\alpha^{(2)}|$, and again Lemma 1.5 will provide an explicit bound. For a complex conjugate it was necessary in proving Theorem 1.2 to appeal to the fact that α has infinitely many partial quotients ≥ 2 in its continued fraction. More precisely, we needed the product of the first m partial quotients to be larger than a bound which depends on the imaginary part of the conjugate of α. It is at this point that the argument is not effective, since it is not clear how many partial quotients are needed to make this product big enough.

Chapter 2. Characterizations of Ancestors

In this chapter we prove several results which help to identify when a reduced number is an ancestor. They serve as preparation for Theorem 2.9, which asserts that the set of all ancestors in a given real number field of degree at least three is dense in $[1,\infty)$. We begin with a series of results which answer the following question: If α is not reduced, when is the first reduced successor of α an ancestor?

Proposition 2.1. Let α be a real algebraic number of degree at least three, and not reduced. Let α_k be its first reduced successor, and let $v = [\alpha_{k-1}]$. Then α_k is not an ancestor if and only if there exists $N \leq v - 2$ in Z such that $N < \text{Re}\,\alpha'_{k-1} < N + 1$ for each conjugate α'_{k-1} of α_{k-1} distinct from α_{k-1}.

Proof. We have $\alpha_{k-1} = v + \frac{1}{\alpha_k}$ and α_{k-1} is not reduced. Let $\zeta = u + \frac{1}{\alpha_k}$. α_k is not an ancestor if and only if ζ is reduced for some choice of u, i.e., $u \geq 1$ and $-1 < \text{Re}\,\zeta' < 0$ for each conjugate $\zeta' \neq \zeta$. Let $N = v - u - 1$. The last conditions are equivalent to $N \leq v - 2$ and $N < \text{Re}\,\alpha'_{k-1} < N + 1$. Conversely, if such N exists, let $u = v - N - 1$ and then $\zeta = u + \frac{1}{\alpha_k}$ will be reduced.

Corollary 2.2. Let α be as above, and assume $\alpha > 1$. Suppose that α has one conjugate $\alpha^{(2)}$ with $\text{Re}\,\alpha^{(2)} \geq 0$ and another, $\alpha^{(3)}$, with $\text{Re}\,\alpha^{(3)} \leq 0$. Then the first reduced successor of α is an ancestor.

Proof. If α_1 is reduced, it is an ancestor by Proposition 2.1. Otherwise, $-1 < \text{Re}\,\alpha_1^{(3)} < 0$ and some other conjugate has real part outside this range. Further non-reduced successors will have the same property. Then Proposition 2.1 implies the desired result.

For example, let $\alpha = \sqrt[n]{q}$ where $q \in Q$, $q > 1$, $n \geq 4$, and α has degree n over Q. Then α satisfies the conditions of Corollary 2.2, so the first reduced successor of α is an ancestor (note that α itself is not reduced). One may consider the question of how many steps are necessary to reduce such an α. Let t_n be the maximum number of steps required to reduce an nth root $\alpha > 1$. The following table gives the first few values of t_n:

n	4	5	6	7	8
t_n	1	1	1	2	2

We prove the result for $n = 4, 5, 6$. As n increases, the computations get more and more tedious, and are not particularly enlightening. So let $\alpha = \sqrt[n]{q}$, as above, where $n \leq 6$. Any conjugate of α with real part ≤ 0 trivially reduces in one step; thus we need only consider what happens to the conjugate $\beta + i\gamma = \alpha\rho = \alpha e^{\frac{2\pi i}{n}} = \alpha \cos \frac{2\pi}{n} + i\alpha \sin \frac{2\pi}{n}$ where $n = 5$ or 6. From (1) of chapter one we have

$$\beta_1 = \frac{\beta - u}{(\beta-u)^2+\gamma^2} \qquad (u = [\alpha])$$

$\beta = \alpha \cos \frac{2\pi}{n} \leq \frac{1}{2}\alpha$, so $\beta < u$ and $\beta_1 < 0$. We show $\beta_1 > -1$ by showing that the denominator is greater than the absolute value of the numerator. $(\beta-u)^2 + \gamma^2 - |\beta-u| = (\beta-u)^2 + \gamma^2 + \beta - u =$

$$(\alpha \cos \frac{2\pi}{n} - u)(\alpha \cos \frac{2\pi}{n} - u + 1) + \alpha^2 \sin^2 \frac{2\pi}{n} =$$

$$\alpha^2 + \alpha \cos \frac{2\pi}{n}(1-2u) + u^2 - u = \alpha(\alpha + \cos \frac{2\pi}{n}(1-2u)) + u(u-1).$$

Now $u(u-1) \geq 0$ and $\alpha + \cos \frac{2\pi}{n}(1-2u) \geq \alpha + \frac{1-2u}{2} = \alpha - u + \frac{1}{2} > 0$.

Thus $\beta_1 > -1$, and so α_1 is reduced, as claimed.

It is easy to see that $\sqrt[n]{2^n-1}$ takes at least two steps for $n \geq 7$, since $\beta_1 > 0$ in the notation above; this shows that $t_n \geq 2$ if $n \geq 7$. In fact, it is not difficult to show that $t_n \to \infty$ as $n \to \infty$. We argue as follows: Let $\alpha = \sqrt[N]{q}$ where $q \in Q$ and α is sufficiently close to $\theta = \frac{1+\sqrt{5}}{2} = [1,1,1,\ldots]$. Let $\beta + i\gamma = \alpha\rho = \alpha \cos \frac{2\pi}{N} + i\alpha \sin \frac{2\pi}{N}$; by taking N large we make γ small and β arbitrarily close to α (and θ, for appropriate choice of q). We can show by induction that β_n is still close to θ if N is large enough, and α is close enough to θ. From (1) of chapter one we have

$$|\gamma_{n+1}| < \frac{|\gamma_n|}{(\beta_n-u_n)^2} .$$

Now if α is close enough to θ, the first M partial quotients of α are ones, for M arbitrarily large (this depends on q). If $\beta_n > \frac{3}{2}$, then $|\gamma_{n+1}| < 4|\gamma_n|$; hence by induction if $\beta_0, \beta_1, \ldots, \beta_n > \frac{3}{2}$, then $|\gamma_{n+1}| < 4^{n+1}|\gamma_0|$. Again from (1) of chapter one we have

$$\beta_{n+1} = \frac{\beta_n - u_n}{(\beta_n-u_n)^2+\gamma_n^2} .$$

Let $\beta_n = \theta + \delta_n$, and assume $u_0 = u_1 = \cdots = u_n = 1$. Then

$$\beta_{n+1} - \theta = \frac{(\beta_n-1)(1-\theta(\beta_n-1))-\theta\gamma_n^2}{(\beta_n-1)^2+\gamma_n^2} = \frac{-\theta(\gamma_n^2+\delta_n(\theta-1+\delta_n))}{(\beta_n-1)^2+\gamma_n^2} ,$$

and so $|\delta_{n+1}| < \dfrac{\theta(\gamma_n^2+\delta_n(\theta-1+\delta_n))}{(\theta-1+\delta_n)^2}$. If $|\delta_n| < \theta - \frac{3}{2}$, then $\theta - 1 + \delta_n > \frac{1}{2}$, and thus $|\delta_{n+1}| < \theta(4\gamma_n^2+2|\delta_n|) < 4(2\gamma_n^2+|\delta_n|)$. Now if $|\delta_0| < \gamma_0^2$ (choice of q), and $|\gamma_0|$ is small enough (choice of N), then $|\gamma_1| < 4|\gamma_0|$, and $|\delta_1| < 4(3\gamma_0^2) < 16\gamma_0^2 = 4^2\gamma_0^2$. Thus $|\delta_2| < 4(32\gamma_0^2 + 16\gamma_0^2) < 16^2\gamma_0^2 = 4^4\gamma_0^2$. In general, $|\delta_n| < 4^{2n}\gamma_0^2$ if $|\gamma_0|$ is small enough. Thus given k and $\varepsilon > 0$, by taking N large enough and q appropriately, we can insure $|\delta_k| < \varepsilon$, so $\beta_k > 1$ and α_k is not reduced yet. Hence at least k steps are required to reduce α.

We return now to the previous discussion. The next result is in some sense a strengthening of Corollary 2.2.

Corollary 2.3. Let α be as in Proposition 2.1. Suppose that α has one conjugate $\alpha^{(2)}$ with real part $\geq u$ and another, $\alpha^{(3)}$, with real part $\leq u$, where $u = [\alpha]$. Then the first reduced successor of α is an ancestor.

Proof. The corresponding conjugates $\alpha_1^{(2)}$ and $\alpha_1^{(3)}$ satisfy $\text{Re}\,\alpha_1^{(2)} \geq 0$ and $\text{Re}\,\alpha_1^{(3)} \leq 0$. As $\alpha_1 > 1$ is not reduced, we may apply Corollary 2.2.

Definition. We say that α has "dispersed conjugates" if there is no integer N such that $N < \text{Re}\,\alpha' < N + 1$ for the conjugates α' distinct from α.

Proposition 2.4. If $\overline{\alpha}$ is an ancestor with at least one real conjugate, then any immediate predecessor to $\overline{\alpha}$ has dispersed conjugates.

Proof. Let $\zeta = u + \frac{1}{\overline{\alpha}}$ be one such immediate predecessor. We know ζ is not reduced. Suppose that $N < \text{Re}\,\zeta' < N + 1$ for each conjugate ζ'. Then $N \leq u - 1$, or else $\overline{\alpha}$ would not be reduced. Further, if $N = u - 1$, then the real conjugate of $\overline{\alpha}$ would be less than -1. So

$N \leq u - 2$. But then Proposition 2.1 implies that $\bar{\alpha}$ is not an ancestor. So no such N exists.

Theorem 2.5. Let α be a real algebraic number of degree at least three over Q, and not reduced. Suppose α has dispersed conjugates and that $\text{Re}\ \alpha' < \alpha$ for the conjugates α' distinct from α. Then the first reduced successor of α is an ancestor.

Proof. Let $u = [\alpha]$. If $\text{Re}\ \alpha' \geq u$ for each conjugate, then equality must hold for one of them, since the conjugates are dispersed. Thus, say, $\text{Re}\ \alpha^{(2)} = u$ and $\text{Re}\ \alpha^{(3)} \geq u$. Then Corollary 2.3 implies the result. Again, if there are two conjugates, one with real part $\leq u$ and one with real part $\geq u$, the same corollary applies. Thus we may assume $\text{Re}\ \alpha' < u$ for each conjugate. Since the conjugates are dispersed, we have $\text{Re}\ \alpha' \leq u - 1$ for at least one conjugate, say, $\alpha^{(2)}$. This implies that $-1 < \text{Re}\ \alpha_1^{(2)} < 0$. Now if α_1 is reduced, it is an ancestor, by Proposition 2.1. If α_1 is not reduced, then the real part of some conjugate lies outside the interval $(-1,0)$. Further non-reduced successors will have the same property; Proposition 2.1 then implies the desired result.

Example. Let $f(x) = x^4 - 14x^2 + 9$; f is irreducible over Q, and its roots are $\pm\alpha$ and $\pm\beta$, where $\alpha = \sqrt{5} + \sqrt{2}$ and $\beta = \sqrt{5} - \sqrt{2}$. As $\alpha \sim -\alpha$, they have the same ancestor; the same is true, of course, for β and $-\beta$. We will find the ancestors for α and β. α satisfies the conditions of Corollary 2.2, and β those of Corollary 2.3. Alternatively, we may apply Theorem 2.5 to α. At any rate, in each case the first reduced successor is an ancestor. Following their continued fractions, we have $\alpha = [3,\alpha_1]$ and $\beta = [0,1,4,\beta_3]$ where α_1 and β_3 are ancestors. They satisfy the polynomials $36x^4 - 24x^3 - 40x^2 - 12x - 1$ and

$281x^4 - 284x^3 - 248x^2 - 56x - 4$, respectively. An immediate consequence is that $\alpha \not\sim \beta$, although this could have been determined by other means as well.

Let K be a real but not totally real field of degree three over Q, and let α be an irrational in K. Denote the conjugates of α by $\beta \pm i\gamma$. Since $\alpha + 2\beta \in Q$, we know β cannot be an integer, and so α never will have dispersed conjugates -- we have $N < \beta < N + 1$, where $N = [\beta]$. Suppose that α is not reduced but α_1 is. Then we must have $N \leq [\alpha] - 1$, or else $\beta_1 > 0$ (from (1) of chapter one). Now Proposition 2.1 says that α_1 is an ancestor if and only if $N = [\alpha] - 1$, i.e., $N < \beta < N + 1 < \alpha < N + 2$ for some N. If we replace α by $\alpha - N$ this does not change α_1, and has the effect of normalizing $N = 0$. This suggests looking at the following sets:

$$S = \{\alpha \in K - Q \mid 1 < \alpha < 2 \text{ and } 0 < \beta < 1, \text{ where } \beta = \operatorname{Re} \alpha'\}$$

$$T = \{\alpha \in S \mid \alpha_1 \text{ is reduced}\}.$$

The argument above shows that if $\alpha_1 \in K$ is an ancestor, then $\alpha = 1 + \frac{1}{\alpha_1} \in T$. Thus, the immediate successors of elements of T are exactly the ancestors in K. The set T forms a useful canonical set of immediate predecessors for ancestors in this type of field. The set $S - T$ has a simple characterization:

<u>Proposition 2.6</u>. $\alpha \in S - T$ if and only if $\alpha = [1, M, \eta_k]$, where η_0 is an ancestor, $k \geq 1$, and $M < w = [\eta_{k-1}]$. In other words, α reduces in two steps, and its first reduced successor is not an ancestor.

<u>Proof</u>. Let α be in $S - T$. Then $\alpha = 1 + \frac{1}{\alpha_1}$ where α_1 is not reduced. Since $0 < \beta < 1$, we have $\beta_1 < 0$ and so $\beta_1 < -1$ since

α_1 is not reduced. Now α_2 is reduced regardless of the next partial quotient; further, α_2 is not an ancestor, by Proposition 2.1. So $\alpha_2 = \eta_k$ where η_k is as in the statement of the proposition. Thus α has the form $[1,M,\eta_k]$ where we know as yet only that $M \neq w$. Now let $\alpha = [1,M,\eta_k]$, and determine conditions on M so that $\alpha \in S - T$. Let $\eta_k' = \mu + i\nu$ and let $\beta = \mathrm{Re}\,\alpha'$. We have $[1,M,\eta_k] = 1 + \frac{\eta_k}{M\eta_k+1}$, so

$$\alpha' = 1 + \frac{\mu + i\nu}{(M\mu+1)+iM\nu} \quad \text{and} \quad \beta = 1 + \frac{M\mu^2+\mu+M\nu^2}{(M\mu+1)^2+M^2\nu^2}.$$

Since η_k is not an ancestor, we have $w < \frac{-\mu}{\mu^2+\nu^2} < w + 1$, where $w = [\eta_{k-1}]$ and η_{k-1} is the reduced immediate predecessor of η_k (from (2) of chapter one). We may rewrite this inequality as

$$(1) \quad (\mu^2+\nu^2)w + \mu < 0 < \mu + (w+1)(\mu^2+\nu^2).$$

From (1) we see that $M(\mu^2+\nu^2) + \mu < 0$ if and only if $M \leq w$; thus $\beta < 1$ if and only if $M \leq w$. Now if $M = w$ then α_1 is reduced; so we have proved that $\alpha \in S - T$ implies $\alpha = [1,M,\eta_k]$ with $M < w$. Finally, if α has this form and $M < w$, then α_1 is not reduced and $\beta < 1$. It remains only to show that $\beta > 0$ to conclude that $\alpha \in S - T$. From (2) of chapter one we have $w < \frac{-\mu}{\mu^2+\nu^2} < \frac{-\mu}{\mu^2}$, so $\mu > \frac{-1}{w}$; this combined with the fact that $M < w$ shows that $M\mu + 1 > 1 - \frac{M}{w} > 0$. Thus $|M\mu+1| - |\mu| = M\mu + 1 + \mu = 1 + (M+1)\mu > 1 - \frac{M+1}{w} \geq 0$, and so $|\mu| < M\mu+1$. Then $|M\mu^2+\mu+M\nu^2| \leq |M\mu^2+\mu| + M\nu^2 < (M\mu+1)^2 + M^2\nu^2$, so we have

$$-1 < \frac{M\mu^2+\mu+M\nu^2}{(M\mu+1)^2+M^2\nu^2} < 0.$$

This implies $0 < \beta < 1$, as desired.

One conclusion we may draw from this is that there are infinitely many numbers in $S - T$. Any ancestor η_0 has infinitely many partial quotients >1; thus $S - T$ contains numbers of the form $[1,1,\eta_k]$ where $[\eta_{k-1}] \geq 2$. One may define analogous sets to S and T for any real number field of degree ≥ 3, although in this case not all ancestors arise as immediate successors of numbers from T. (Proposition 2.4 sheds some light on this question). However, the characterization of $S - T$ remains the same.

The rest of this chapter is devoted to proving Theorem 2.9, which states that the set of all ancestors in a real number field of degree at least three is dense in $[1,\infty)$. The only really difficult case occurs for non-totally real cubic fields; in such a case we will make use of the set T defined above.

<u>Lemma 2.7</u>. Let $K = Q(\zeta)$ where ζ is real and $|K:Q| \geq 3$. Further, assume that K is totally real if $|K:Q| = 3$. Then some reduced successor of ζ has two conjugates with distinct real parts.

<u>Proof</u>. By Theorem 1.2 we know ζ has a reduced successor, say, ζ_k. If ζ_k does not have the property desired, we will show that ζ_{k+1} does. Now ζ_k must have two conjugates, say $\zeta_k^{(2)}$ and $\zeta_k^{(3)}$, which are not complex conjugates of each other (this follows by assumption of the nature of K). If $\mathrm{Re}\,\zeta_k^{(2)} \neq \mathrm{Re}\,\zeta_k^{(3)}$ we are done. Otherwise, since $|\mathrm{Im}\zeta_k^{(2)}| \neq |\mathrm{Im}\zeta_k^{(3)}|$, we will have $\mathrm{Re}\,\zeta_{k+1}^{(2)} \neq \mathrm{Re}\,\zeta_{k+1}^{(3)}$, by (1) of chapter one.

<u>Lemma 2.8</u>. Let K be a real but not totally real field of degree 3 over Q. Then $K = Q(\zeta)$ where ζ satisfies an equation of the form $\zeta^3 + a\zeta - b = 0$, where a and $b \in Z$, $b > 0$, and if $a < 0$ then

$\frac{b}{|a|\zeta} > \frac{1}{3}$.

Proof. Let α be a generator for K, and let $a_3x^3 + a_2x^2 + a_1x + a_0$ be its minimal polynomial over Z. Then $\beta = \alpha + \frac{a_2}{3a_3}$ satisfies a polynomial of the form $b_3x^3 + b_1x + b_0$; let $\zeta = b_3\beta$. Then ζ satisfies a polynomial of the form $x^3 + ax - b$ where $a,b \in Z$. We may replace ζ by $-\zeta$ if necessary to assume $b > 0$. If $a \geq 0$ this polynomial will have only one real root, as needed. If $a < 0$, the polynomial will have only one real root if and only if it takes on a negative value at the local maximum $x = -\sqrt{\frac{-a}{3}}$ (since the value at 0 is negative). At $-\sqrt{\frac{-a}{3}}$, the polynomial is $\frac{a}{3}\sqrt{\frac{-a}{3}} - a\sqrt{\frac{-a}{3}} - b = \frac{-2a}{3}\sqrt{\frac{-a}{3}} - b$. This is negative if and only if $b^2 > \frac{-4a^3}{27}$. This is equivalent to the statement in the lemma; for $\zeta < \frac{-3b}{a}$ if and only if the polynomial is positive at $\frac{-3b}{a}$, which happens if and only if $b^2 > \frac{-4a^3}{27}$.

Theorem 2.9. Let $K = Q(\zeta)$ be a real number field of degree at least three over Q. Then the ancestors in K are dense in $[1,\infty)$.

Proof. There are four cases to consider.

Case 1: K is not a non-totally real cubic field. Then take ζ as in Lemma 2.7; that is, ζ is reduced and at least two conjugates of ζ have different real parts, say, $\zeta^{(2)}$ and $\zeta^{(3)}$. Let θ be an arbitrary real number in (1,2), and set $\alpha = r\zeta + t$ where r and t are rational numbers to be determined so that α is close to θ and $\frac{1}{\alpha-1} = \alpha_1$ is an ancestor. This will prove density of ancestors in $[1,\infty)$. Select $r \in Q$ so that

$$r > \frac{2}{\zeta} \quad \text{and} \quad r > \frac{1}{|\mathrm{Re}\,\zeta^{(2)} - \mathrm{Re}\,\zeta^{(3)}|}.$$

Define κ by $r\zeta = (1+\kappa)\theta$; since $r\zeta > 2$, $\kappa > 0$. Let $t = -\kappa\theta + \varepsilon$ where ε is small and chosen so that $t \in Q$. Then $t < 0$. $\alpha = r\zeta + t = \theta + \varepsilon$, and the choice of r insures that α has dispersed conjugates; $|\alpha^{(2)} - \alpha^{(3)}| > 1$. $\text{Re}\,\alpha^{(k)} = r\text{Re}\,\zeta^{(k)} + t < 0$ for $k \neq 1$; since $[\alpha] = 1$ we have $-1 < \text{Re}\,\alpha_1^{(k)} < 0$, and so α_1 is reduced. Then α_1 is an ancestor, by Proposition 2.1. As ε is arbitrarily small, the result follows.

Case 2: K is a non-totally real cubic field with $a \geq 0$ in Lemma 2.8. Let ζ be a generator for K as in Lemma 2.8. It will suffice to prove that T is dense in (1,2). Denote the conjugates of ζ by $\mu \pm i\nu$. We have $\mu = -\frac{\zeta}{2}$ and $\zeta(\mu^2+\nu^2) = b$ which implies

$$\nu^2 = \frac{b-\frac{1}{4}\zeta^3}{\zeta} = \frac{4b-\zeta^3}{4\zeta} = \frac{3b+a\zeta}{4\zeta}.$$

Let $\alpha = r\zeta + t$ where r and t are to be chosen in Q, and denote the conjugates of α by $\beta \pm i\gamma$. Then $\beta = -\frac{r\zeta}{2} + t$ and $\gamma = r\nu$. Now if $\alpha \in S$ and $|\gamma| \geq \frac{1}{2}$ then $\alpha \in T$ (that is, α_1 is reduced). This follows from (1) of chapter one. Since $\nu^2 = \frac{3b+a\zeta}{4\zeta}$, we have

$$\frac{\zeta}{2\nu} = \frac{\zeta}{2}\sqrt{\frac{4\zeta}{3b+a\zeta}} = \sqrt{\frac{b-a\zeta}{3b+a\zeta}} \leq \frac{1}{\sqrt{3}}.$$

So if r is chosen so that $r\zeta > \frac{1}{\sqrt{3}}$, then $r > \frac{1}{2\nu}$ and $|\gamma| > \frac{1}{2}$ is assured.

Let θ be an arbitrary real number in (1,2), and set $r\zeta = \frac{3}{5}\theta + \varepsilon$ and $t = \frac{2}{5}\theta + \delta$ where ε and δ are small and chosen to make r and t rational. Then $r\zeta > \frac{3}{5} > \frac{1}{\sqrt{3}}$, $\alpha = \theta + \varepsilon + \delta$ is close to θ, and $\beta = \frac{1}{10}\theta + \delta - \frac{\varepsilon}{2}$ is between 0 and 1 if δ and ε are small enough. So $\alpha \in T$ and can be made arbitrarily close to θ.

Case 3: K is as in Case 2 except that $a < 0$, and restrict $b > |a|\zeta$. Renotate so that $a > 0$ and $\zeta^3 - a\zeta - b = 0$. Let $\mu \pm i\nu$ be the conjugates of ζ as before. We have $\mu = -\frac{\zeta}{2}$, and $\frac{\zeta}{2\nu} = \sqrt{\frac{b+a\zeta}{3b-a\zeta}}$. Also,

$$\nu^2 - \mu^2 = \frac{b-\frac{1}{4}\zeta^3}{\zeta} - \frac{\zeta^2}{4} = \frac{b-\frac{1}{2}\zeta^3}{\zeta} = \frac{b-a\zeta}{2\zeta} > 0.$$

Take $\theta \in (1,2)$ as before and let $\alpha = r\zeta^2 + t\zeta$ where again r and t are rationals to be determined. Notating as before, we have $\beta = r(\mu^2-\nu^2) + t\mu = \frac{-r}{2\zeta}(b-a\zeta) - \frac{t\zeta}{2}$ and $\gamma = -\nu(r\zeta-t)$. Take $r\zeta^2 = (1+\kappa)\theta + \delta$ and $t\zeta = -\kappa\theta + \varepsilon$ where $\kappa > 0$ is to be determined. Then $r > 0$ and $t < 0$ (for δ,ε small enough), so $|\gamma| > \nu r\zeta > \frac{1}{2}$ if $r\zeta^2 > \frac{\zeta}{2\nu}$. Now $\frac{\zeta}{2\nu} = \sqrt{\frac{b+a\zeta}{3b-a\zeta}} < 1$ since $b > a\zeta$. Thus $|\gamma| > \frac{1}{2}$ if $r\zeta^2 > 1$; this will be assured if $\kappa > 0$. So we need only determine κ so that $\kappa > 0$ and $0 < \beta < 1$; we have assured that α is close to θ. Let $\sigma = \frac{b-a\zeta}{b+a\zeta}$; then $0 < \sigma < 1$. We have

$$\beta = -\frac{r\zeta^2\sigma}{2} - \frac{t\zeta}{2} = -\frac{\sigma\theta(1+\kappa)}{2} + \frac{\kappa\theta}{2} + \text{error terms}.$$

To get $\beta > 0$, we need $\kappa > \sigma(1+\kappa)$, i.e., $\kappa > \frac{\sigma}{1-\sigma}$ (for δ,ε small enough). Similarly, $\beta < 1$ if $\kappa\theta - \sigma\theta(1+\kappa) < 2$, i.e., $\kappa < \frac{\frac{2}{\theta}+\sigma}{1-\sigma}$. Thus $0 < \beta < 1$ if we take κ so that

$$\frac{\sigma}{1-\sigma} < \kappa < \frac{\frac{2}{\theta}+\sigma}{1-\sigma}.$$

Now σ is fixed, and this interval is non-empty, so such κ exists. Thus $\alpha \in T$, and so T is dense in $(1,2)$.

Case 4: K is as in Case 3, except that $\frac{1}{3} < \frac{b}{a\zeta} < 1$. Let $\sigma = \frac{-b+a\zeta}{b+a\zeta}$ and $\tau = \frac{b+a\zeta}{3b-a\zeta}$. We have $0 < \sigma < \frac{1}{2}$ and $1 < \tau < \infty$. Take $\theta \in (1,2)$, and let $\alpha = r\zeta^2 + t\zeta + u$, where r, t, and $u \in Q$ are to be determined. Then $\beta = \frac{r\zeta^2\sigma}{2} - \frac{t\zeta}{2} + u$ and $\gamma = -\nu(r\zeta - t)$, so $|\gamma| > \frac{1}{2}$ for sure if $r\zeta^2 - t\zeta > \sqrt{T}$. Take $r\zeta^2 = (1+\kappa+\lambda)\theta + \delta_1$, $t\zeta = -\kappa\theta + \delta_2$, and $u = -\lambda\theta + \delta_3$ where κ and λ are to be determined, and each δ_j is small. Then

$$\beta = \frac{(1+\kappa+\lambda)\theta\sigma}{2} + \frac{\kappa\theta}{2} - \lambda\theta + \text{error terms.}$$

To get $\alpha \in T$, we need the three inequalities $|\gamma| > \frac{1}{2}$, $\beta > 0$, and $\beta < 1$. For small enough δ_j, these translate to

$$\begin{aligned}
(1+2\kappa+\lambda)\theta &> \sqrt{T} \\
\lambda(2-\sigma) &< \sigma + \kappa(1+\sigma) \\
2 - \theta\sigma &> \theta(\kappa(\sigma+1)+\lambda(\sigma-2)).
\end{aligned}$$

Now take λ so that $\lambda(2-\sigma) = \sigma + \kappa(1+\sigma) - 1$. Then $\lambda > 0$ if κ is large enough. The second inequality is satisfied automatically; the third becomes $2 - \theta\sigma > \theta - \theta\sigma$, i.e., $\theta < 2$, which is satisfied. Finally, κ may be taken as large as necessary to satisfy the first inequality. This completes the proof.

Chapter 3. The Distribution of Ancestors Within an Ideal of a Real Number Field.

Theorem 2.9 shows that the ancestors within a real number field of degree at least three are dense in $[1,\infty)$. The purpose of this chapter is to investigate the distribution of ancestors when they are restricted to lie in a particular (fractional) ideal of a real number field. Primary interest is focused on the special case of the ideal of all algebraic integers in the field. One interesting point that arises is that there is a profound difference between the totally real fields and those which are real but not totally real. The really important distinction is that in a non-totally real field ancestors exist whose conjugates have arbitrarily large imaginary parts. Why this is important is revealed in Proposition 3.2.

Throughout this chapter K denotes a real number field of degree at least three over Q.

Proposition 3.1. Let α be reduced, but not an ancestor. Then $|\alpha'| < 1$ for the other conjugates of α.

Proof. If α' is real, the statement is obvious. So assume $\alpha' = \beta + i\gamma$, $\gamma \neq 0$. Let α_{-1} be the reduced immediate predecessor of α; $\alpha_{-1} = u_{-1} + \frac{1}{\alpha}$, say. Let $\beta_{-1} + i\gamma_{-1}$ be the conjugate corresponding to $\beta + i\gamma$, so $\beta_{-1} + i\gamma_{-1} = u_{-1} + \frac{1}{\beta+i\gamma}$. Thus $\beta = \frac{\beta_{-1} - u_{-1}}{(\beta_{-1}-u_{-1})^2+\gamma_{-1}^2}$ and $\gamma = \frac{-\gamma_{-1}}{(\beta_{-1}-u_{-1})^2+\gamma_{-1}^2}$. Hence

$$\beta^2 + \gamma^2 = \frac{1}{(\beta_{-1}-u_1)^2+\gamma_{-1}^2} < \frac{1}{(\beta_{-1}-u_{-1})^2} < 1 \text{ since } \beta_{-1} < 0 \text{ and } u_{-1} \geq 1.$$

In particular, if α is an algebraic integer, it is a PV number (a PV number is an algebraic integer > 1 all of whose other conjugates have absolute value < 1). See [2] for more about the properties of PV numbers.

Proposition 3.2. Let A be an ideal of K. Then there can be only finitely many reduced non-ancestors from A in a bounded interval. If K is totally real, the same is true for reduced numbers in general.

Proof. Let q be a positive integer such that $(q)A$ is an integral ideal. Suppose that there are infinitely many of the numbers in some bounded interval. For each such number α, $q\alpha$ is an algebraic integer, and all of the conjugates of $q\alpha$ are bounded independently of α. Let p be a large prime in Z. Since there are only finitely many residue classes in $K \bmod p$, there must be two of the numbers in the sequence, say, α and β, such that $q\alpha \equiv q\beta \bmod p$. Then $\frac{q\alpha - q\beta}{p} \neq 0$ is an algebraic integer. But for p large enough, all of the conjugates of this number are less than one in absolute value. This is a contradiction.

From this result, we see that if K is totally real, every reduced number in the ideal A is isolated (bounded away from all other such numbers). Exactly the opposite is true if K is not totally real. To prove this, we need to use a theorem of Minkowski [2] on homogeneous linear forms. The version we will use is the following:

Theorem (Minkowski). Let $\sum_{j=1}^{n} a_{ij} x_j$ $(1 \leq i \leq m)$ be m linear forms in n variables, where $m < n$. Let $c_1, \ldots, c_m$ be m positive real numbers, no matter how small. Then there is a non-trivial integral solution $x_1, \ldots, x_n$ to the system

$$\left|\sum_{j=1}^{n} a_{ij} x_j\right| < c_i \quad \text{for} \quad 1 \leq i \leq m.$$

Theorem 3.3. Let A be an ideal in K, and assume K is not totally real. Then no reduced number in A is isolated.

Proof. Let a Z-basis for A be $\zeta_1, \ldots, \zeta_n$ where $n = |K:Q|$. Let the conjugates of ζ_k be denoted by $\zeta_k = \zeta_k^{(1)}, \zeta_k^{(2)}, \ldots, \zeta_k^{(n)}$, and let $\mu_k^{(m)} = \operatorname{Re} \zeta_k^{(m)}$. Let $\alpha = \sum_{j=1}^{n} a_j \zeta_j$ be a given reduced number in A ($a_j \in Z$). If we can find $c_1, \ldots, c_n \in Z$ such that $|\sum_{j=1}^{n} c_j \mu_j^{(k)}| < \varepsilon$ for $k = 1, 2, \ldots, n$ and $\varepsilon > 0$ arbitrarily small, then $\beta = \sum_{j=1}^{n} (a_j + c_j)\zeta_j$ will be reduced and as close to α as desired, if ε is small enough (each conjugate of β is within ε of the corresponding conjugate of α, in real part). Let $n = r + 2s$ where r is the number of real conjugates of a generator of K, and 2s the number of complex conjugates. To find the c_j, we need to satisfy simultaneously

$$|\sum_{j=1}^{n} c_j \zeta_j^{(k)}| < \varepsilon \quad \text{for} \quad k = 1, 2, \ldots, r$$

$$|\sum_{j=1}^{n} c_j \mu_j^{(k)}| < \varepsilon \quad \text{for} \quad k = r + 1, \ldots, r + s.$$

K is not totally real, so there are fewer conditions than variables; thus Minkowski's theorem guarantees that non-trivial solutions exist for any $\varepsilon > 0$.

Actually, we proved slightly more -- namely, that reduced numbers exist arbitrarily close on both sides of α. To see this, simply observe that if $(c_1, \ldots, c_n)$ is a solution to the inequalities above, so is $(-c_1, \ldots, -c_n)$.

To insure that this theorem and related results are not vacuous, we prove the existence of reduced numbers in an ideal A in K. Again we make use of Minkowski's theorem, which has been used in a similar context by Salem [9], where it is proved that PV numbers exist in any real number field.

Proposition 3.4. Let A be an ideal in K. Then there exists a reduced number in A.

Proof. Clearly it suffices to assume A is an integral ideal, as the introduction of denominators merely adds more numbers to the ideal. Use the same notation for a Z-basis as in the previous theorem. In addition, denote $\zeta_j^{(k)} = \mu_j^{(k)} + i\nu_j^{(k)}$ for the complex conjugates $(k > r)$. First we find $a_1, \ldots, a_n \in Z$ so that $|\sum_{j=1}^{n} a_j\zeta_j^{(k)}| < 1$ for $k = 2, \ldots, n$. Certainly this will be true if

$$|\sum_{j=1}^{n} a_j\zeta_j^{(k)}| < 1 \quad \text{for} \quad k = 2, \ldots, r$$

$$|\sum_{j=1}^{n} a_j\mu_j^{(k)}| < \frac{1}{2} \quad \text{for} \quad k = r+1, \ldots, r+s$$

$$|\sum_{j=1}^{n} a_j\nu_j^{(k)}| < \frac{1}{2} \quad \text{for} \quad k = r+1, \ldots, r+s.$$

The number of conditions is $n - 1 < n$, so such $a_1, \ldots, a_n$ exist (not all zero). Let $\alpha = \sum_{j=1}^{n} a_j\zeta_j$. We have $\alpha \neq 0$ and $|\alpha^{(k)}| < 1$ for $k = 2, \ldots, n$, so $|\alpha| > 1$. Replace α by α^2 to assume $\alpha > 1$. There exists an integer $q > 0$ such that $A|(q)$; take p prime in Z large enough that $p > 2q$ and $(\alpha,p) = (1)$. Then $\alpha^m \equiv 1 \bmod p$ for some $m > 0$ in Z; thus $\beta = \frac{\alpha^{tm}-1}{p}$ is a reduced algebraic integer for each $t > 0$ in Z. Further, $q\beta \in A$ and $-1 < q\,\mathrm{Re}\,\beta^{(j)} < 0$ for $j = 2, \ldots, n$, i.e., $q\beta$ is a reduced number in A.

Note that by taking t arbitrarily large, we have proved that A

contains arbitrarily large reduced numbers.

Corollary 3.5. Let A be an ideal in K, and assume K is not totally real. Then there are ancestors in A, and the ancestors in A are not isolated.

Proof. This is immediate from Proposition 3.2, Theorem 3.3, and Proposition 3.4.

One question that has not yet been settled is whether or not there exists an ancestor in a given ideal of a totally real field. The existence, in fact, of infinitely many such ancestors is demonstrated in the following proposition.

Proposition 3.6. Let A be an ideal in K, where K is totally real. Then there are infinitely many ancestors in A.

Proof. Let α be a reduced algebraic integer in A; such an α exists by Proposition 3.4. If α has a conjugate between -1 and $-\frac{1}{2}$ and another between $\frac{-1}{2}$ and 0, then α must be an ancestor (by (2) of chapter one). If not, then all conjugates other than α itself lie between -1 and $-\frac{1}{2}$ or all lie between $-\frac{1}{2}$ and 0. In the first case, let $\alpha_1 = 2\alpha + 1$; in the second, let $\alpha_1 = 2\alpha$. In either case α_1 is a reduced algebraic integer, and the distance between the conjugates of α_1 is twice that for α. So eventually we will arrive at an ancestor by continuing this process. Thus K contains an integral ancestor.

Now let α be an integral ancestor in K, constructed as above so that $-\frac{1}{2}$ is between two of the conjugates, say, α' and α''. Let q be a positive integer such that $A|(q)$, and let k be a large odd integer. We assert that for k large enough, $q\alpha^k$ is an ancestor in A. Certainly $q\alpha^k \in A$, and is reduced for k large enough. We have $-1 < \alpha' < -\frac{1}{2} < \alpha'' < 0$. Let $\delta = |\alpha' - \alpha''|$. Now

$$|(\alpha')^k - (\alpha'')^k| = \delta((\alpha')^{k-1} + (\alpha')^{k-2}\alpha'' + \cdots + (\alpha'')^{k-1}) > \delta(\alpha')^{k-1} > \frac{\delta}{2^{k-1}}.$$

Now if $q(\alpha')^k$ and $q(\alpha'')^k$ both are between $\frac{-1}{M}$ and $\frac{-1}{M+1}$, then $M > \frac{2^k}{q} - 1$, since $\frac{q}{2^k}$ is between $|q(\alpha')^k|$ and $|q(\alpha'')^k|$. This implies that

$$\left|\frac{1}{M} - \frac{1}{M+1}\right| < \left|\frac{q}{2^k-q} - \frac{q}{2^k}\right| = \frac{q^2}{2^k(2^k-q)} .$$

This will produce a contradiction if

$$\frac{q\delta}{2^{k-1}} > \frac{q^2}{2^k(2^k-q)}, \quad \text{i.e.,}\ 2^k - q > \frac{q}{2\delta} ,$$

which is satisfied for all large k, as q and δ are fixed. Thus, if k is large enough the conjugates $q(\alpha')^k$ and $q(\alpha'')^k$ cannot lie in the same interval $(\frac{-1}{M}, \frac{-1}{M+1})$. This proves that $q\alpha^k$ is an ancestor. Since there are infinitely many k, and the numbers $q\alpha^k$ are distinct, there are infinitely many ancestors.

Thus in a totally real field there are infinitely many ancestors within a given ideal; however, they are all isolated, by Proposition 3.2. We turn now to a more detailed investigation of the case in which K is not totally real. From previous results we know that within any ideal A in K no ancestor is isolated. In fact, much more is true. In "most" cases (this will be made more precise later) the ancestors in A are dense in a collection of non-trivial intervals. The goal of this chapter is to prove this result, giving as precise sufficient conditions as possible, and also to determine these intervals where possible. In many cases, the ancestors in A will be dense in the whole of $[1,\infty)$; when they are not, one can ask how large the ideal must be in order to fill up the entire interval $[1,\infty)$. In this way one can give a refinement of Theorem 2.9. We start with some preparatory results about traces and differents.

For the rest of this chapter we assume that K is not totally real.

Lemma 3.7. Let $g = (a_1,a_2)$, where a_1 and a_2 are positive integers and $a_1 \geq a_2$. Then there exists a unimodular 2×2 matrix M such that

$$M \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} g \\ 0 \end{bmatrix}$$

Proof. This follows directly from the Euclidean Algorithm. Write

$$a_1 = r_1 a_2 + a_3$$

$$a_2 = r_2 a_3 + a_4$$

$$\vdots$$

$$a_{n-1} = r_{n-1}\, a_n + g$$

$$a_n = r_n\, g + 0$$

where $g = a_{n+1} = (a_1,a_2)$. Let $\frac{p_k}{q_k} = [r_1,r_2,\ldots,r_k]$; then $\frac{p_n}{q_n} = \frac{a_1}{a_2}$. Since p_n and q_n are relatively prime, it must be that $p_n g = a_1$ and $q_n g = a_2$. We know by properties of the continued fraction that $q_{n-1}p_n - q_n p_{n-1} = \pm 1$; multiplying by g shows that $q_{n-1}a_1 - p_{n-1}a_2 = \pm g$.

Thus we have

$$\begin{bmatrix} \pm q_{n-1} & \mp p_{n-1} \\ q_n & -p_n \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} g \\ 0 \end{bmatrix}$$

Proposition 3.8. Let A be an ideal in K and let $\zeta_1, \ldots, \zeta_n$ be a Z-basis for A. Then there is another Z-basis $\eta_1, \ldots, \eta_n$ such that $\mathrm{Tr}\,\eta_1 = \cdots = \mathrm{Tr}\,\eta_{n-1} = 0$, and $\mathrm{Tr}\,\eta_n = \frac{p}{q}$ where p and q are relatively prime positive integers.

Proof. We may assume $\mathrm{Tr}\,\zeta_k \geq 0$ for each k by replacing ζ_k with $-\zeta_k$ if necessary. At least one of the ζ_k has non-zero trace; we may assume it is ζ_n. Let ζ_k be an element of the basis other than ζ_n for which $\mathrm{Tr}\,\zeta_k \neq 0$. Then we have $\mathrm{Tr}\,\zeta_k = \frac{a_1}{b}$ and $\mathrm{Tr}\,\zeta_n = \frac{a_2}{b}$ where $(a_1, a_2, b) = 1$. By Lemma 3.7, we may replace ζ_n and ζ_k with η_n and η_k, where $\mathrm{Tr}\,\eta_n = \frac{(a_1, a_2)}{b}$ and $\mathrm{Tr}\,\eta_k = 0$. Continuing in this way, we arrive at a basis of the form asserted in the statement of the proposition.

Theorem 3.9. Let A be an ideal in K, and let $\zeta_1, \ldots, \zeta_n$ be a Z-basis for A of the type constructed in the previous proposition; that is, only ζ_n has non-zero trace. Let $\alpha = \sum_{j=1}^{n} a_j \zeta_j$, $a_j \in Z$, be a reduced number in A. Then

$$a_n \frac{p}{q} < \alpha < a_n \frac{p}{q} + n - 1,$$

where $\frac{p}{q} = \mathrm{Tr}\,\zeta_n$.

Proof. Let $\mu_j^{(k)} = \mathrm{Re}\,\zeta_j^{(k)}$ where $\zeta_j^{(k)}$ is the k^{th}-conjugate of ζ_j. Since α is reduced, we have $-1 < \mathrm{Re}\,\alpha^{(k)} < 0$ for $k = 2, \ldots, n$; in terms of the ζ's and μ's, this is

$$(*)\quad -1 < \sum_{j=1}^{n} a_j \zeta_j^{(k)} < 0 \quad \text{for} \quad k = 2, \ldots, r, \quad \text{and}$$

$$(**)\quad -1 < \sum_{j=1}^{n} a_j \mu_j^{(k)} < 0 \quad \text{for} \quad k = r+1, \ldots, r+s.$$

Add twice the (**) inequalities to the (*) inequalities to see that

$$-(n-1) < \sum_{j=1}^{n} a_j \sum_{k=2}^{n} \zeta_j^{(k)} < 0.$$

Since $\sum_{k=2}^{n} \zeta_j^{(k)} = \mathrm{Tr}\,\zeta_j - \zeta_j$, we have $-(n-1) < a_n \frac{p}{q} - \alpha < 0$, i.e.,

$$a_n \frac{p}{q} < \alpha < a_n \frac{p}{q} + n - 1.$$

Example. Let $K = Q(\sqrt[p]{p})$ where p is an odd prime, and let $A = (1)$ = the ideal of all algebraic integers in K. Let $\zeta = \sqrt[p]{p}$ (i.e., the real positive root). We claim that the smallest trace from A is $\mathrm{Tr}\,1 = p$. To see this, it suffices to observe that no number of the form

$$\frac{a_0 + a_1\zeta + \cdots + a_k\zeta^k}{p},$$

where $p \nmid a_0$, is an algebraic integer. Thus an integral basis for K/Q is $1, \omega_1, \ldots, \omega_{p-1}$, where the ω's do not involve 1, and so have trace zero (actually, it is easy to show that $1, \zeta, \ldots, \zeta^{p-1}$ is an integral basis, but we don't need that fact here). Therefore, all reduced numbers in A must lie in intervals of the form $(kp, kp+p-1)$. so in particular it is impossible for the integral ancestors in K to be dense in all of $[1,\infty)$. Theorem 3.9 by itself does not say, of course, whether or not the intervals above are filled in; this is a deeper question.

By Proposition 3.8, all traces from an ideal A have the form $a\frac{p}{q}$ for $a \in Z$ and $\frac{p}{q}$ a fixed rational number. In other words, all traces are divisible by $\frac{p}{q}$. This condition may be rephrased in terms of the different of K; this is particularly convenient when A is an integral ideal. The different of K, which we will denote by δ, is the smallest integral ideal with the property that $\frac{1}{\delta}|B$ for any ideal B such that $\alpha \in B$ implies $\mathrm{Tr}\,\alpha \in Z$. We will need the following facts about the different:

$\frac{1}{\delta}|B$ if and only if $\mathrm{Tr}\,\alpha \in Z \quad \forall\alpha \in B$.

$\frac{1}{\delta}$ has an element with trace 1.

The norm of δ is Δ, the discriminant of K.

Also, we will use Dedekind's Theorem (stated below). For proofs we refer the reader to Hasse [4], Chapter 25.

Theorem (Dedekind). Let p be a prime number in Z, and let $(p) = p_1^{e_1} \cdots p_g^{e_g}$ be the factorization of (p) in K. Then the contribution of p to δ is

$$\delta_p = \prod_{j=1}^{g} p_j^{\bar{e}_j - 1}$$

where $\bar{e}_j = e_j$ if $p \nmid e_j$, and $\bar{e}_j > e_j$ if $p | e_j$.

For A an ideal in K, let us introduce the following notation:

$\tau(A)$ is the least positive trace of a number from A

$L(A) = \{\theta \geq 1 | \theta \text{ is a limit of ancestors in } A\}$.

Theorem 3.9 gives a necessary condition that $\theta \in L(A)$. If $|K:Q| = 3$, this condition is sufficient, as the following theorem shows:

Theorem 3.10. Let A be an ideal in K, where $|K:Q| = 3$. Then $\theta \in L(A)$ if and only if $\theta \geq 1$ and θ lies in an interval of the form $[a\tau(A), a\tau(A)+2]$ for some $a \in Z$. Thus $L(A) = [1,\infty)$ exactly when $\tau(A) \leq 2$; when $\tau(A) > 2$, $L(A)$ consists of intervals of length 2 with gaps of length $\tau(A) - 2$.

Proof. In view of the preceding remarks, we need only show that if θ is an interval of the form above, then an ancestor $\alpha \in A$ can be found as close as desired to θ. Since $L(A)$ is a closed set, we need consider only a $\theta > 1$ such that strict inequality holds; that is, $a\tau(A) < \theta < a\tau(A) + 2$. Also, by virtue of Proposition 3.2, we need only show that reduced numbers in A may be found close to θ. Let ζ_1, ζ_2, and ζ_3 be a Z-basis for A as constructed in Proposition 3.8: $\mathrm{Tr}\,\zeta_1 = \mathrm{Tr}\,\zeta_2 = 0$, and $\mathrm{Tr}\,\zeta_3 = \tau(A)$. Let $\alpha = a_1\zeta_1 + a_2\zeta_2 + a_3\zeta_3$ where the a_j are to be determined so that $|\alpha - \theta|$ is small and α is reduced. We will take $a_3 = a$. Now since K is a cubic non-totally real field, to check that α is reduced requires examining only one conjugate, $\alpha^{(2)}$. From the proof of Theorem 3.9, in this case $-1 < \mathrm{Re}\,\alpha^{(2)} < 0$ actually is equivalent to $a\tau(A) < \alpha < a\tau(A) + 2$. So if $|\alpha - \theta|$ is small enough, we will have $\alpha > 1$ and $a\tau(A) < \alpha < a\tau(A) + 2$ (since these are true for θ), which will imply that α is reduced. Therefore, we need only select a_1 and a_2 so that

$$|a_1\zeta_1 + a_2\zeta_2 - (\theta - a\zeta_3)| < \varepsilon.$$

This always can be done; since $\dfrac{\zeta_2}{\zeta_1}$ is irrational, we may find a_2 such that

$$\left\| a_2 \frac{\zeta_2}{\zeta_1} - \frac{\theta - a\zeta_3}{\zeta_1} \right\| < \frac{\varepsilon}{|\zeta_1|} \qquad \text{(see, for example, [2], p. 48)}$$

Then let a_1 be the integer such that $|a_1 + a_2\frac{\zeta_2}{\zeta_1} - \frac{\theta - a\zeta_3}{\zeta_1}| = \|a_2\frac{\zeta_2}{\zeta_1} - \frac{\theta - a\zeta_3}{\zeta_1}\|$. These choices for a_1 and a_2 solve the inequality needed. As $\varepsilon > 0$ may be arbitrarily small, we may force α as close to θ as desired.

Proposition 3.11. Let A be an ideal in K, and $t \in Z$. Then $t|\tau(A)$ if and only if $(t)|A\delta$.

Proof. Write $A = \frac{B}{(d)}$ where B is integral and $d \in Z$. Then $t|\tau(A)$ if and only if $dt|\tau(B)$ (since $\tau(A) = \frac{\tau(B)}{d}$). Since B is integral $\tau(B)$ is integral; thus $dt|\tau(B)$ if and only if $C = \frac{B}{(dt)}$ is an ideal all of whose elements have integral trace. By the definition of δ, this is equivalent to $\frac{1}{\delta}|C$, i.e., $(t)|A\delta$.

Theorem 3.10 and Proposition 3.11 have several consequences:

Corollary 3.12. If $|K:Q| = 3$, then $L(\frac{1}{\delta}) = [1,\infty)$.

Proof. Since $L(\frac{1}{\delta})$ has an element of trace 1, we have $\tau(\frac{1}{\delta}) = 1$. The result follows immediately from Theorem 3.10.

Corollary 3.13. If $|K:Q| = 3$, then the integral ancestors of K are dense in $[1,\infty)$ if and only if $27 \nmid \Delta$.

Proof. Since $\operatorname{Tr} 1 = 3$, we have $\tau(1) = 3$ or $\tau(1) \leq 2$. Thus, by Theorem 3.10, $L(1) \neq [1,\infty)$ exactly when $3|\tau(1)$, i.e., $(3)|\delta$, by Proposition 3.11. Thus it remains to prove that $(3)|\delta$ if and only if $27|\Delta$. Since $N(\delta) = \Delta$, one direction is immediate. To prove the converse, we use Dedekind's Theorem. Assuming $27|\Delta$, then 3 ramifies; so it has the factorization

$$(3) = P_1^2 P_2, \quad \text{or}$$

$$(3) = P^3 .$$

The first is inconsistent with $27 \mid \Delta$. For if $(3) = P_1^2 P_2$, then by Dedekind's Theorem $\delta_3 = P_1$, and so $\Delta = N(\delta) = 3m$, where $3 \nmid m$. In the second case, $\delta_3 = P^e$ where $e \geq 3$, and so $(3) \mid \delta$, as claimed.

Corollary 3.14. Let A be an integral ideal of K, and assume $|K:Q| = 3$. Then $L(A) \neq [1,\infty)$ if and only if there exists $p \neq 2$ prime in Z such that $\frac{(p)}{(p,\delta)} \mid A$ or $\frac{(4)}{(4,\delta)} \mid A$.

Proof. We know $L(A) \neq [1,\infty)$ if and only if $\tau(A) \geq 3$. The assertion then follows immediately from Proposition 3.11.

Example 1. Let $K = Q(\zeta)$ where $\zeta = \sqrt[3]{10}$. The discriminant $\Delta = -300$, so the only ramified primes are 2, 3, and 5. The ideals (2), (3), and (5) factor as follows:

$$(2) = (2,\zeta)^3$$

$$(5) = (5,\zeta)^3$$

$$(3) = (3,\alpha)^2(3,\alpha-1) \quad \text{where} \quad \alpha = \frac{\zeta^2+\zeta+1}{3}.$$

Therefore, by Dedekind's Theorem the different $\delta = (2,\zeta)^2(5,\zeta)^2(3,\alpha)$. We see that $|N(\delta)| = 300$, as required. Now let A be an integral ideal of K. Let us denote by A_3, A_4, and A_5 the ideals $\frac{(3)}{(3,\delta)}$, $\frac{(4)}{(4,\delta)}$, and $\frac{5}{(5,\delta)}$, respectively. We may write explicitly

$$A_3 = (3,\alpha)(3,\alpha-1)$$

$$A_4 = (2)(2,\zeta)$$

$$A_5 = (5,\zeta).$$

Then, by Corollary 3.14, $L(A) = [1,\infty)$ unless A is a multiple of A_3, A_4, A_5, or (p), where p is a prime ≥ 7 in Z. In particular, $L(1) = [1,\infty)$, so the integral ancestors of K are dense in $[1,\infty)$.

Example 2. Let $K = Q(\zeta)$, where $\zeta^3 - \zeta - 1 = 0$. Here we have $\Delta = -23$, so 23 is the only ramified prime. In K (23) factors as

$$(23) = (23,\zeta-10)^2(23,\zeta-3).$$

Thus the different is $\delta = (23,\zeta-10)$. Let $A_{23} = \frac{(23)}{(23,\delta)} = (23,\zeta-10)(23,\zeta-3)$. Let A be any ideal in K, and write $A = (\frac{t}{d})B$, where d and $t \in Z$, B is an integral ideal, and $(k) \nmid B$ for $k > 1$ in Z (such factors are to be incorporated into (t)). Now clearly $\tau(A) = \frac{t}{d}\tau(B)$; further, from the way B was defined, $\tau(B) = 1$ unless $A_{23}|B$, in which case $\tau(B) = 23$. Thus we can say precisely when $L(A) = [1,\infty)$:

1. If $\frac{t}{d} \leq \frac{2}{23}$ then $L(A) = [1,\infty)$.
2. If $\frac{2}{23} < \frac{t}{d} \leq 2$ and $A_{23} \nmid B$, then $L(A) = [1,\infty)$.
3. If $\frac{t}{d} > 2$, or $\frac{t}{d} > \frac{2}{23}$ and $A_{23}|B$, then $L(A) \neq [1,\infty)$.

As in the previous example, we have $L(1) = [1,\infty)$. In addition, if a is an integer such that $a \not\equiv 3$ or 10 mod 23, then we can say that $L(\zeta - a) = [1,\infty)$. Setting $A = (\zeta - a)$, we have $\frac{t}{d} = 1$ (no integer divides $\zeta - a$). Let $f(x) = x^3 - x - 1$; then $N(\zeta - a) = -f(a)$, and so $23 \nmid N(\zeta - a)$ by our choice of a. As a consequence, $A_{23} \nmid A$, and thus $L(A) = [1,\infty)$, as asserted.

In general one can perform this sort of analysis for any non-totally real cubic field. The breakdown into cases will usually be more complicated, due to the presence of more ramified primes to consider. When one restricts attention to integral ideals, the situation is somewhat simpler, as illustrated in the first example.

We return now to the general question of determining the nature of the set $L(A)$ for A an ideal in a real but not totally real number field K.

<u>Definition</u>. Let $\theta \geq 1$ be a real number. We say that θ is "trace-allowed" (referring to a particular ideal A) if θ satisfies the condition in Theorem 3.9; that is, $a\tau(A) \leq \theta \leq a\tau(A) + n - 1$, for some $a \in Z$.

For example, Theorem 3.10 says that in a cubic field, $L(A)$ consists exactly of the trace-allowed numbers. By previous results, we know that it is necessary that θ be trace-allowed in order for θ to belong to $L(A)$; in general, though, this is not sufficient.

Let us maintain the previous notation for a Z-basis of A as $\zeta_1, \ldots, \zeta_n$, where $\mathrm{Tr}\,\zeta_n = \tau(A)$ and $\mathrm{Tr}\,\zeta_1 = \cdots = \mathrm{Tr}\,\zeta_{n-1} = 0$, and let $\mu_j^{(k)} = \mathrm{Re}\,\zeta_j^{(k)}$. For technical reasons, it is desirable to insure yet another condition on the basis. Namely, we observe that we can make $|\zeta_n|$ as large as we please without affecting any of the traces. To do this, simply replace ζ_n by $\zeta_n + m\zeta_1$ where m is a large integer.

Now let $\overline{\theta} \in L(A)$, so $a\tau(A) \leq \overline{\theta} \leq a\tau(A) + n - 1$ for some $a \in Z$. There is a sequence of ancestors in A converging to $\overline{\theta}$; for each such ancestor $\alpha = \sum_{j=1}^{n} a_j\zeta_j$ we have $a_n\tau(A) < \alpha < a_n\tau(A) + n - 1$ by Theorem 3.9. Since the α's converge to $\overline{\theta}$, only finitely many distinct a_n can occur; thus there is a subsequence of α's all of which have the same value of a_n. Then clearly $a_n\tau(A) \leq \overline{\theta} \leq a_n\tau(A) + n - 1$. We will restrict the sequence to this subsequence and renotate so that for each α in the sequence, $a\tau(A) < \alpha < a\tau(A) + n - 1$. For each α, we have $-1 < \mathrm{Re}\,\alpha^{(k)} < 0$ by definition of α being reduced. Define φ_k for $k = 2, \ldots, r + s$ by $\mathrm{Re}\,\alpha^{(k)} = a\mu_n^{(k)} - \varphi_k$, i.e., $\varphi_k = -\sum_{j=1}^{n-1} a_j\mu_j^{(k)}$.

The condition $-1 < \text{Re}\, \alpha^{(k)} < 0$ translates to $a\mu_n^{(k)} < \varphi_k < a\mu_n^{(k)} + 1$. Define the parameters $\lambda_2, \ldots, \lambda_{r+s-1}$ by $\varphi_k = \lambda_k \varphi_{r+s}$. We will show presently that this can be made well-defined (i.e., $\varphi_{r+s} \neq 0$).

Lemma 3.15. We may restrict to a subsequence and reorder the conjugates, if necessary, so that $|\lambda_k| \leq 1$ for each k and each α in the sequence.

Proof. As noted above, we may assume $|\zeta_n| > \tau(A) + n - 1$. But then

$$\tau(A) = \text{Tr}\, \zeta_n = \zeta_n + \mu_n^{(2)} + \mu_n^{(3)} + \cdots + \mu_n^{(n)},$$

which implies that $|\mu_n^{(k)}| > 1$ for at least one k. Now consider an α in the sequence converging to $\overline{\theta}$. It is impossible that $\varphi_k = 0$, for the interval $(a\mu_n^{(k)}, a\mu_n^{(k)}+1)$ cannot contain zero. Thus, for each α, the j for which $|\varphi_j|$ is maximal satisfies $\varphi_j \neq 0$. But there are only finitely many choices for j, so we may restrict to a subsequence so that for some j, $|\varphi_j|$ is maximal for each α in the sequence. Reorder the conjugates so that the jth is the $(r+s)$th; then we have $\varphi_{r+s} \neq 0$ and $|\lambda_k| = \left|\frac{\varphi_k}{\varphi_{r+s}}\right| \leq 1$ for each α.

As a consequence of this lemma, the set of points $(\lambda_2, \ldots, \lambda_{r+s-1})$ in R^{r+s-2} associated with each ancestor in the sequence must have an accumulation point, which we will denote by $(\overline{\lambda}_2, \ldots, \overline{\lambda}_{r+s-1})$. Thus $\overline{\theta} \in L(A)$ implies that the system

$$(1) \qquad \begin{cases} |\alpha - \overline{\theta}| < \varepsilon \\ |\varphi_k - \overline{\lambda}_k \varphi_{r+s}| < \varepsilon \quad \text{for } k = 2, \ldots, r+s-1 \end{cases}$$

is solvable in the integral variables $a_1, \ldots, a_{n-1}$ for $\varepsilon > 0$ arbitrarily small. We can push this further -- for each α in the sequence, the λ_k will have to satisfy certain inequalities in order that α be reduced. Specifically, by adding the equations $\operatorname{Re}\alpha^{(k)} = a\mu_n^{(k)} - \varphi_k$ for $k = 2, \ldots, r+s$ (doubling the complex ones), we obtain $\operatorname{Tr}\alpha - \alpha = a(\operatorname{Tr}\zeta_n - \zeta_n) - \lambda\varphi_{r+s}$, where $\lambda = t_2\lambda_2 + \cdots + t_{r+s-1}\lambda_{r+s-1} + t_{r+s}$ and each $t_j = 1$ or 2 depending on whether the jth conjugate is real or complex. Since $\operatorname{Tr}\alpha = a\operatorname{Tr}\zeta_n$, this simplifies to $\alpha = a\zeta_n + \lambda\varphi_{r+s}$. Let $\bar{\lambda} = t_2\bar{\lambda}_2 + \cdots + t_{r+s-1}\bar{\lambda}_{r+s-1} + t_{r+s}$.

Lemma 3.16. In the notation above, $\bar{\lambda} \neq 0$.

Proof. As before, we may assume $|\zeta_n| > \tau(A) + n - 1$. Since φ_{r+s} is bounded, it is impossible to have $|\lambda|$ small, since this would contradict $a\tau(A) < \alpha < a\tau(A) + n - 1$ due to the size of ζ_n, unless $a = 0$. But if $a = 0$ and $|\lambda|$ is small this contradicts $\alpha > 1$.

Let us restrict the sequence of α's again to a subsequence so that $\lambda_k \to \bar{\lambda}_k$ for each k. Then we have

$$\varphi_{r+s} = \frac{\bar{\theta} - a\zeta_n}{\bar{\lambda}} + \delta$$

where δ is small and tends to zero as ε does. Since $a\mu_n^{(k)} < \varphi_k < a\mu_n^{(k)} + 1$, we see on passing to the limit that

$$(2)\quad \begin{cases} a\mu_n^{(r+s)} \leq \dfrac{\bar{\theta} - a\zeta_n}{\bar{\lambda}} \leq a\mu_n^{(r+s)} + 1 \\[2ex] a\mu_n^{(k)} \leq \dfrac{\bar{\lambda}_k(\bar{\theta} - a\zeta_n)}{\bar{\lambda}} \leq a\mu_n^{(k)} + 1 \text{ for } k = 2, \ldots, r+s-1. \end{cases}$$

It will be convenient to divide $L(A)$ into the following subsets:

$L_0(A) = \{\theta \in L(A) \mid$ each inequality of (2) is strict, for some sequence $\alpha \to \theta$, i.e., some values of $\bar{\lambda}_2, \ldots, \bar{\lambda}_{r+s-1}$ satisfying (1)$\}$

$E(A) = L(A) - L_0(A)$

$E_0(A) = \{\theta \in E(A) \mid \theta \text{ is isolated in } E(A)\}$

$E_1(A) = E(A) - E_0(A).$

Thus we have $L(A) = L_0(A) \cup E_0(A) \cup E_1(A)$. It is not difficult to get some control over $L_0(A)$ and $E_0(A)$, but the author has not been able to do this for $E_1(A)$. The structure of $L(A)$ can be resolved under fairly general conditions, however; we will say more about this later.

Suppose that $\overline{\theta} \geq 1$ is a real number for which $\overline{\lambda}_2, \ldots, \overline{\lambda}_{r+s-1}$ exist satisfying (1) and (2) for ε arbitrarily small. We cannot conclude in general that $\overline{\theta} \in L(A)$, because of the possibility of equality in (2). However, if each condition of (2) is strict, then we can make this conclusion:

<u>Proposition 3.17</u>. Let $\overline{\theta} \geq 1$ be a real number. If $\overline{\theta} \in L(A)$, then there exist $\overline{\lambda}_2, \ldots, \overline{\lambda}_{r+s-1}$ such that (1) and (2) holds, and $\overline{\lambda} \neq 0$. Conversely, if such parameters exist and (2) holds with strict inequalities, then $\overline{\theta} \in L_0(A)$.

<u>Proof</u>. We already have shown one direction, so we need only argue that if $\overline{\lambda}_2, \ldots, \overline{\lambda}_{r+s-1}$ exist satisfying (1) and (2) strictly, then $\overline{\theta} \in L_0(A)$. Let $\alpha = \sum_{j=1}^{n} a_j\zeta_j$ be a solution to (1) with small ε. Then, as in the derivation of (2), we have

$$\varphi_{r+s} = \frac{\overline{\theta}-a\zeta_n}{\overline{\lambda}} + \delta$$

where δ is small $(\delta \to 0 \text{ as } \varepsilon \to 0)$. We know that $a\mu_n^{(r+s)} < \frac{\overline{\theta}-a\zeta_n}{\overline{\lambda}} < a\mu_n^{(r+s)} + 1$, so if δ is small enough, φ_{r+s} satisfies this inequality as well. Similarly,

$$\varphi_k = \lambda_k \varphi_{r+s} = \bar{\lambda}_k \varphi_{r+s} + \delta_k = \frac{\bar{\lambda}_k(\bar{\theta} - a\zeta_n)}{\bar{\lambda}} + \delta_k + \delta\bar{\lambda}_k$$

where $|\delta_k| < \varepsilon$. Again, since $a\mu_n^{(k)} < \frac{\bar{\lambda}_k(\bar{\theta}-a\zeta_n)}{\bar{\lambda}} < a\mu_n^{(k)} + 1$, the same is true for φ_k if ε is small enough. We have observed before that these conditions are equivalent to $-1 < \operatorname{Re} \alpha^{(k)} < 0$, i.e., α is reduced. Thus $\bar{\theta}$ is a limit of reduced numbers in A; by virtue of Proposition 3.2, $\bar{\theta} \in L(A)$, and in fact in $L_0(A)$ by its definition.

At this point we need to examine the system (1) more closely, in order to determine when it is solvable. Let us first rewrite the system in terms of the integral variables $a_1, \ldots, a_{n-1}$. We have $\alpha = \sum_{j=1}^{n} a_j\zeta_j$ (a_n = a, determined by $\bar{\theta}$) and $\varphi_k = -\sum_{j=1}^{n-1} a_j\mu_j^{(k)}$. So (1) becomes

$$(3) \quad \begin{cases} |a_1\zeta_1 + \cdots + a_{n-1}\zeta_{n-1} - (\bar{\theta}-a\zeta_n)| < \varepsilon \\ |a_1\nu_1^{(k)} + \cdots + a_{n-1}\nu_{n-1}^{(k)}| < \varepsilon \text{ for } k = 2, \ldots, r+s-1 \end{cases}$$

where $\nu_j^{(k)} = \bar{\lambda}_k\mu_j^{(r+s)} - \mu_j^{(k)}$. Let $t = r + s - 1$, and denote this system as

$$(4) \quad \begin{cases} |L_1 - (\bar{\theta}-a\zeta_n)| < \varepsilon \\ |L_k| < \varepsilon \text{ for } k = 2, \ldots, t \end{cases}$$

where L_j is the appropriate linear form in $a_1, \ldots, a_{n-1}$. A theorem of Rogers [8] states when a system of this type may be solved for ε arbitrarily small. We state here Theorem A of [8]:

Theorem A (Rogers). Let $L_1, \ldots, L_n$ be n linear forms in n variables such that the coefficient matrix has non-zero determinant Δ.

Assume that $|\Delta| < M_n$, where M_n is a positive absolute constant depending only on n (Rogers states explicitly what M_n is, but that will not be needed here). Let $\theta_1, \ldots, \theta_n$ be n real numbers, and let r be less than n. Then the solvability of $|L_j - \theta_j| < \varepsilon$ $(j = 1,\ldots,r)$ and $\prod_{j=1}^{n} |L_j - \theta_j| < 1$ for ε arbitrarily small is equivalent to the following condition:

<u>Condition A</u>. If $x_1, \ldots, x_r$ are real numbers such that $\sum_{j=1}^{r} x_j L_j$ is a form with integral coefficients, then $\sum_{j=1}^{r} x_j \theta_j \in Z$.

Rogers was interested in deeper questions than the solvability of a system such as (4); some of the theorem above is superfluous for our present concerns, and so we need to rephrase his theorem in a more convenient way. First, we may discard the conclusion $\prod_{j=1}^{n} |L_j - \theta_j| < 1$, since the solvability for ε arbitrarily small of $|L_j - \theta_j| < \varepsilon$ $(j = 1,\ldots,r)$ by itself implies Condition A. For if $L = \sum_{j=1}^{r} x_j L_j$ has integral coefficients, then

$$|L - \sum_{j=1}^{r} x_j \theta_j| \le \sum_{j=1}^{r} x_j |L_j - \theta_j| < \varepsilon \sum_{j=1}^{r} x_j$$

and so $|L - \sum_{j=1}^{r} x_j \theta_j|$ may be made arbitrarily small. Since L always is an integer, it follows that $\sum_{j=1}^{r} x_j \theta_j \in Z$.

Next, if we are given $r < n$ linearly independent vectors in R^n, $n - r$ additional vectors can be found such that the resulting determinant is non-zero; further, we may multiply the last vector (one of the additions) by a small scalar to make the determinant as small as necessary. Thus, the determinant condition in Theorem A is not important, as long as the r given forms have linearly independent coefficient vectors.

This enables us to rephrase Theorem A as follows:

Theorem B. Let $L_1, \ldots, L_t$ be $t < n$ linear forms in n variables, with linearly independent coefficient vectors. Let $\theta_1, \ldots, \theta_t$ be t real numbers. Then we may solve simultaneously $|L_j - \theta_j| < \varepsilon$ $(j = 1, \ldots, t)$ for ε arbitrarily small if and only if Condition A holds.

In our system (3) we have $t = r + s - 1 = n - 1 - s$ forms in $n - 1$ variables. As K is not totally real, $s > 0$. The next lemma will show that the condition of linear independence is satisfied, and so Theorem B will apply to our system.

Lemma 3.18. The forms in (3) may be assumed to be linearly independent; that is, any dependences which exist do not affect the solvability of (3).

Proof. Suppose there is a dependence which does not involve the first form. Since the other forms all have zero as the inhomogeneous terms, such a dependence merely shows that one of the forms trivially would satisfy a bound if the rest did. Thus we may discard the superfluous forms, and the solvability of (3) is not affected.

It is not possible that there is a dependence which involves L_1. For if $\sum_{j=1}^{t} x_j L_j = 0$ and $x_1 \neq 0$, then for any $\theta \in L(A)$ we have $x_1(\theta - a\zeta_n) = 0$. This implies that $\theta = a\zeta_n$, and thus θ is isolated in $L(A)$, contradicting Theorem 3.3. Hence no such dependence relation is possible.

It is expedient at this point to change the notation slightly. Specifically, let θ be a trace-allowed number; we will regard $\lambda_2, \ldots, \lambda_t$ as variable parameters which we try to adjust so that (2) and Condition A are satisfied. First, we show that (2) can be satisfied:

Lemma 3.19. Let θ be a strictly trace-allowed number; that is, $a\tau(A) < \theta < a\tau(A) + n - 1$ for $a \in Z$. Then there exist $\lambda_2, \ldots, \lambda_t$ satisfying (2) strictly, such that $\lambda \neq 0$.

Proof. We exhibit such a solution explicitly: Let $\theta = a\tau(A) + \kappa$, where $0 < \kappa < n - 1$. We set

$$\lambda_k = \frac{a\mu_n^{(k)} + \frac{\kappa}{n-1}}{a\mu_n^{(r+s)} + \frac{\kappa}{n-1}} \quad \text{for} \quad k = 2, \ldots, t$$

$$\text{Then} \quad \lambda = \sum_{k=2}^{t} t_k\lambda_k + t_{r+s} = \frac{a(\sum_{k=2} t_k\mu_n^{(k)} + t_{r+s}\mu_n^{(r+s)}) + \frac{\kappa}{n-1}(n-1)}{a\mu_n^{(r+s)} + \frac{\kappa}{n-1}} =$$

$$= \frac{a(\mathrm{Tr}\zeta_n - \zeta_n) + \kappa}{a\mu_n^{(r+s)} + \frac{\kappa}{n-1}} = \frac{a\tau(A) + \kappa - a\zeta_n}{a\mu_n^{(r+s)} + \frac{\kappa}{n-1}} = \frac{\theta - a\zeta_n}{a\mu_n^{(r+s)} + \frac{\kappa}{n-1}} .$$

So $\frac{\theta - a\zeta_n}{\lambda} = a\mu_n^{(r+s)} + \frac{\kappa}{n-1}$, and $\frac{\lambda_k(\theta - a\zeta_n)}{\lambda} = a\mu_n^{(k)} + \frac{\kappa}{n-1}$. Thus $\lambda_2, \ldots, \lambda_t$ satisfy (2) strictly. Finally, we may assume $\lambda \neq 0$ by taking ζ_n big enough that $|\zeta_n| > \tau(A) + n - 1$, so $\theta \neq a\zeta_n$.

Now let $\theta, \lambda_2, \ldots, \lambda_t$ be fixed, and suppose that there exist real numbers $x_1, \ldots, x_t$ such that $\sum_{j=1}^{t} x_jL_j$ has integral coefficients. This implies that for some integers $m_1, \ldots, m_{n-1}$, the following system of equations is solvable:

$$(5) \qquad \begin{bmatrix} \zeta_1 & \nu_1^{(2)} & \cdots & \nu_1^{(t)} \\ \vdots & \vdots & & \vdots \\ \zeta_{n-1} & \nu_{n-1}^{(2)} & \cdots & \nu_{n-1}^{(t)} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_t \end{bmatrix} = \begin{bmatrix} m_1 \\ \vdots \\ m_{n-1} \end{bmatrix}$$

There are two possibilities. First, it might happen that this solution to (5) is a special case of an "indeterminate solution"; that is $x_1, \ldots, x_t$ exist as functions of $\lambda_2, \ldots, \lambda_t$ such that (5) holds identically. Or, it may be that this particular solution to (5) is an isolated numerical accident, so to speak. We will refer to this as a "coincidental solution". We show in the next theorem that only indeterminate solutions need be considered.

Theorem 3.20. If (5) is solvable for $\lambda_2, \ldots, \lambda_t$, and $\lambda \neq 0$, then this is a special case of an indeterminate solution.

Proof. The system (5) is a system of $n - 1$ equations in $t = n - 1 - s < n - 1$ unknowns. Therefore (5) is solvable only when the rows of the matrix satisfy certain dependence relations. Our solution to (5) is part of an indeterminate solution exactly when these dependence relations hold as identities in $\lambda_2, \ldots, \lambda_t$. We will show that this is the case, provided that $\lambda \neq 0$. Let us denote the rows of the matrix as $B_1, \ldots, B_{n-1}$, and assume $c_1 B_1 + \cdots + c_{n-1} B_{n-1} = 0$. This implies the conditions

$$c_1\zeta_1 + \cdots + c_{n-1}\zeta_{n-1} = 0 \quad \text{and}$$

$$c_1\nu_1^{(k)} + \cdots + c_{n-1}\nu_{n-1}^{(k)} = 0 \quad \text{for } k = 2, \ldots, t.$$

Now $\nu_j^{(k)} = \lambda_k \mu_j^{(r+s)} - \mu_j^{(k)}$, so we may rewrite the second type of relation as

$$\lambda_k \sum_{j=1}^{n-1} c_j \mu_j^{(r+s)} = \sum_{j=1}^{n-1} c_j \mu_j^{(k)} \quad \text{for} \quad k = 2, \ldots, t.$$

If $\sum_{j=1}^{n-1} c_j \mu_j^{(r+s)} = 0$, then this dependence holds identically in $\lambda_2, \ldots, \lambda_t$. Otherwise, we may solve for λ_k and compute λ as follows:

$$\lambda = \sum_{k=2}^{t} t_k \lambda_k + t_{r+s} = \frac{\sum_{k=2}^{t} t_k \sum_{j=1}^{n-1} c_j \mu_j^{(k)} + t_{r+s} \sum_{j=1}^{n-1} c_j \mu_j^{(r+s)}}{\sum_{j=1}^{n-1} c_j \mu_j^{(r+s)}} .$$

The numerator of λ is thus

$$\sum_{j=1}^{n-1} c_j \left(\sum_{k=2}^{t} t_k \mu_j^{(k)} + t_{r+s} \mu_j^{(r+s)} \right) = \sum_{j=1}^{n-1} c_j (\mathrm{Tr}\,\zeta_j - \zeta_j) = -\sum_{j=1}^{n-1} c_j \zeta_j = 0.$$

Hence $\lambda = 0$, as promised.

Lemma 3.19 and Theorem 3.20 together provide a complete determination of $L(A)$ in the case that no indeterminate solutions to (5) exist:

<u>Theorem 3.21</u>. If no functions $x_1, \ldots, x_t$ exist such that $\sum_{j=1}^{t} x_j L_j$ has integral coefficients identically in $\lambda_2, \ldots, \lambda_t$, then $L(A)$ consists of all trace-allowed numbers.

<u>Proof</u>. Since $L(A)$ is closed, it suffices to consider only strictly trace-allowed numbers -- that is, numbers of the form $\theta \geq 1$ such that $a\tau(A) < \theta < a\tau(A) + n - 1$ for $a \in Z$. By Lemma 3.19, there exist $\lambda_2, \ldots, \lambda_t$ for θ satisfying (2) strictly, and $\lambda \neq 0$. In view of Theorem 3.20, there are no $x_1, \ldots, x_t$ satisfying (5), so Condition A holds and (1) is solvable. Thus $\theta \in L_0(A)$, by Proposition 3.17.

This proves the theorem.

We consider now the possibility that such functions $x_1, \ldots, x_t$ exist. It is convenient first to derive a more explicit representation for the x_k. From (5) we see that the set of solutions $(x_1,\ldots,x_t)$ forms a Z-module. We may choose a basis for this module so that each basis vector has the form $(0,x_2,\ldots,x_t)$ except the first (see [2], p. 147). Thus, any solution to (5) has the form

$$(x_1,x_2,\ldots,x_t) = c(y_1,\ldots,y_t) + (0,z_2,\ldots,z_t)$$

where $c \in Z$ and $(y_1,\ldots,y_t)$ is the first basis vector. Now, Condition A is satisfied trivially if $x_1 = 0$, so we may assume $x_1 \neq 0$. Thus we need only consider one solution of (5) in verifying Condition A, namely, $(y_1,\ldots,y_t)$. Therefore, by Proposition 3.17 and Theorem B, we know that $\overline{\theta} \in L_0(A)$ if and only if $\overline{\lambda}_2, \ldots, \overline{\lambda}_t$ exist satisfying (2) strictly, and $y_1(\overline{\lambda}_2,\ldots,\overline{\lambda}_t)(\overline{\theta} - a\zeta_n) \in Z$, where a is an integer such that $a\tau(A) \leq \overline{\theta} \leq a\tau(A) + n - 1$. Our first goal is to show that if $\overline{\theta} \in L_0(A)$, then $\overline{\theta}$ lies in an open interval contained in $L_0(A)$.

If the forms in (3) are linearly dependent, then we know from Lemma 3.18 that the first form is not involved. Thus we may order the conjugates so that the last j forms are superfluous -- this has the effect of deleting the last j columns of the matrix in (5) and replacing t by $t - j$. Thus (5) is equivalent to

$$(6) \qquad \begin{bmatrix} \zeta_1 & \nu_1^{(2)} & \cdots & \nu_1^{(t-j)} \\ \vdots & \vdots & & \vdots \\ \zeta_{t-j} & \nu_{t-j}^{(2)} & \cdots & \nu_{t-j}^{(t-j)} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_{t-j} \end{bmatrix} = \begin{bmatrix} m_1 \\ \vdots \\ m_{t-j} \end{bmatrix}$$

upon a suitable reordering of $\zeta_1, \ldots, \zeta_{n-1}$ if necessary. The coefficient matrix now has rank $t - j$, and so is non-singular. Thus there is a unique solution (for given $m_1,\ldots,m_{t-j}$), which we may express using Cramer's Rule. In view of the previous remarks, we are interested in y_1 only. Write $y = y_1$. Then

$$(7) \qquad y(\lambda_2,\ldots,\lambda_t) = \frac{\begin{vmatrix} m_1 & \nu_1^{(2)} & \cdots & \nu_1^{(t-j)} \\ \vdots & \vdots & & \vdots \\ m_{t-j} & \nu_{t-j}^{(2)} & \cdots & \nu_{t-j}^{(t-j)} \end{vmatrix}}{\begin{vmatrix} \zeta_1 & \nu_1^{(2)} & & \nu_1^{(t-j)} \\ \vdots & \vdots & & \\ \zeta_{t-j} & \nu_{t-j}^{(2)} & & \nu_{t-j}^{(t-j)} \end{vmatrix}}$$

where $m_1, \ldots, m_{t-j}$ are fixed integers, and $\nu_i^{(k)} = \lambda_k \mu_i^{(r+s)} - \mu_i^{(k)}$. From this we see that y is fractional linear in each λ_k separately; that is, y has the form

$$(8) \qquad y(\lambda_2,\ldots,\lambda_t) = \frac{A\lambda_k + B}{C\lambda_k + D}$$

where A, B, C, and D do not depend on λ_k.

Now let $\overline{\theta} \in L_0(A)$, so there exist $\overline{\lambda}_2, \ldots, \overline{\lambda}_t$ such that (2) is satisfied strictly, $\overline{\lambda} \neq 0$, and $y(\overline{\lambda}_2,\ldots,\overline{\lambda}_t)(\overline{\theta}-a\zeta_n) = m \in Z$. The denominator of y is non-zero at this point, so all of the partial derivatives are continuous in an open ball around it. The next proposition follows from the implicit function theorem:

<u>Proposition 3.22</u>. In the notation above, if $\frac{\partial y}{\partial \lambda_k}(\overline{\lambda}_2,\ldots,\overline{\lambda}_t) \neq 0$ for

some k, then $\overline{\theta}$ lies in an open interval which is contained in $L_0(A)$.

Proof. As before, we may assume $\overline{\theta} \neq a\zeta_n$ by taking $|\zeta_n|$ large. Let $h(\theta,\lambda_2,\ldots,\lambda_t) = (\theta - a\zeta_n)y(\lambda_2,\ldots,\lambda_t) - m$. We have $h(\overline{\theta},\overline{\lambda}_2,\ldots,\overline{\lambda}_2) = 0$ and $\frac{\partial h}{\partial \lambda_k}(\overline{\theta},\overline{\lambda}_2,\ldots,\overline{\lambda}_t) = (\overline{\theta} - a\zeta_n)\frac{\partial y}{\partial \lambda_k}(\overline{\lambda}_2,\ldots,\overline{\lambda}_t) \neq 0$. The relevant continuity conditions on h clearly hold. It follows by the implicit function theorem that one may satisfy Condition A for all θ in an open interval around $\overline{\theta}$, and the corresponding points $(\lambda_2,\ldots,\lambda_t)$ lie in a small open ball around $(\overline{\lambda}_2,\ldots,\overline{\lambda}_t)$. Since $\overline{\lambda} \neq 0$, we will have $\lambda \neq 0$ for each point in this ball if it is small enough. Thus, by Theorem 3.20, no coincidental solutions to (5) are introduced. Finally, θ, λ_2, ..., λ_t will satisfy (2) strictly if the ball is small enough. Thus Proposition 3.17 applies to θ.

We need a more elaborate argument in case $\frac{\partial y}{\partial \lambda_k}(\overline{\lambda}_2,\ldots,\overline{\lambda}_t) = 0$ for each k.

Lemma 3.23. If $\frac{\partial y}{\partial \lambda_k}(\overline{\lambda}_2,\ldots,\overline{\lambda}_t) = 0$, then it is zero identically on the line through $(\overline{\lambda}_2,\ldots,\overline{\lambda}_t)$ and parallel to the λ_k-axis.

Proof. In (7) denote the numerator of y by f and the denominator by g.

Then we have

$$\frac{\partial y}{\partial \lambda_k} = \frac{g\frac{\partial f}{\partial \lambda_k} - f\frac{\partial g}{\partial \lambda_k}}{g^2}.$$

From (8) we see that $\frac{\partial^2 f}{\partial \lambda_k^2} = \frac{\partial^2 g}{\partial \lambda_k^2} = 0$, so the numerator of $\frac{\partial y}{\partial \lambda_k}$ does not involve λ_k. The conclusion follows.

Lemma 3.24. It is impossible that y is constant in an open ball around $(\overline{\lambda}_2,\ldots,\overline{\lambda}_t)$.

Proof. By our construction of $\overline{\lambda}_2, \ldots, \overline{\lambda}_t$, if α is an ancestor in a particular subsequence converging to $\overline{\theta}$, then the $\lambda_2, \ldots, \lambda_t$ for α are close to $\overline{\lambda}_2, \ldots, \overline{\lambda}_t$. Since $\alpha \in L(A)$, Condition A is satisfied: $y(\lambda_2,\ldots,\lambda_t)(\alpha - a\zeta_n) = m' \in Z$. This is a contradiction if y is constant and α is close enough to $\overline{\theta}$. (Note that y is not identically zero, by assumption).

Corollary 3.25. If $\frac{\partial y}{\partial \lambda_k}(\overline{\lambda}_2,\ldots,\overline{\lambda}_t) = 0$ for each k, then the point $y(\overline{\lambda}_2,\ldots,\overline{\lambda}_t)$ must be a saddle point rather than a local extremum.

Proof. By Lemma 3.23, if y had a local extremum at $(\overline{\lambda}_2,\ldots,\overline{\lambda}_t)$ it would have to be constant in an open neighborhood of $(\overline{\lambda}_2,\ldots,\overline{\lambda}_t)$, in contradiction to Lemma 3.24.

Proposition 3.26. Suppose that $\frac{\partial y}{\partial \lambda_k}(\overline{\lambda}_2,\ldots,\overline{\lambda}_t) = 0$ for each k. Then given $\varepsilon > 0$, there exist $\lambda_2', \ldots, \lambda_t'$ such that

1. $y(\lambda_2',\ldots,\lambda_t') = y(\overline{\lambda}_2,\ldots,\overline{\lambda}_t)$.
2. $(\lambda_2',\ldots,\lambda_t')$ is within an open ε-ball around $(\overline{\lambda}_2,\ldots,\overline{\lambda}_t)$.
3. $\frac{\partial y}{\partial \lambda_k}(\lambda_2',\ldots,\lambda_t') \neq 0$ for some k.

Proof. We know that if $(\lambda_2',\ldots,\lambda_t') \neq (\overline{\lambda}_2,\ldots,\overline{\lambda}_t)$ and is close enough, then some partial derivative is non-zero, or else y would be constant in an open neighborhood of $(\overline{\lambda}_2,\ldots,\overline{\lambda}_t)$, contradicting Lemma 3.24. So the last condition is not a restriction. The existence of $(\lambda_2',\ldots,\lambda_t')$ is now guaranteed by the definition of a saddle point; y must increase in some direction and decrease in another, so on some path it remains constant.

Theorem 3.27. Let $\bar{\theta} \in L_0(A)$. Then $\bar{\theta}$ is in an open interval which is contained in $L_0(A)$.

Proof. If no $x_1, \ldots, x_t$ exist such that $\sum_{j=1}^{t} x_j L_j$ has integral coefficients identically in $\lambda_2, \ldots, \lambda_t$, Theorem 3.21 applies. If such functions exist, we need to consider only one solution $(y_1,\ldots,y_t)$ which is a basis element of the solutions $(x_1,\ldots,x_t)$ and for which $y_1 \neq 0$. Let $\bar{\lambda}_2, \ldots, \bar{\lambda}_t$ be the parameters satisfying (1) and (2) strictly. If $\frac{\partial y_1}{\partial \lambda_k}(\bar{\lambda}_2,\ldots,\bar{\lambda}_t) \neq 0$ for some k, then Proposition 3.22 applies. Finally, if all the partial derivatives are zero, we may replace $(\bar{\lambda}_2,\ldots,\bar{\lambda}_t)$ by $(\lambda_2',\ldots,\lambda_t')$ as in Proposition 3.26. Since $(\bar{\lambda}_2,\ldots,\bar{\lambda}_t)$ satisfies (2) strictly, so will $(\lambda_2',\ldots,\lambda_t')$ if it is close enough; similarly, $\lambda' \neq 0$. Thus Proposition 3.22 applies.

Corollary 3.28. Let α be an ancestor in A. Then there is an open interval around α which is contained in $L_0(A)$.

Proof. This result follows directly from Theorem 3.27 upon observing that $\alpha \in L_0(A)$.

The last result shows that the ancestors in A are dense wherever they occur. We have shown that $L_0(A)$ is well-behaved, so to speak -- the next result establishes some control over $E_0(A)$.

Proposition 3.29. Let $\bar{\theta} \in E_0(A)$. Then all points in an interval of the form $(\bar{\theta},\bar{\theta}+\delta)$ or $(\bar{\theta}-\delta,\bar{\theta})$ are in $L_0(A)$.

Proof. We know $\bar{\theta}$ is not isolated in $L(A)$. Further, by definition, it is isolated in $E(A)$, so in some interval $(\bar{\theta}-\varepsilon,\bar{\theta}+\varepsilon)$ all numbers in $L(A)$ are in $L_0(A)$, except for $\bar{\theta}$ itself. There is a sequence of ancestors in A converging to $\bar{\theta}$ on at least one side, say, from the left. Let α be a fixed ancestor in $(\overline{\theta}-\varepsilon,\overline{\theta})$.

Let $w = \inf\{x > \alpha \mid x \notin L(A)\}$. Certainly $w \in L(A)$. We claim that $w \geq \overline{\theta}$; this will prove the proposition. If $w < \overline{\theta}$, then $w \in L_0(A)$. But then w lies in an open interval which is contained in $L_0(A)$, by Theorem 3.27. This contradicts the definition of w as the greatest lower bound.

Unfortunately, the author was not able to prove a similar result for $E_1(A)$, although he conjectures that it is true. Except for $E_1(A)$, we have shown that $L(A)$ consists of nontrivial intervals (that is, there are no singletons). In any event, we have shown in Corollary 3.28 that around each ancestor in A there is an open interval contained in $L(A)$. However, this still leaves open the possibility that there is a singleton in $L(A)$ which is approached by a sequence of (small) intervals from one side. It is suspected that this sort of thing cannot happen. Indeed, the examples which follow suggest a large amount of "nice" structure in $L(A)$.

We regard the situation in Theorem 3.21 as typical; that is, given an ideal A, it is to be expected that no functions $x_1, \ldots, x_t$ exist satisfying the necessary properties. For if $L = \sum_{j=1}^{t} x_j L_j$ has integral coefficients identically in $\lambda_2, \ldots, \lambda_t$, this means that we can solve $n - 1$ equations in $t = n - 1 - s$ unknowns, for appropriate choice of the integers $m_1, \ldots, m_{n-1}$ on the right hand side. One would not expect to be able to do this very often, but rather only when the numbers $\mu_j^{(k)}$ are "organized" in some fashion. Thus, we expect that the usual situation is that $L(A)$ is all trace-allowed numbers.

We conclude this chapter with two examples which illustrate to some extent the range of possibilities involved.

Example 1. Let $K = Q(\zeta)$, where $\zeta = \sqrt[4]{2}$, and let $A = (1)$. An integral basis for A is simply ζ, ζ^2, ζ^3, and 1, so $\tau(A) = 4 = \mathrm{Tr}\ 1$. The following table shows the values of $\mu_j^{(k)}$ for the relevant values of j and k. Here, $\zeta^{(2)}$ is the conjugate $-\zeta$, and $\zeta^{(3)}$ is the conjugate $i\zeta$.

(j,k)	$(1,2)$	$(2,2)$	$(3,2)$	$(1,3)$	$(2,3)$	$(3,3)$
$\mu_j^{(k)}$	$-\zeta$	ζ^2	$-\zeta^3$	0	$-\zeta^2$	0

Thus the system (3) is

$$|a_1\zeta + a_2\zeta^2 + a_3\zeta^3 - (\theta - a)| < \varepsilon$$

$$|a_1\zeta - a_2\zeta^2(1+\lambda_2) + a_3\zeta^3| < \varepsilon$$

and the system (2) is

$$a \le \frac{\theta - a}{\lambda} \le a + 1$$

$$a \le \frac{\lambda_2(\theta - a)}{\lambda} \le a + 1$$

where $\lambda = \lambda_2 + 2$. In (3) there is a solution x_1, x_2 to $x_1L_1 + x_2L_2 = L$, a form with integral coefficients, namely, $x_1 = \frac{1}{\sqrt{2}(\lambda_2+2)}$ and $x_2 = \frac{-1}{\sqrt{2}(\lambda_2+2)}$. It is easy to see that this is the minimal solution. Thus (3) is solvable if and only if Condition A is satisfied, i.e.,

$$\frac{\theta - a}{\sqrt{2}\lambda} \in Z.$$

Let $k = \frac{\theta-a}{\sqrt{2}\lambda}$; substituting this into (2) shows that

$$a \le k\sqrt{2} \le a + 1, \text{ and}$$

$$a \le k\lambda_2\sqrt{2} \le a + 1.$$

Since $a \ge 0$, we must have $a = [k\sqrt{2}]$. This by itself puts a restriction on a -- for example, $a = 3$ is impossible, and no integral ancestor occurs in $[12,15]$. Also, $k\lambda_2\sqrt{2} = k\sqrt{2}(\lambda-2) = \theta - a - 2k\sqrt{2}$, so the second inequality becomes

$$2a + 2k\sqrt{2} \le \theta \le 2a + 2k\sqrt{2} + 1.$$

Since $a = [k\sqrt{2}]$, $2a + 2k\sqrt{2} \ge 4a$ and $2a + 2k\sqrt{2} + 1 \le 4a + 3$. Thus $\theta \in [4a, 4a+3]$, as we knew from Theorem 3.9. This completes the determination of $L(A)$. In each interval $[4a, 4a+3]$ where $a = [k\sqrt{2}]$, there is a subinterval of length one, namely, $[2a+2k\sqrt{2}, 2a+2k\sqrt{2}+1]$ which lies in $L(A)$, provided we assume also that $a > 0$, since $\theta \in L(A)$ implies $\theta \ge 1$. In particular, the smallest number in $L(A)$ is $2 + 2\sqrt{2}$.

If we replace 2 by $N = 2p$, p prime in Z and let $\zeta = \sqrt[4]{N}$, the same computations carry over. That is, an integral basis is ζ, ζ^2, ζ^3, and 1, and $L(A)$ takes the same shape. Thus the smallest number in $L(A)$ is $2(\sqrt{N}+[\sqrt{N}])$, and so all integral reduced numbers are larger than this number. As a consequence, there are fields for which all integral reduced numbers are larger than a given bound.

Example 2. Let us generalize the situation in Example 1. Let $K = Q(\zeta)$, $\zeta = \sqrt[n]{q}$, where q is a positive rational number. Assume $|K:Q| = n$, and n is odd, ≥ 5. Consider ancestors of the form

$a_1\zeta + a_2\zeta^2 + \cdots + a_{n-1}\zeta^{n-1} + a_n\zeta_n$, where ζ_n is not yet determined.

Let $\rho = e^{\frac{2\pi i}{n}}$ and $w_k = \text{Re}\,\rho^k$. We order the conjugates of ζ as follows:

$$\zeta^{(k)} = \zeta\rho^k \quad \text{for} \quad k = 2, 3, \ldots, r+s-1$$

$$\zeta^{(r+s)} = \zeta\rho.$$

Thus $\nu_j^{(k)} = \lambda_k\mu_j^{(r+s)} - \mu_j^{(k)} = \lambda_k\zeta^j w_j - \zeta^j w_{jk}$. Similarly,

$\nu_{n-j}^{(k)} = \lambda_k\zeta^{n-j}w_{n-j} - \zeta^{n-j}w_{(n-j)k}$. But $w_{n-j} = w_j$, so $\nu_{n-j}^{(k)} = \frac{\zeta^{n-j}}{\zeta^j}\nu_j^{(k)}$.

Hence the system (5) is

$$\begin{bmatrix} \zeta & \nu_1^{(2)} & \cdots & \nu_1^{(t)} \\ \vdots & \vdots & & \vdots \\ \zeta^{\frac{n-1}{2}} & \nu_{\frac{n-1}{2}}^{(2)} & \cdots & \nu_{\frac{n-1}{2}}^{(t)} \\ \zeta^{\frac{n+1}{2}} & \nu_{\frac{n+1}{2}}^{(2)} & \cdots & \nu_{\frac{n+1}{2}}^{(t)} \\ \vdots & \vdots & & \vdots \\ \zeta^{n-1} & \nu_{n-1}^{(2)} & \cdots & \nu_{n-1}^{(t)} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_t \end{bmatrix} = \begin{bmatrix} m_1 \\ \vdots \\ m_{n-1} \end{bmatrix}$$

Let B be the matrix above. Denote the rows of B by $B_1, \ldots, B_{n-1}$. We have $B_j = \frac{\zeta^j}{\zeta^{n-j}} B_{n-j}$, so if $B_j \cdot [x_1,\ldots,x_t]$ and $B_{n-j} \cdot [x_1,\ldots,x_t]$ both are integers, this implies both are zero, since $\frac{\zeta^j}{\zeta^{n-j}} \notin Q$. Thus the only solution to (5) occurs when each $m_j = 0$.

Now let ζ_n be an integer in K such that $\mathrm{Tr}\,\zeta_n > 0$ and is as small as possible. Then ζ_n has the form

$$\zeta_n = \frac{b_0+b_1\zeta+\cdots+b_{n-1}\zeta^{n-1}}{d} \quad \text{where} \quad b_0 \neq 0.$$

Thus $\zeta, \ldots, \zeta^{n-1}, \zeta_n$ is a field basis for K/Q, and so the Z-module generated by $\zeta, \ldots, \zeta^{n-1}, \zeta_n$ contains an ideal. Now we may use the result of Lemma 3.18 that there is no dependence of the columns of B which involves the first column. But our system (5) is exactly such a dependence -- therefore, $x_1 = 0$ and there are no non-trivial solutions $x_1, \ldots, x_t$ to consider for Condition A. Now let A be an ideal which contains the Z-module generated by $\zeta, \ldots, \zeta^{n-1}$, and ζ_n. Then L(A) consists of all trace-allowed numbers, by Theorem 3.21. In particular, this holds for A = (1). Thus the integral ancestors in K are dense in either $[1,\infty)$ or $[1,n-1] \cup \bigcup_{k=1}^{\infty} [kn, kn+n-1]$.

Chapter 4. Equivalence of Binary Forms

We conclude with an application of ancestors to the problem of determining whether or not two given binary forms are equivalent. That is, given two binary forms $F(x,y)$ and $G(x,y)$, is there a transformation $x_1 = ax + by$, $y_1 = cx + dy$ with $ad - bc = \pm 1$, $a, b, c,$ and $d \in Z$, and $F(x_1,y_1) = G(x,y)$? We will restrict ourselves to irreducible binary homogeneous forms of degree at least three, with integer coefficients and at least one real root (by a root of the form $F(x,y)$ we mean a root of the polynomial $F(x,1)$). For the sake of brevity, we will refer to these simply as forms from now on.

Let F be a form with r real roots $\alpha^{(1)}, \ldots, \alpha^{(r)}$. To each $\alpha^{(k)}$ there corresponds one ancestor $\overline{\alpha}_k$ (it is possible for two conjugates to have the same ancestor, but in general the ancestors are distinct -- in fact, the number of distinct ancestors divides r; this will be proved later). Define the set A_F to be $\{\overline{\alpha}_1,\ldots,\overline{\alpha}_r\}$. If F and G are equivalent forms; then their roots are equivalent under the same transformation. As equivalent numbers have the same ancestor, we see that $A_F = A_G$. Conversely, suppose that F and G are two forms of the same degree, and $A_F \cap A_G \neq \emptyset$. Then there is an ancestor which is equivalent to a root of F and to a root of G, so these two roots are equivalent. Thus we have $\alpha \sim \beta$, where β is a root of G and $\alpha = \alpha^{(1)}, \ldots, \alpha^{(n)}$ are the roots of F. From the relation $\beta = \frac{a\alpha+b}{c\alpha+d}$ we see that the numbers $\frac{a\alpha^{(k)}+b}{c\alpha^{(k)}+d}$ all are conjugates of β, and are distinct as k ranges from 1 to n. So all roots of G have this form, and the transformation $x_1 = ax + by$, $y_1 = cx + dy$ takes G to tF for some integer t. Since F and G are irreducible, it follows that $t = \pm 1$. We conclude that $F \sim \pm G$, and $A_F = A_G$. This proves the following theorem:

<u>Theorem 4.1</u>. Let F and G be two forms of the same degree. Then

1. $A_F = A_G$ or $A_F \cap A_G = \emptyset$.

2. $A_F = A_G$ if and only if $F \sim \pm G$.

It remains now to resolve the sign ambiguity in Theorem 4.1. If F has odd degree, then the transformation $x_1 = -x$, $y_1 = -y$ always is an equivalence between F and $-F$, so this ambiguity presents itself only in the cases of even degree. The following theorem characterizes when this can happen:

<u>Theorem 4.2</u>. Let F be a form of even degree $n \geq 4$, and assume $F \sim -F$ by the transformation $x_1 = ax + by$, $y_1 = cx + dy$. Then $a = -d$, $ad - bc = 1$, and $N_{Q(\alpha)/Q}(c\alpha+d) = -1$ for any root α of F. These conditions imply the further restriction $n \equiv 2 \bmod 4$.

<u>Proof</u>. Let $\Delta = ad - bc = \pm 1$. If α is a root of F, then $\frac{a\alpha+b}{c\alpha+d}$ is another root, say, $\alpha^{(2)}$. If $\alpha = \alpha^{(2)}$, then $c\alpha^2 + (d-a)\alpha - b = 0$. Since α does not satisfy a non-trivial quadratic equation, this forces $b = c = 0$ and $a = d = \pm 1$; however, this transformation takes F to $+F$, not $-F$. So $\alpha \neq \alpha^{(2)}$. Write this in matrix notation:

$$A\begin{bmatrix}\alpha\\1\end{bmatrix} = \begin{bmatrix}\alpha^{(2)}\\1\end{bmatrix} \quad \text{where } A = \begin{bmatrix}a & b\\c & d\end{bmatrix}.$$

Inductively, $A^k\begin{bmatrix}\alpha\\1\end{bmatrix} = \begin{bmatrix}\alpha^{(k+1)}\\1\end{bmatrix}$ where $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots$ are some of the conjugates of α. Eventually we get back to α, so $A^k = \pm I$ for some $k \geq 1$. This implies that the minimum polynomial of A divides $x^k \pm 1$, so in particular, all the eigenvalues are roots of unity. Further, the characteristic polynomial of A is quadratic, so if there were repeated roots then the minimum polynomial would be $x \pm 1$, implying $A = \pm I$ which we already know is impossible. Thus the characteristic polynomial of A is $x^2 \pm 1$ or $x^2 \pm x + 1$. Also, we can write out the characteristic polynomial explicitly in terms of the entries of A: it is $x^2 - x(a+d) + \Delta$.

Case 1: The characteristic polynomial is $x^2 \pm x + 1$. Then $\Delta = 1$ and $a + d = \pm 1$. We may assume $a + d = 1$ by replacing (a,b,c,d) with $(-a,-b,-c,-d)$ if necessary. Let $K = Q(\alpha)$. We see that $N_{K/Q}(c\alpha - a) = -1$ on comparing the coefficients of x^n in $F(x_1,y_1)$ and $F(x,y)$. Let $\beta = c\alpha - a = c\alpha + d - 1$. Then we have

$$\beta^{(2)} = c\alpha^{(2)} - a = \frac{ac\alpha+bc}{c\alpha+d} - a = \frac{bc-ad}{c\alpha-a+1} = \frac{-\Delta}{\beta+1} = \frac{-1}{\beta+1}.$$

Thus the map $x \mapsto \frac{-1}{x+1}$ takes a conjugate of β to another conjugate of β.

This map has order 3:

$$\frac{-1}{\beta^{(2)}+1} = \frac{-(\beta+1)}{\beta} = \beta^{(t)}, \quad \text{say}; \quad \frac{-1}{\beta^{(t)}+1} = \beta.$$

Thus the conjugates of β are grouped in $\frac{n}{3}$ triples of the form $\beta, \frac{-1}{\beta+1}, \frac{-(\beta+1)}{\beta}$. Since the product of these three is $+1$, we see that $N_{K/Q}(\beta) = +1$, in contradiction to the above. So this case is impossible.

Case 2: The characteristic polynomial is $x^2 \pm 1$. Thus $a + d = 0$ and $\Delta = \pm 1$. We have $N_{K/Q}(c\alpha - a) = -1$, as in Case 1. Let $\beta = c\alpha - a = c\alpha + d$. Then

$$\beta^{(2)} = c\alpha^{(2)} - a = \frac{ac\alpha+bc}{c\alpha+d} - a = \frac{-\Delta}{\beta}.$$

Thus the conjugates of β are grouped in $\frac{n}{2}$ pairs of the form $\beta, \frac{-\Delta}{\beta}$.

Then $N_{K/Q}(\beta) = (-\Delta)^{\frac{n}{2}} = -1$ if and only if $\Delta = 1$ and $n \equiv 2 \bmod 4$.

Actually, the conditions in the statement of Theorem 4.2 are both necessary and sufficient. That is, if β is an algebraic number such that $|Q(\beta) : Q| = n \geq 4$, $n \equiv 2 \bmod 4$, and $\frac{-1}{\beta}$ is a conjugate of β, then forms F which are equivalent to their negatives can be constructed as follows: Let c and d be integers such that $c > 0$ and $c | d^2 + 1$. Let $a = -d$ and $b = \frac{-d^2-1}{c}$. Then the form F which has $\alpha = \frac{\beta - d}{c}$ as a root will be equivalent to its negative, and by the theorem, all such forms arise in this way.

Such forms do exist; for example, let $F(x,y) = x^{4n+2} - x^{2n+1}y^{2n+1} - y^{4n+2}$. The transformation $x_1 = -y$, $y_1 = x$ takes F to $-F$. The roots of F are the $(2n+1)^{th}$ roots of $\frac{1 \pm \sqrt{5}}{2}$; since $\frac{1+\sqrt{5}}{2}$ is the fundamental unit $Q(\sqrt{5})$, it is not a power of any number in $Q(\sqrt{5})$. The irreducibility of F follows (see, for example, [5], p. 221).

The next proposition helps to pin down the size of A_F -- namely, we prove that $|A_F|$ divides r.

<u>Proposition 4.3</u>. Let F be a form with r real roots and $2s$ complex roots. Then $t|A_F| = r$ for some integer t. Further, $t | (r, 2s)$.

<u>Proof</u>. Let $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ be the roots of F, where $\alpha^{(1)}, \ldots, \alpha^{(r)}$ are real. The equivalence relation $\sim$ divides the roots into equivalence classes. Denote the equivalence class containing $\alpha^{(j)}$ by C_j. Note that each C_j contains only real roots or only non-real roots. Let K be the normal closure of $Q(\alpha)$,

and let $\alpha^{(j)}$ be a conjugate not in C_1 (if there is one). Then there is an automorphism σ of K/Q which takes α to $\alpha^{(j)}$. We claim that in fact σ takes C_1 onto C_j in a one-to-one fashion. Let $\alpha^{(k)} \in C_1$, so $\alpha^{(k)} = \frac{a\alpha+b}{c\alpha+d}$. Then $\alpha^{(k)}\sigma = \frac{a\alpha^{(j)}+b}{c\alpha^{(j)}} \sim \alpha^{(j)}$, so $\alpha^{(k)}\sigma \in C_j$. Thus $C_1\sigma \subseteq C_j$. It is clear that σ is one-to-one since it is an automorphism. Since $C_j\sigma^{-1} \subseteq C_1$, we have that σ takes C_1 onto C_j. Thus $|C_j| = |C_1|$ for each j. Let $t = |C_1|$; in view of the remarks above, $t|(r,2s)$. Further, the number of distinct real equivalence classes is exactly $|A_F|$. This completes the proof.

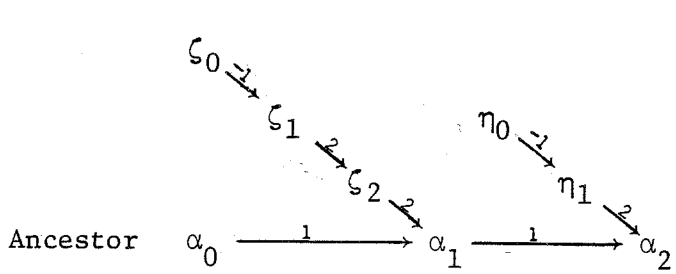
In particular, if r is odd and s is a power of two, then $|A_F| = r$. We can say in any event that $|A_F| \geq \frac{r}{(r,2s)}$. In general, no further restriction can be given.

We illustrate Theorem 4.1 with two examples:

<u>Example 1</u>. Let $F(x,y) = x^3 + 3xy^2 + 2y^3$

and $G(x,y) = 116x^3 + 219x^2y + 138xy^2 + 29y^3$.

Let η_0 be the real root of F, and ζ_0 the real root of G (each form has only one real root). The ancestor for η_0 was found in an example in chapter one; it is the real root of $2x^3 - 3x^2 - 1$. The ancestor for ζ_0 may be found by the same method; it is in fact the same. ζ_0 and η_0 are related as indicated in the diagram. In this notation, $\alpha \xrightarrow{u} \beta$ means $\alpha = u + \frac{1}{\beta}$.



Since η_0 and ζ_0 have the same ancestor, $F \sim G$ (there is no ambiguity of sign since the degree is odd). Further, from the partial quotients in the diagram we can determine explicitly what the transformation is which takes η_0 to ζ_0 (and F to G). We get

$$\zeta_0 = \frac{1-2\eta_0}{3\eta_0-2} .$$

Hence $G(2x-y, -3x+2y) = F(x,y)$.

Example 2. Let $F(x,y) = x^4 - 14x^2y^2 + 9y^4$

and $G(x,y) = x^4 + 8x^3y + 8x^2y^2 - 32xy^3 - 44y^4$.

The form F has been considered in an example in chapter 2; $A_F = \{\overline{\alpha},\overline{\beta}\}$, where $\overline{\alpha}$ is the reduced root of $36x^4 - 24x^3 - 40x^2 - 12x - 1$ and $\overline{\beta}$ of $281x^4 - 284x^3 - 248x^2 - 56x - 4$. There are only two ancestors because the roots of F come in equivalent pairs. That is, if α is a root of F, so is $-\alpha$, and these two numbers have the same ancestor. G has four real roots (as does F), of which one is positive, say, γ. γ is not reduced, but its conjugates are dispersed (there is one between -2 and -1 and another between -3 and -2). So by Theorem 2.5, the first reduced successor of γ is an ancestor. In fact, the immediate successor $\gamma_1 = \frac{1}{\gamma-1}$ is reduced, and hence is the ancestor equivalent to γ. The polynomial which γ_1 satisfies is $59x^4 - 12x^3 - 38x^2 - 12x - 1$, and so $\gamma_1 \notin A_F$. Thus $A_F \neq A_G$, and $F \not\sim G$.

Finally, it should be noted that the reduced numbers defined in this thesis may be used to construct a theory of reduction of forms. Namely, we define a form to be reduced if it has a reduced root (obviously, a form can have at most one reduced root). Similarly, we define a reduced form to be an ancestor if its reduced root is an ancestor. This theory of reduction differs from the existing theories, the most general of which is due to Hermite and Julia. In their method, a quadratic covariant is constructed from a given form by a somewhat complicated process; then the form is defined to be reduced if this quadratic covariant is. Theoretically, this method is powerful enough to prove that there are only finitely many classes of forms with a given set of invariants. However, the computations are sufficiently involved that in any particular case (for example, to see if two given forms are equivalent) this method is impractical. For a more detailed account of this, see Chapter 18 of [6].

Conclusion

In several places in this thesis, there are results which are either incomplete or suggest generalizations. We will mention some of these here. Probably the most obvious such incomplete result is the lack of a good description of L(A) when A is an ideal in a non-totally real field of degree at least four. In addition to showing that L(A) consists of genuine intervals (or, if not, characterizing it in some other way), one would like to know more about how these intervals behave. For example, the examples considered so far suggest that the length is constant. Is this true? Also, it is plausible (from the system (2) of chapter three) that the endpoints of the intervals lie in the normal closure of K. Perhaps a more fundamental problem is to characterize when L(A) is the set of all trace-allowed numbers. Theorem 3.21 gives a sufficient condition for this to happen; it is reasonable to conjecture that it is necessary. Even so, it would be nice to give a condition that is easier to check.

Ancestors have possible applications to other important problems. One such possibility is in determining the number of equivalence classes of binary forms of a given discriminant (or, more generally, a given set of invariants). One might be able to bound the coefficients of the polynomials which the ancestors satisfy in terms of these invariants. If this could be done, it would be a vast improvement over what can be done with Hermite's method. Another possible application of ancestors is in studying the continued fraction of a real algebraic number of degree at least three. In fact, this was the original motivation in studying reduced numbers -- it was hoped that information about the continued fractions of cubic numbers could be obtained in this way.

This is possible to some extent; for example, the author was able to show that if $\alpha = [u_0, u_1, u_2, \ldots]$ is a totally real reduced cubic number, then the partial quotient's growth is bounded by

$$u_n < A^{\sqrt{3}^n}$$

where A is an effective (and easily computed) constant depending on α. This was done by sandwiching α between a rational and a quadratic number which agreed to two continued fraction places (these numbers were constructed from the coefficients of the covariants of the polynomial satisfied by α). Unfortunately, this is very far from what is presumed to be the truth, and this method does not appear to be capable of significant refinement.

Finally, several generalizations of reduced numbers are conceivable. For example, one could try to develop a theory of reduction for complex numbers, using Hurwitz's complex continued fractions. Similarly, one could develop a p-adic analogue. The main problem to overcome in these developments is to find the "correct" region in which the conjugates of an algebraic number are supposed to stay. For the reduced numbers defined here, the region is the infinite strip $\{z \mid -1 < \operatorname{Re} z < 0\}$ in the complex plane. It is not immediately obvious how this region is to be generalized in the situations described above.

References

[1] D. Cantor, P. Galyean, and H. Zimmer, A Continued Fraction Algorithm for Real Algebraic Numbers, Math. of Comp. 26, 785-791.

[2] J.W.S. Cassels, An Introduction to Diophantine Approximation, Cambridge University Press, 1957.

[3] B. N. Delone and D. K. Faddeev, The Theory of Irrationalities of the Third Degree, Amer. Math. Soc., 1964.

[4] H. Hasse, Number Theory, Springer, 1980.

[5] S. Lang, Algebra, Addison Wesley, 1971.

[6] L. J. Mordell, Diophantine Equations, Academic Press, 1969.

[7] O. Perron, Die Lehre von den Kettenbrüchen, B. G. Teubner, 1913.

[8] C. A. Rogers, The Product of n Non-homogeneous Linear Forms, Proc. Lon. Math. Soc. (3), 4, 50-83.

[9] R. Salem, Algebraic Numbers and Fourier Analysis, Heath, 1963.