THE TABULATION OF COMPLEX CUBIC FIELDS
WITH UNITS AND CLASS-NUMBERS

I. O. ANGELL

ROYAL HOLLOWAY COLLEGE, LONDON

SUPERVISOR:- PROFESSOR H. J. GODWIN

R. H. C LIBRARY
CLASS No. AOE Ang
ACC. No. 108310
DATE ACQ Oct '72

ProQuest Number: 10096770

All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.

ProQuest 10096770

Published by ProQuest LLC(2016). Copyright of the Dissertation is held by the Author.

All rights reserved.
This work is protected against unauthorized copying under Title 17, United States Code.
Microform Edition © ProQuest LLC.

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

ACKNOWLEDGEMENTS

I should like to thank my supervisor, Professor H. J. Godwin for his invaluable advice and encouragement in our many discussions on this work. The majority of the results obtained in this thesis are to the best of my knowledge, new, the remainder having new proofs.

I am also grateful to Professor H. P. F. Swinnerton-Dyer for his comments on Hasse's theorem. My thanks are also due to the University of London Computer Centre, on whose C.D.C. 6600 and ATLAS machines this work was run, and to the Science Research Council for financing the work.

CONTENTS

The Table of Complex Cubic Number Fields together with Units and Class Numbers is to be found in the Appendix volume of this Thesis.

R.H.C.
LIBRARY

ERRATA

Page 4	line 5	for Jacobi (24) read (,see Jacobi (24))
	line 7	for Vorondi read Voronoi
	line 1 up	for scarce read scarce.
Page 5	line 6	for discriminant read discriminant Δ
Page 8	line 10 up	for roats read roots
Page 13	(Title)	for Theorem's read Theorems
Page 17	line 3 up	for minimice read minima
Page 30	line 1	for Voronoi (23) read Voronoi (D+F(12))
	line 6	for Delone and Faddeev (13) read Delone and Faddeev (12)
	line 7 up	for distance of $\underline{z}'$ for 0 read distance of $\underline{z}$ from 0
Page 45	line 6	for past-multiplying read post-multiplying
Page 60	line 9	for know read now
Page 64	line 11	for Voronai's read Voronoi's
Page 80	ref 12	for Vol read Vol 10
	ref 14	for J.C.F.Causs read C.F.Gauss
Page 82	ref 33	add St Petersburg (1869)

ABSTRACT

The purpose of the work is to tabulate the cubic number fields with discriminants between -20,000 and 0; for each field there is given:-

the discriminant DIS;

the coefficients A, B, C of a polynomial, a zero θ of which generates the field;

the index of the polynomial over the field, INDEX;

the fundamental unit of the field $\frac{I\theta^2 + J\theta + K}{L}$;

the class number H;

the minimum ideal norm P, required in the search for the class number.

The completed table, together with computer programs used in the calculations, and one program used for checking the discriminant values, are found in the appendix to the thesis. Also a note is given of the only seven fields in the above range whose class group is not cyclic.

PART I

The theory needed to calculate the complex cubic number fields with discriminant greater than -20,000, their units and class numbers.

INTRODUCTION

The earliest tables of algebraic number fields were naturally those of quadratic fields. Most elementary text books give the process of obtaining field discriminants, defining polynomials and integral basis elements for such fields, and they prove that K($\sqrt{-3}$) and K($\sqrt{-1}$) are the only imaginary quadratic fields with units other than ± 1. In real quadratic fields the unit problem is neatly solved by use of a continued fraction algorithm. Gauss and Hermite head the list of authors on the work of finding the class number of these fields, which produced an elegant continued fraction reduction technique for ideals in real fields, (Dickson(13), Bachmann(3)). Sommer (29) gives an example of such tables for fields of discriminants between -100 and 100, but also includes other relevant facts such as ideal and genus structures.

The problem is more involved in fields of higher degree. Mathews (26) gives a method of finding a list of polynomials, which contain all defining polynomials for fields of negative discriminant greater than a given bound; he includes a table of fields with discriminant greater than -1000. His method was to produce bounds for the polynomial coefficients; similar methods were used by Minkowski (29), and by Godwin and Samet (15) who calculated the totally real cubic fields with discriminant less than 20,000, and whose method is used in this thesis. Hasse (23) approached the problem by class field theory; he reduces the question to certain calculations in quadratic fields, but unfortunately this method furnishes only the field discriminants, and gives no information about the defining polynomials of the respective fields.

Bounds have been given by Davenport and Heilbronn (10) for the density of both kinds of cubic fields. Zolotareff (33) using an idea of Hermite gives a method of finding units of pure cubic fields (i.e. generated by a polynomial $x^3 = n$). Berwick (7) using an extension of continued fractions in the cubic case Jacobi (24), produced an algorithm to calculate the fundamental units of cubic fields. Delone and Faddeev (12) gave two methods, basically the work of G.F. Vorondi (31), and one of these methods is used in this thesis to calculate the fundamental unit of cubic fields with signature 1. Other methods of unit calculation are notably those of Uspensky (32), Bergmann (4), (5), Hasse and Bernstein (6) and Tszekeres. Godwin (16) gives a method of ascertaining if two units in a totally real cubic field form a fundamental pair. Using Mathews table and Voronoi's algorithm, Delone and Latysheva (D + F) produced a table of fundamental units for all cubic fields with negative discriminant greater than -369. Dedekind (11) produced a method to find the class number of pure cubic fields and Reid (30) has a table of the class numbers of fields corresponding to other special types of polynomials. Godwin (17) gives the class numbers of all the real cubic fields in his table mentioned above.

Tables of higher degree are scarce. Godwin (18)(19)(20)(21)(22), produced tables of all types of quartic fields with small discriminant.

CHAPTER 1

The calculation of all complex cubic fields with discriminant greater than -20,000

1.1 The basis of the above calculation is the following theorem, similar to one used by Godwin (20).

Theorem 1.1 Let K be a cubic field having signature one and discriminant Then there is at least one polynomial

$$P(x) = x^3 - ax^2 + bx - c$$

where a, b, c are rational integers, having zeros $\alpha, \beta \pm i\gamma$, such that K is generated by one of these zeros, and for which

$$S = S(\alpha,\beta,\gamma) = (\alpha-\beta)^2 + \sigma\gamma^2 \leq \left(-\frac{\sigma\Delta}{3}\right)^{\frac{1}{2}} \qquad (\sigma \text{ an integer} > 0)$$

Proof

The integers of K form a 3-dimensional lattice $\mathcal{L}_1$ with determinant $\sqrt{\Delta}$. We may order the base vectors of $\mathcal{L}_1$ so that the real one comes first, and we apply the transformation defined by the matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \\ 0 & -i\sqrt{\frac{\sigma}{8}} & i\sqrt{\frac{\sigma}{8}} \end{bmatrix}$$

producing a real lattice $\mathcal{L}_2$. which contains the points O (o,o,o) and I (1,1,0).

Now we project $\mathcal{L}_1$ into the 2-dimensional lattice $\mathcal{L}_3$ in the hyperplane perpendicular to OI. By Minkowski's Theorem on Convex Bodies we see that there is a point of $\mathcal{L}_3$ such that its distance ρ from OI satisfies

$$0 < \rho \leq \frac{2}{\sqrt{3}} \det \mathcal{L}_3$$

If $(\alpha, \beta+i\gamma, \beta-i\gamma)$ is the corresponding point of $\mathcal{L}_1$ then

$$\rho^2 = \alpha^2+\beta^2 - \tfrac{1}{2}(\alpha+\beta)^2 + \frac{\sigma\gamma^2}{2}$$

$$= \frac{(\alpha-\beta)^2+\sigma\gamma^2}{2}$$

Now $\det \mathcal{L}_3 = \frac{1}{\sqrt{2}}\cdot\det\mathcal{L}_2 = \frac{1}{\sqrt{2}}\cdot\sqrt{\frac{\sigma}{8}}\cdot\sqrt{-\Delta}$

$$= \frac{\sqrt{-\sigma\Delta}}{4}$$

and so $S = 2\rho^2 \leq 2\cdot\frac{2}{\sqrt{3}}\cdot\frac{\sqrt{-\sigma\Delta}}{4}$

$$= \sqrt{\frac{-\sigma\Delta}{3}}$$

1.2 We now choose Δ_0, so that we wish to find all complex cubic fields with discriminant greater than Δ_0. $S_0 = \left(\frac{-\sigma\Delta_0}{3}\right)^{\frac{1}{2}}$ is obtained from the theorem and we consider all polynomials with $S < S_0$. These polynomials will have discriminants greater than or equal to Δ_1. We will choose σ so that $|\Delta_1|$ is as small as possible, hoping that this will maximize the proportion of polynomials for which the zeros yield fields with discriminants not less than $|\Delta_0|$. However, there being no relationship between polynomials and their corresponding fields this need not be true.

To find Δ_1 we maximise

$$\sqrt{-\Delta} = 2\gamma\left((\alpha-\beta)^2+\gamma^2\right) \qquad \text{subject to}$$

$$\sqrt{3}\,S = \sqrt{3}\left((\alpha-\beta)^2+\sigma\gamma^2\right) = \sqrt{-\sigma\Delta_0}$$

i.e. maximise $2\gamma(\xi^2+\gamma^2)$ subject to $\xi^2+\sigma\gamma^2 = \sqrt{\frac{-\sigma\Delta}{3}} = \lambda^2$

Let $\xi = \lambda\cos\theta \qquad \gamma = \frac{\lambda}{\sqrt{\sigma}}\sin\theta$

Then $$\sqrt{-\Delta} = \frac{2\lambda\sin\theta}{\sqrt{\sigma}} \cdot \left(\lambda^2\cos^2\theta + \frac{\lambda^2}{\sigma}\sin^2\theta\right)$$

$$= \frac{2\lambda^3}{\sqrt{\sigma}} \cdot \left(\cos^2\theta\sin\theta + \frac{\sin^3\theta}{\sigma}\right)$$

This has maximum or minimum at

$$\cos\theta = 0 \qquad \text{and} \qquad \tan^2\theta = \frac{\sigma}{2\sigma-3}$$

i) if $\cos\theta = 0$ $\qquad \xi = 0 \qquad \gamma = \frac{\lambda}{\sqrt{\sigma}}$

and so $$\sqrt{-\Delta} = 2\gamma^3 = \frac{2\lambda^3}{\sigma\sqrt{\sigma}}$$

$$= \frac{2\sigma^{\frac{3}{4}}\Delta_0^{\frac{3}{4}}}{\sigma\sqrt{\sigma}\;3^{3/4}}$$

$$= 2\left(\frac{\Delta_0}{3\sigma}\right)^{3/4}$$

ii) if $\tan^2\theta = \frac{\sigma}{2\sigma-3}$ then $\cos\theta = \frac{\sqrt{2\sigma-3}}{\sqrt{3\sigma-3}}$ $\qquad \sin\theta = \frac{\sqrt{\sigma}}{\sqrt{3\sigma-3}}$

and $$\sqrt{-\Delta} = \frac{2\lambda^3\sqrt{\sigma}}{\sqrt{\sigma}\;\sqrt{3\sigma-3}} \cdot \left(\frac{2\sigma-3}{3\sigma-3} + \frac{1}{3\sigma-3}\right)$$

$$= \frac{2\lambda^3}{\sqrt{3}\;\sqrt{\sigma-1}} \cdot \frac{2}{3} = \frac{4}{3\sqrt{3}} \cdot \frac{\sigma^{3/4}\,\Delta_0^{3/4}}{3^{3/4}\,\sqrt{\sigma-1}}$$

$$= \frac{4}{\sqrt{\sigma-1}} \cdot \left(\frac{\Delta_0\sigma}{27}\right)^{3/4}$$

$$\text{Max}\,\sqrt{-\Delta} = \text{Max}\left(\frac{4}{\sqrt{\sigma-1}} \cdot \left(\frac{\Delta_0\sigma}{27}\right)^{3/4},\ 2\left(\frac{\Delta_0}{3\sigma}\right)^{3/4}\right)$$

and for positive integral values of σ, this takes a minimum at $\sigma = 3$.

1.3 Let a field of discriminant Δ be generated by a zero of a polynomial P(x), with discriminant D. Then $D = \Delta k^2$, where k is called the index of P.

We now produce a bound for k

We have $D = -4\gamma^2((\alpha-\beta)^2+\gamma^2)^2$ and $S = (\alpha-\beta)^2 + \sigma\gamma^2$ where again we assume σ is an arbitrary rational integer.

$$S < -\frac{\sigma\Delta}{3} = -\frac{\sigma D}{3k^2}$$

$$\therefore \quad k^2 < \frac{4\sigma\gamma^2}{3} \cdot \left(1 - \frac{(\sigma-1)}{S}\right)^2$$

and since $(\sigma-1)\gamma^2 < S$ the r.h.s. has a maximum when

$$\gamma^2 = \sqrt{\frac{-D}{3}} \cdot \frac{1}{3(\sigma-1)K}$$

i.e. $$k^2 \leq \frac{16}{81\sqrt{3}} \cdot \frac{\sigma\sqrt{-\sigma D}}{(\sigma-1)\ K}$$

$$= \frac{16}{81\sqrt{3}} \cdot \frac{\sigma\sqrt{-\sigma\Delta}}{(\sigma-1)}$$

The r.h.s. has a minimum at $\sigma = 3$, and so this reinforces our original choice of σ giving $k^2 \leq \left(\frac{2}{3}\right)^3 \sqrt{-\Delta}$

1.4 In this section, bounds for the polynomial coefficients, which we dependent on the discriminant of the field, are produced. Consider the field generated by one of the roats $\alpha, \beta \pm i\gamma$ of $x^3 - ax^2 + bx - c = 0$. We may assume without loss of generality that $0 < \alpha < 1$, $0 < \beta$ since any polynomial may be transformed into one of this type by the substitution $y = \pm x + n$ where n is a rational integer.

Now
$$a = \alpha + 2\beta$$
$$b = 2\alpha\beta + \beta^2 + \gamma^2$$
$$c = \alpha(\beta^2 + \gamma^2)$$

Thus a, b, c are greater than zero. We now consider the case when a = 1 i.e. $P(x) = x^3 - x^2 + bx - c$, which has zeros $\alpha, \beta \pm i\gamma$. Thus the polynomial with zeros $(1-\alpha), (1-\beta) \pm i\gamma$ is $Q(x) = x^3 - 2x^2 + (b+1)x$

- (1 - a + b - c). The discriminant of Q equals the discriminant of P and $S(1-\alpha, 1-\beta, \gamma) = S(\alpha, \beta, \gamma)$. Now $P(o) = - c < o$ and since $P(x)$ cuts the x axis only once, between 0 and 1, then $P(1) > 0$ i.e. $1 - a + b - c > o$. Also $b + 1 > o$ and so $Q(x)$ satisfies all the conditions of the theorem. Thus we need only consider one of the cases a = 1 or a = 2, so we assume that $a \geq 2$, and $b, c \geq 1$ ......(1).

Now $4b - a^2 = 6\alpha\beta - \alpha^2 + 4\gamma^2 > 0$

Thus $b > \frac{a^2}{4}$ ......(2).

Now $S = (\alpha-\beta)^2 + 3\gamma^2 < |\Delta_0|^{\frac{1}{2}}$

Hence $a = \alpha+2\beta = 3\alpha+2(\beta-\alpha) \leq 3 + 2|\Delta_0|^{\frac{1}{2}}$ ......(3)

Also $(\alpha-\beta)^2 = a^2 - 3b + 3\gamma^2 \geq 0$

and so $S = |a^2-3b+6\gamma^2| \geq |a^2-3b|$ which implies $|\Delta_0|^{\frac{1}{2}} \geq |a^2-3b|$

i.e. $\frac{a^2 - |\Delta_0|^{\frac{1}{2}}}{3} \leq b \leq \frac{a^2 + |\Delta_0|^{\frac{1}{2}}}{3}$ ......(4)

If $a \geq 3$ this result can be sharpened to

$$b \leq \frac{a^2+|\Delta_0|^{\frac{1}{2}}}{3} - \frac{(a-3)^2}{6} \qquad ......(4a)$$

since $b = 2\alpha\beta + \beta^2 + \gamma^2 \leq 2\beta\alpha + \beta^2 + \frac{|\Delta_0|^{\frac{1}{2}} - (\alpha-\beta)^2}{3}$

$$= \frac{a^2 + |\Delta_0|^{\frac{1}{2}}}{3} - \frac{2}{3}(\alpha-\beta)^2$$

and $\beta - \alpha > \frac{a-3}{2}$ from (3)

Since a polynomial has only one real zero and this is in the interval $[0,1]$ we have,

$$P(0) = -c < 0$$

$$P(1) = 1 + b - a - c \geq 1$$

so $$c \leq b + a \qquad \ldots\ldots(5)$$

1.5 If a polynomial $P(x)$ satisfies these conditions, it is automatically irreducible, and if it has discriminant D then its zeros generate a cubic field $K(\theta)$, with discriminant $\Delta = \frac{D}{k^2}$

If Δ_0 is taken as -20,000 then we see that $S^2 \leq 20{,}000$ and $k \leq 6$. We now give a method of finding the index and discriminant of P, if its coefficients lie within the given bounds. To find k we first find the number k' so that $\frac{D}{k'^2}$ is square free and check to see if the factors of k' divide the index of P. This is done in three stages:-

i) In order to find if a prime p divides the index of a polynomial $P(x)$ we use a theorem found in Bachmann (2), which states:-

The necessary and sufficient condition for p to divide the index of P is that if $P(x) = H(x) - pM(x)$, then some repeated factor of H divides M modulo p. Suppose $P(x) = x^3 - ax^2 + bx - c$ and $P'(x) = 3x^2 - 2ax + b$ then any repeated factor $x - x_1$ of $H(x)$ must be a repeated factor of P mod p and so

$$P'(x_1) \equiv 0 \bmod p$$

Now $H(x_1) \equiv 0 \bmod p^2$ and, since $M(x_1) \equiv 0 \bmod p$, we have $P(x_1) \equiv 0 \bmod p^2$. Thus we find all the solutions of $P'(x) \equiv 0 \bmod p$ and then we know that one of these solutions will satisfy $P(x) \equiv 0 \bmod p^2$ if and only if p divides the index of P.

ii) If we have discovered that $p|k$, and if p^2/k', we now need to know if $p^2|k$. To do this we check if any of the numbers $\frac{\theta^2+d\theta+e}{p^2}$ $0 \leq d, e, \leq p^2 - 1$ satisfies a monic cubic polynomial equation with rational integral coefficients i.e. we see if any of these numbers are algebraic integers.

If $p^2 | k$ and $p^3 | k'$ we need to check if there is an algebraic integer of the form $\frac{\theta^2+d\theta+e}{p^3}$ $0 \leq d, e \leq p^3 - 1$ in the above manner. If one does not exist this does not necessarily mean $p^3 \nmid k$. We now must use iii).

iii) Here we check for an algebraic integer of the form $\frac{\theta+j}{p}$ $0 \leq j \leq p - 1$ in a manner similar to ii). We need not check if higher powers of p divide the index of P since by the choice of σ we know that $k \leq 6$.

1.6 It remains to test if fields with the same discriminant are in fact the same field. This is done with the knowledge of the zeros of the polynomials $P(x)$, $Q(x)$ which generate the fields, and an integral basis for one of them.

If the zeros of P, Q are respectively $\alpha, \beta \pm i\gamma$; $\alpha', \beta' \pm i\gamma'$ and an integral basis of the first field is $\left[1, \theta, \frac{\theta^2+d\theta+e}{k}\right]$ where θ is one of the zeros of $P(x)$.

If the fields are the same there will exist rational integral r, s, t so that
$$\alpha' = \frac{r\,(\alpha^2+d\alpha+e)}{k} + s\alpha + t$$
$$\beta'+i\gamma' = \frac{r\,((\beta\pm i\gamma)^2+d\,(\beta\pm i\gamma)+e)}{k} + s\,(\beta\pm i\gamma)+t$$

and from these relations two possible sets of triads r, s, t can be found, and if they are rational integers then the fields would be the same.

1.7 A theorem of Hasse (23), a description of which is to be found in Chapter 2, was used as a final check, to see if all the required fields had in fact been found. This theorem finds how many non-conjugate fields exist with discriminant D, by considering the uniquely defined quadratic field with discriminant d and the ideal groups of index 3 within this number field. Here $D = df^2$ where d is square free or of the form $4d'$ and d' is square free and f a rational integer.

This theorem confirmed that there were 3169 non-conjugate complex cubic number fields with discriminant D in the range $-20{,}000 \leq D \leq 0$.

There are 2853 discriminants with 1 associated non-conjugate field
27 discriminants with 2 associated non-conjugate fields
58 discriminants with 3 associated non-conjugate fields
22 discriminants with 4 associated non-conjugate fields -

CHAPTER 2

Hasse's Theorem's on the number of cubic fields of given discriminant.

This Chapter states Hasse's results without their proof. The theorems answer the question, if $D \neq 0$ is a rational integer which is $\equiv 0$ or $1 \bmod 4$, when is it the discriminant of at least one cubic field, and how many such fields, $N(D)$, are there.

Hasse first produces a necessary condition for $N(D) > 0$.

Theorem 2.1 If $D = df^2$, where d is the discriminant of a quadratic field Q, and f is a rational integer then either a) $f = p_1 \, p_2 \, \ldots\ldots \, p_n$

or b) $f = p_1 p_2 \, \ldots\ldots \, p_n \; 3^w$

$w = 1$ or 2

and where p_i $(i = 1, \ldots\ldots n : n \geq o)$ are rational primes, not equal to 3, such that $p_i \equiv \frac{d}{p_i} \bmod 3$ (Kronecker symbol)

In case b) we also have the conditions

if $d \not\equiv 0 \bmod 3$ then $w = 2$

if $d \equiv 3 \bmod 9$ then $w = 1$

or if $d \equiv -3 \bmod 9$ then $w = 1$ or 2

Let e be the number of ideal classes of index 3 prime to f in Q, then we have the theorem.

Theorem 2.2

If $f = 1$ then $N(D) = \dfrac{3^e - 1}{2}$

If $f > 1$ then the calculation is more involved. For each $p_i \neq 3$ we choose a number ρ_i such that:

$$\rho_i \equiv \text{ a primitive root mod } \mathfrak{p}_i$$

and $$\rho_i \equiv 1 \bmod \frac{f}{\mathfrak{p}_i}$$

where $\mathfrak{p}_i$ is one of the prime divisors of p_i in Q.

We also choose δ of these ρ's in the case where $3 | f$. In case a) thus, $\delta = 0$ however in case b) we have

$b_1)$ $d \equiv 0 \bmod 3$; $w = 2$ then $\delta = 1$ and

$\rho_{n+1} \equiv 1 + 3\sqrt{d} \bmod 9$; $\rho_{n+1} \equiv 1 \bmod \frac{f}{9}$

$b_2)$ $d \equiv \pm 3 \bmod 9$; \ $w = 1$ then $\delta = 1$ and

$\rho_{n+1} \equiv 1 + \sqrt{d} \bmod 3$; $\rho_{n+1} \equiv 1 \bmod \frac{f}{3}$

$b_3)$ $d \equiv -3 \bmod 9$; $W = 2$ then $\delta = 2$ and

$\rho_{n+1} \equiv 1 + 3\sqrt{d} \bmod 9$; $\rho_{n+1} \equiv 1 \bmod \frac{f}{9}$

$\rho_{n+2} \equiv 1 + \sqrt{d} \bmod 9$; $\rho_{n+2} \equiv 1 \bmod \frac{f}{9}$

Let Z be the number group of all $\alpha_0^3 r \gamma$, where α_0 is a prime number in Q, r is a rational number prime to f, and $\gamma \equiv 1 \bmod f$ is in Q. Then $\prod_{i=1}^{n+\delta} \rho_i^{y_i}$ ($y_i = 0, 1, 2$) represents each number in Q, prime to f modulo Z. Let $\mathfrak{R}_i$ ($i = 1, \ldots\ldots, e : e \geq 0$) be a basis of the ideal groups modulo 3 prime to f. Consider $\varepsilon_k = \mathfrak{R}_k^3$ and l = e, or if the field has discriminant positive or equal to -3, we put l = e + 1, and ε_l is set to the fundamental unit of the field. We find $y_{ik} = 1, \ldots\ldots, n + \delta$ $k = 1, \ldots\ldots, l$ such that

$$\varepsilon_k \sim \sum_{i=1}^{n+\delta} \rho_i^{y_{ik}} \qquad (Z)$$

These values of y_{ik} now give us the answer to our question.

Theorem 2.3

If L(D) is the number of non-proportional solutions $(Y_1 \,\ldots\ldots, Y_{n+\delta})$ of $\sum_{i=1}^{n+\delta} y_{ik} Y_i \equiv 0 \bmod 3 \quad k = 1, \ldots\ldots, l$ and $Y_i \neq 0$ for all $i = 1 \ldots\ldots n + 1$.

Then $N(D) = 3^e \,.\, L(D)$

Corollary If $y_{ik} = 0$ for all i, k we have

$$N(D) = 3^e \,.\, 2^{n+\delta-1} \quad \text{if} \quad \delta \neq 2$$

$$N(D) = 3^{e+1} \,.\, 2^n \quad \text{if} \quad \delta = 2$$

CHAPTER 3

The Calculation of Class Numbers of Algebraic Number Fields

3.1 An algorithm for calculating the class number of cubic fields is given by Voronoi (Delone and Faddeev (12)). A brief summary and explanation of the algorithm for the complex cubic case is given in Chapter 4.

This chapter describes what are known as relative minima of a lattice, shows some of the properties of these points, and gives a connection between sets or 'productions' of these relative minima and the class numbers of the field containing the lattice.

Finally, it is shown how the algorithm in the case of real quadratic fields reduces to finding chains of Hermite-Reduced Ideals i.e. chains of reduced ideals related by the continued fraction algorithm (see Bachmann (3)).

3.2 Let the algebraic number field K(θ) be generated by a zero ϑ of the polynomial

$$f\ (x) = x^{n} - a_{n-1}\ .\ x^{n-1} + \ldots\ldots + (-1)^{n}\ a_{o}$$

Let the zeros of f be α_1 , ... , α_r (real) and $\beta_1 \pm i\gamma_1, \cdots, \beta_s \pm i\gamma_s$

We consider the space Y with general point $(\alpha_1, \cdots, \alpha_r, \beta_1 + i\gamma_1, \cdots, \beta_s + i\gamma_s)$

Let ϕ = P(θ) = $b_{n-1}\theta^{n-1} + \cdots + b_0$ be a number in K(ϑ), and let $\underline{\phi}$ denote the point (P(α_1), ... , P($\beta_s + i\gamma_s$)) of Y. We shall distinguish between a polynomial and the associated point of Y by underlining it in this way.

Let $T_{r,s}$ be the set of points $\underline{\phi}$, where ϕ is any point of K(θ). The isomorphism $\phi \Leftrightarrow \underline{\phi}$ establishes an isomorphism K(ϑ) $\Leftrightarrow T_{r,s}$. Let Kr,s be the space (x_1, ..., x_r, y_1 + iz, ..., y_s + iz_s)

where $x_1, y_1, z_i \in \mathbb{R}$, the real numbers. Then $K_{r,s} \supset T_{r,s}$ Addition, subtraction, multiplication and division are defined componentwise in both $K_{r,s}$ and $T_{r,s}$. If $\underline{t} = (x_1, \ldots\ldots x_r, y_1 + iz_1, \ldots\ldots y_s + iz_s) \in K_{r,s}$, define the r + s directional parameters ρ_j thus

$$\rho_j(t) = |x_j| \qquad 1 \leq j \leq r$$

$$= y_{j-r}^2 + z_{j-r}^2 \qquad r + 1 \leq j \leq r + s$$

The ρ_j's are multiplicative.

We define the normed body of a point $\underline{\eta} \in T_{r,s}$ to be the region $V \subset K_{r,s}$ where

$$V = \{ \underline{t} : \underline{t} \in K_{r,s}, \rho_j(\underline{t}) < \rho_j(\underline{\eta}) \ ; \quad 1 \leq j \leq r + s \}$$

Now we consider multiplicative lattices in $T_{r,s}$ i.e. lattices S, such that the product of any two points of S, also belong to S.

If $\underline{\alpha} \in S$ then the totality of points $\{ \underline{\alpha}\underline{\gamma} \ ; \underline{\gamma} \in S \}$ is also in S and is thus a multiplicative lattice S'; we write S' = $\underline{\alpha}$ S and we define point-lattices multiplication as such.

If there exists a multiplicative lattice S" such that S = $\underline{\alpha}$ S" then we define point-lattice division by $\frac{1}{\underline{\alpha}}$ S = S"

A point of such a lattice S in $T_{r,s}$ is called a relative minimum of S if its normed body contains no other point of S apart from the origin. Diagram 3.1 gives an example of such points. The dotted lines show the integral lattice of the quadratic field generated by a zero ω of the polynomial $P(x) = x^2 - 14$. i.e. the points $(n\omega + m, n\bar{\omega} + m)$ where $\omega = \sqrt{14}$, $\bar{\omega} = -\sqrt{14}$ and n, m take all rational integral values. Five relative minimice are shown, viz $\underline{1}$, $\underline{\omega + 3}$, $\underline{\omega + 4}$, $\underline{3\omega + 11}$, $\underline{4\omega + 15} = \underline{\varepsilon}$ the fundamental automorphism of the lattice.

Half of the normed body (i.e. that part with positive first coordinate)

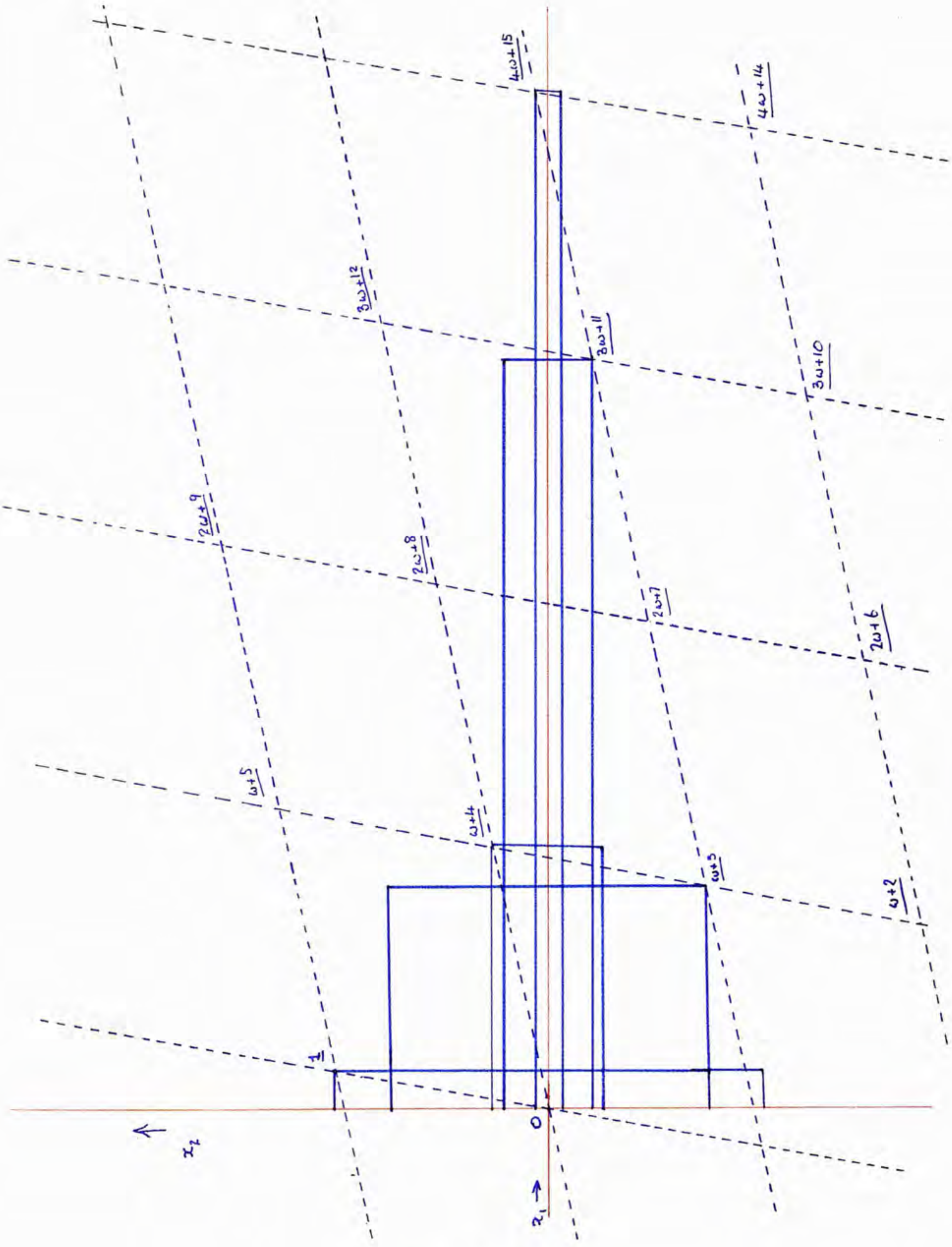


Diagram 3.1

of each of these relative minima is shown by a continuous line. This is all that is required since the lattice is symmetric about the line OI. From the diagram it is seen that I = $\underline{1}$, $\underline{\omega+3}$, $\underline{\omega+4}$, $\underline{3\omega+11}$, $\underline{4\omega+15}$ are relative minima, whereas $\underline{2\omega+7}$ = (14.48 ..., - 0.52 ...) is not since its normed body contains $\underline{\omega+4}$ = (7.74 ..., 0.26 ...).

3.3 If $\underline{\Omega}$ is a relative minimum of S, then we consider the region V(d) defined by

$$\left.\begin{array}{ll} V(d) = \underline{t} : \rho_j(\underline{t}) < \rho_j(\underline{\Omega}) \ , \ j \neq J & \text{for some } J \text{ such that} \\ & \quad 1 \leq J \leq r+s \\ \quad : \rho_J(\underline{t}) \leq \rho_J(\underline{\Omega}) + d \qquad d > 0 \quad d \in \mathbb{R} & \end{array}\right\} (a)$$

As d increases from zero, Minkowski's convex body theorem tells us there is a lattice point, say $\underline{\Omega}_1$, which lies in V(d) for some d > 0. If $\underline{\Omega}_1$ is the first point obtained by increasing d from zero then the normed body of $\underline{\Omega}_1$ contains no other point of S apart from the origin.

Now $\underline{t}$ and $-\underline{t}$ satisfy the same conditions for $\underline{\Omega}_1$, as do the points $\underline{\omega}^k . \underline{t}$, if K(ϑ) contains a root of unity ω. We can define $\underline{\Omega}_1$ to lie in a certain region which will uniquely determine its choice, as follows

If $1 \leq j \leq r$ choose the region of space such that $x_j \geq 0$

If $r + 1 \leq j \leq r + s$ and if the field contains k roots of unity, choose the region such that

$$-\frac{\pi}{k} < \arg(Y_j + iZ_j) < \frac{\pi}{k}$$

Hence $\underline{\Omega}_1$ is a uniquely determined relative minimum.

Repeating this process we get an infinite sequence of relative minima

Voronoi proves that we may point - lattice - divide S successively by these relative minima and get a sequence of lattices

$$S_0 = \frac{S}{\underline{\Omega}_0} , \quad S_1 = \frac{S}{\underline{\Omega}_1} , \dots , \quad S_p = \frac{S}{\underline{\Omega}_p}$$

and that the above method produces only a finite number of different lattices. Thus the sequence of lattices $S_0 , S_1 , \cdots , S_p$ must have two lattices the same.

Suppose S_k is the first lattice to be repeated, say for the first time in S_{k+m} . Then $\underline{\varepsilon}_1 = \underline{\Omega}_{k+m} / \underline{\Omega}_k$ is a multiplicative automorphism for S. $\underline{\varepsilon}_1$ belongs to S_k and is the mth relative minimum in the chain generated by $\underline{I}$ = (1, 1, 1, ... , 1), where $\underline{I}$ must be a relative minimum of S_k.

Therefore we have a chain of relative minima

$$\underline{\Phi} = \underline{I} , \underline{\Phi}_1 , \cdots , \underline{\Phi}_m , \underline{\Phi}_{m+1} , \cdots$$

where $\underline{\Phi}_i = \dfrac{\underline{\Omega}_{k+i}}{\underline{\Omega}_k}$ and $\underline{\Phi}_m = \underline{\varepsilon}_1$ (b)

since $\underline{\Phi}_0 = \underline{I}$ goes into $\underline{\varepsilon}_1 = \underline{\varepsilon}_1 \underline{\Phi}_0 = \underline{\Phi}_m$

then $\underline{\Phi}_{m+q} = \underline{\varepsilon}_1 \cdot \underline{\Phi}_q$ (c)

Thus the sequence of relative minima is of the form

$$\underline{\Phi}_0 = \underline{I} , \underline{\Phi}_1 , \cdots , \underline{\Phi}_{m-1} , \underline{\varepsilon}_1 , \underline{\varepsilon}_1 \underline{\Phi}_1 , \cdots , \underline{\varepsilon}_1 \underline{\Phi}_{m-1} , \underline{\varepsilon}_1^2 , \cdots$$

Using (b) and (c) we can extend the chain in the opposite direction to get a two-way infinite chain of relative minima.

$\underline{\Phi}_1 , \cdots , \underline{\Phi}_m$ are called the principal relative minima of direction J.

Thus starting at a multiplicative lattice S we get a sequence of lattices

$$S = S_0 , S_1 , \cdots , S_k , \cdots , S_{m-1+k} , S_{m+k} , \cdots$$

The set of lattices $S_k, \dots, S_{k+m-1}$ is called a loop of lattices. Starting at a lattice, which belongs to a loop, using the above process, we naturally enter the same loop.

Suppose we consider the loop of lattices $R_1, \dots, R_m$ where the principal relative minima of R_1 are $\underline{\Phi}_1, \dots, \underline{\Phi}_m = \underline{\varepsilon}_1$. If we start with a lattice R_i whose principal relative minima are $\underline{\theta}_1, \dots, \underline{\theta}_m = \underline{\varepsilon}_1$ then we know that $R_{i+l} = \dfrac{R_i}{\underline{\theta}_{i+l-1}}$ and $R_i = \dfrac{R_1}{\underline{\Phi}_{i-1}}$

hence
$$R_i = \frac{R_1}{\underline{\theta}_{i+l-1} \cdot \underline{\Phi}_{i-1}}$$
$$= \frac{R_1}{\underline{\Phi}_{i+l-1}}$$

and so
$$\underline{\theta}_{i+l-1} = \frac{\underline{\Phi}_{i+l-1}}{\underline{\Phi}_{i-1}}$$

The two way infinite chain of relative minima in direction d_1 is called a d_1 - chain of relative minima.

3.4 Suppose we have a point $\underline{\eta} \in T_{r,s}$, and define the norm of $\underline{\eta}$, $N(\underline{\eta})$, to be
$$N(\underline{\eta}) = \prod_{j=1}^{r+s} \rho_j(\underline{\eta})$$
If η is the algebraic number corresponding to $\underline{\eta}$ then
$$N(\underline{\eta}) = |\,Norm\,(\eta)|$$
Hence the multiplicity of norm, N, follows; and no ambiguity arises between the definition of the norm of a point in $T_{r,s}$ and the norm of an algebraic number in $K(\theta)$.

Lemma 3.1 If $\underline{\alpha}$ and $\underline{\beta}$ are relative minima of a lattice S, then $\dfrac{\underline{\beta}}{\underline{\alpha}}$ is a relative minima of the lattice $\dfrac{S}{\underline{\alpha}}$.

<u>Proof</u> Suppose $\frac{\beta}{\underline{\alpha}}$ is not a relative minimum of $\frac{S}{\underline{\alpha}}$ i.e. $\exists$ a relative minimum $\underline{\gamma} \in \frac{S}{\underline{\alpha}}$ such that

$$\rho_i(\underline{\gamma}) < \rho_i\left(\frac{\beta}{\underline{\alpha}}\right) \qquad \text{for all } i = 1, \ldots\ldots r + s$$

i.e. $\quad \rho_i(\underline{\gamma}).\rho_i(\underline{\alpha}) < \rho_i(\beta)$

hence $\quad \rho_i(\underline{\gamma}\cdot\underline{\alpha}) < \rho_i(\beta) \qquad$ for all $i = 1, \ldots\ldots r + s$

and since $\underline{\gamma}\cdot\underline{\alpha}$ belongs to S, since $\underline{\gamma} \in \frac{S}{\underline{\alpha}}$ we have is not a relative minimum of S, a contradiction.

For a relative minimum $\underline{\alpha}$ of a lattice S we define the <u>production</u> of $\underline{\alpha}$ in S, PROD $(\underline{\alpha})_S$ as follows. We choose (r + s - 1) directions $d_1, \ldots\ldots, dr + s - 1$ and first starting from $\underline{\alpha}$ in the d_1 direction produce a d_1 - chain a relative minima. Then from each of these relative minima produce d_2 - chains of relative minima, and so on in the remaining directions. The totality of relative minima produced in this way is then called the production of $\underline{\alpha}$ in S. The production depends on the order in which we take directions, and we suppose that we fix a definite order on these directions.

Similarly to lemma3.1 we may prove

$$\text{PROD } (\underline{\alpha})_S \quad = \quad \text{PROD } (\underline{1})_{S/\alpha}$$

<u>Lemma 3.2</u> If, in a lattice S, we have a unit $\underline{\varepsilon}$, then

$$\text{PROD } (\underline{\varepsilon})_S \quad = \underline{\varepsilon}\,.\,\text{PROD } (\underline{1})_S$$

<u>Proof</u> Suppose the next relative minimum to $\underline{\gamma} \in$ PROD $(\underline{1})_S$ in the d_i direction, is $\underline{\alpha}$, and the next relative minimum from $\underline{\varepsilon}\,\underline{\gamma}$ in the d_i direction is β .

If $\underline{\alpha}\cdot\underline{\varepsilon} \neq \beta$ then

$\rho_i(\beta\cdot\underline{\varepsilon}^{-1}) \leq \rho_i(\underline{\alpha})$ since otherwise $\underline{\alpha}\cdot\underline{\varepsilon}$ would be the next relative minimum to $\underline{\varepsilon}\cdot\underline{\gamma}$ in the d_i direction.

But $\rho_i(\underline{\alpha}) \leq \rho_i(\beta\cdot\underline{\varepsilon}^{-1})$ since otherwise $\beta\cdot\varepsilon^{-1}$ would be the next relative minimum of $\underline{1}$ in the d_i direction.

i.e. $\rho_i(\underline{\alpha}) = \rho_i(\underline{\beta} \cdot \underline{\varepsilon}^{-1})$

This is only so if $\underline{\alpha} = \underline{\beta} \cdot \underline{\varepsilon}^{-1}$, a contradiction.

Thus starting with $\underline{\gamma} = \underline{1}$ we prove, the lemma.

Theorem 3.1

Given two equivalent lattices P, Q in K(ϑ), there exist relative minima $\underline{\phi}', \underline{\psi}'$ of P, Q respectively where

$N(\underline{\phi}') = \text{Min}(N(\underline{\phi})) : \underline{\phi}$ a relative minimum of P

$N(\underline{\psi}') = \text{Min}(N(\underline{\psi})) : \underline{\psi}$ a relative minimum of Q

such that $\underline{\psi}' P = \underline{\phi}' Q$

Proof P, Q are equivalent, i.e. there exist $\alpha, \beta \in K(\vartheta)$ such that $\underline{\alpha} P = \underline{\beta}\ Q$

Let $\underline{\Phi}$ be a relative minimum of P with minimum norm, and $\underline{\Psi}$ be a relative minimum of Q with minimum norm.

There exist $\underline{\phi} \in P$ and $\underline{\psi} \in Q$ such that

$$\underline{\alpha} \cdot \underline{\phi} = \underline{\beta} \cdot \underline{\Psi} \qquad \text{...... (1)}$$

$$\underline{\alpha} \cdot \underline{\Phi} = \underline{\beta} \cdot \underline{\psi} \qquad \text{...... (2)}$$

Hence $\underline{\alpha}\, \underline{\beta}\, \underline{\phi}\, \underline{\psi} = \underline{\alpha}\, \underline{\beta}\, \underline{\Psi}\, \underline{\Phi}$

Since norms are multiplicative we have

$N(\underline{\phi})\ N(\underline{\psi}) = N(\underline{\Psi})\ N(\underline{\Phi})$

Hence either $N(\underline{\phi}) \leq N(\underline{\Phi})$ or $N(\underline{\psi}) \leq N(\underline{\Psi})$

If $N(\underline{\phi}) < N(\underline{\Phi})$ the normed body of $\underline{\phi}$ would contain a relative minimum of P, whose norm would thus be less than the norm of $\underline{\Phi}$ - a contradiction.

Hence $N(\underline{\phi}) = N(\underline{\Phi})$ and thus $N(\underline{\psi}) = N(\underline{\Psi})$

From (1) $\dfrac{\underline{\alpha}}{\underline{\beta}} = \dfrac{\underline{\Psi}}{\underline{\phi}}$

and hence $\underline{\Psi} P = \underline{\phi} Q$

and $\underline{\phi}, \underline{\Psi}$ satisfy the conditions of the theorem.

Given a production of relative minima of a lattice S, we point - lattice - divide S by these minima and the resulting set of lattices is called a lattice production in K (ϑ).

We consider the productions of relative minima connected by a unit to be the same since by Lemma 3.2, they give rise to the same lattice productions.

Corollary If there is only one production of relative minima in any lattice of K (ϑ) then the class number of the field K (ϑ) is the number of different lattice productions in the field.

Proof If two lattices belong to the same lattice production they are equivalent. By theorem 3.1 two lattices which are equivalent belong to the same lattice production.

3.5

Theorem 3.2 In any field of signature 1, every lattice contains only one production of relative minima.

Proof Since we have a field with signature 1, there are two parameter directions to be considered, say x and y. If $\underline{\Omega}$ is a relative minimum we let $\Omega^{(x)}$ $\Omega^{(y)}$ be the respective x and y directional parameters of $\underline{\Omega}$.

The production of a lattice S in this type of field reduces to a one-dimensional chain of the form $\{\underline{\Omega}_i\}$ $-\infty < i < \infty$ with the conditions $\Omega_{i+1}^{(x)} > \Omega_i^{(x)}$; $\Omega_{i+1}^{(y)} < \Omega_i^{(y)}$ such that there does not exist another point of the lattice S satisfying

$$\Omega_{i+1}^{(x)} > T^{(x)} > \Omega_i^{(x)}$$

$$\Omega_i^{(y)} > T^{(y)}$$

Let $\underline{\textcircled{H}}$ be any relative minima of S.

Let $\underline{\Omega}_j$ be that member of the chain of relative minima with largest x parameter less than $\textcircled{H}^{(x)}$

i.e. $\Omega_j^{(x)} < \textcircled{H}^{(x)} \leq \Omega_{j+1}^{(x)}$

Now if $\Omega_j^{(y)} \leq \textcircled{H}^{(y)}$ then $\textcircled{H}$ would not be a relative minimum,

hence $\textcircled{H}^{(y)} < \Omega_j^{(y)}$

and thus $\underline{\textcircled{H}} = \underline{\Omega}_{j+1}$

In a field K (θ), with signature 2 we consider 3 parameter directions, say x, y, z. If Ω is a point of K (θ), then $\Omega^{(x)}, \Omega^{(y)}, \Omega^{(z)}$ are the respective x, y, z parameters of $\underline{\Omega}$, x, y, z being arbitrary but fixed.

We now prove that every lattice in a field of signature 2 contains only one production of relative minima. What we prove in fact is that an x - chain from one relative minima always intersects a z - chain from any other relative minima.

The proof given is exactly equivalent to Voronoi's proof, but is stated algebraically as opposed to the latter geometric arguments.

<u>Lemma 3.3</u> There are no two members $\underline{\Omega}_i, \underline{\Omega}_j$ of any x - chain $\{\underline{\Omega}\}_x$ for which the following inequalities hold

$$\Omega_i^{(y)} < \Omega_j^{(y)}$$
$$\Omega_i^{(z)} > \Omega_j^{(z)}$$

<u>Proof</u> If $\Omega_i^{(x)} < \Omega_j^{(x)}$ then by the definition of x chains (§ 3.3) $\Omega_i^{(y)} > \Omega_j^{(y)}$ and $\Omega_i^{(z)} > \Omega_j^{(z)}$ contradicting one of the inequalities. A similar contradiction occurs if $\Omega_j^{(x)} < \Omega_i^{(x)}$

<u>Theorem 3.3</u> Two, two sided chains of relative minima of different directions have a common element.

<u>Proof</u> Let x - chain be $\{\underline{\Omega}\}_x$ and z - chain be $\{I\}_z$

In $\{\underline{T}\}_z$ there is an element $\underline{T}_i$ (i may be negative) such that

$$T_i^{(x)} > \Omega^{(x)}$$
$$T_i^{(y)} > \Omega^{(y)} \qquad \text{.....}\ (i)$$
$$T_i^{(z)} < \Omega^{(z)}$$

This is true since in a chain in one direction there are elements of arbitrary large size in the perpendicular directions.

Similarly $\exists\ \underline{\Omega}_k \in \{\underline{\Omega}\}_x$ such that

$$\Omega_k^{(x)} < T_i^{(x)}$$
$$\Omega_k^{(y)} > T_i^{(y)} \qquad \text{.....}\ (ii)$$
$$\Omega_k^{(z)} > T_i^{(z)}$$

Let $\underline{\Omega}_{j-1}$ be the relative minimum in $\{\underline{\Omega}_k\}_x$ with largest x coordinate satisfying similar conditions i.e.

$$\Omega_{j-1}^{(x)} < T_i^{(x)}$$
$$\Omega_{j-1}^{(y)} > T_i^{(y)} \qquad \text{.....}\ (iii)$$
$$\Omega_{j-1}^{(z)} > T_i^{(z)}$$

If $\Omega_j^{(x)} \geq T_i^{(x)}$ then we would have $\underline{T}_i = \underline{\Omega}_j$ by the definition of consecutive relative minima. Since the conditions

$$\Omega_j^{(x)} < T_i^{(x)}$$
$$\Omega_j^{(y)} < T_i^{(y)}$$
$$\Omega_j^{(z)} < T_i^{(z)}$$

contradict the fact that $\underline{T}_i$ is a relative minimum we have two possibilities

$$\Omega_j^{(x)} < T_i^{(x)}$$
$$\Omega_j^{(y)} < T_i^{(y)} \qquad \text{.....}\ (iv)$$
$$\Omega_j^{(z)} > T_i^{(z)}$$

$$\Omega_j^{(x)} < T_i^{(x)}$$
$$\Omega_j^{(y)} > T_i^{(y)} \qquad \text{.....}\ (v)$$
$$\Omega_j^{(z)} < T_i^{(z)}$$

We now show that (v) is incorrect. Assume the contrary.

Then $\{\underline{\Omega}\}_x$ has two elements $\underline{\Omega}$ and $\underline{\Omega}_j$ such that

$$\begin{aligned} \Omega^{(y)} &< T_i^{(y)} < \Omega_j^{(y)} \\ \Omega^{(z)} &> T_i^{(z)} > \Omega_j^{(z)} \end{aligned} \qquad \ldots\ldots \text{(vi)}$$

by equations (i) and (v), but this contradicts lemma 3.3.

Thus (iv) is the only possibility.

Now consider $\{\underline{T_i}\}_z$. Let $\underline{T}_\ell$ be that element of this z - chain with maximum z - coordinate less than $\Omega_j^{(z)}$

We have
$$T_\ell^{(z)} < \Omega_j^{(z)} \Rightarrow T_\ell^{(z)} < \Omega_{j-1}^{(z)}$$

and hence there are three possible cases.

$$\begin{aligned} \Omega_{j-1}^{(x)} &< T_\ell^{(x)} \\ \Omega_{j-1}^{(y)} &< T_\ell^{(y)} \end{aligned} \qquad \ldots\ldots \text{(vii)}$$

$$\begin{aligned} \Omega_{j-1}^{(x)} &< T_\ell^{(x)} \\ \Omega_{j-1}^{(y)} &> T_\ell^{(y)} \end{aligned} \qquad \ldots\ldots \text{(viii)}$$

and
$$\begin{aligned} \Omega_{j-1}^{(x)} &> T_\ell^{(x)} \\ \Omega_{j-1}^{(y)} &< T_\ell^{(y)} \end{aligned} \qquad \ldots\ldots \text{(ix)}$$

If (vii) is true then by the definition of ℓ, $\underline{T}_{\ell+1} = \underline{\Omega}_{j-1}$

and the chains have a common element.

If (ix) is true from (iii) and (ix) we have that

$$\begin{aligned} T_i^{(x)} &> \Omega_{j-1}^{(x)} > T_\ell^{(x)} \\ T_i^{(y)} &< \Omega_{j-1}^{(y)} < T_\ell^{(y)} \end{aligned} \qquad \ldots\ldots \text{(x)}$$

which contradicts lemma 3.3, leaving us with the possibility (viii).

In this case, if $\Omega_j^{(x)} \geq T_e^{(x)}$ we would necessarily have $\underline{T}_e = \underline{\Omega}_j$ and thus the chains have a common element.

So we assume that $\Omega_j^{(x)} < T_e^{(x)}$.

Also we know that $\Omega_j^{(y)} > T_e^{(y)}$ for otherwise $\underline{T}_{e+1} = \underline{\Omega}_j$

Thus

$$\begin{aligned} \Omega_j^{(x)} &< T_e^{(x)} \\ \Omega_j^{(y)} &> T_e^{(y)} \qquad \text{..... (xi)} \\ \Omega_j^{(z)} &> T_e^{(z)} \end{aligned}$$

So either the two chains have a common element or

$\exists\ \underline{\Omega}_i \in \{\underline{\Omega}\}_x$ and $\underline{T}_e, \underline{T}_i \in \{\underline{T}\}_z$ satisfying inequalities (iv) and (xi) and where

$$\begin{aligned} T_e^{(x)} &< T_i^{(x)} = c_1 \\ T_e^{(y)} &< \min(T_i^{(y)}, \Omega^{(y)}) = c_2 \\ T_e^{(z)} &< \Omega^{(z)} = c_3 \end{aligned}$$

Comparing (i) with (iv) and (ii) with (xi), we may repeat this argument to find our new relative minima

$\underline{\Omega}_{j'} \in \{\underline{\Omega}\}_x$ and $\underline{T}_{e'}, \underline{T}_{i'} \in \{\underline{T}\}_z$ such that

$$\begin{aligned} T_{e'}^{(x)} &< T_e^{(x)} < c_1 \\ T_{e'}^{(y)} &< c_2 \qquad \text{..... (xii)} \\ T_{e'}^{(z)} &< c_3 \end{aligned}$$

which again satisfy conditions similar to (iv) and (xi), or otherwise the chains have a common element. We may repeat this argument, and since there are only finitely many relative minima in a bounded range, then this procedure must eventually terminate. That is $\{\underline{\Omega}\}_x$ and $\{\underline{T}\}_z$ have a common element.

Thus we see that in fields of signature 1 or 2, every lattice has only one production of relative minima and hence, by the corollary to Theorem 3.1, the class number of any one of these fields is the number of different lattice productions in that field.

3.6 If we consider $K(\sqrt{d})$, the field generated by the positive root of $x^2 - d = 0 \quad d > 0$

let $\omega = \sqrt{d}$ if $d \equiv 2, 3 \mod (4)$

$= \frac{1 + \sqrt{d}}{2}$ if $d \equiv 1 \mod (4)$

Consider the ideals $[a', \omega + b']$ in $K(\sqrt{d})$ where $a' \mid N(\omega + b')$

We look at the fractional ideals $\left[1, \frac{\omega + b'}{a'}\right]$ similar to the original.

We consider relative minima in the direction of increasing x, x the direction of ω.

All points of the ideal lattice lie on lines parallel to OI through the points $\left(\frac{n(\omega + b')}{a'}, \frac{n(\bar{\omega} + b')}{a'} \right)$

for rational integral n.

Let two regions V_1, V_2 be defined

$$V_1 = \{ \underline{t} \in K_{2,0} : \underline{t} = (x_1, x_2) \quad -1 < x_2 < 0 \}$$

$$V_2 = \{ \underline{t} \in K_{2,0} : \underline{t} = (x_1, x_2) \quad 0 < x_2 < 1 \}$$

Except for the line through the origin, every line has one lattice point in V_1 and one in V_2.

Now on any line the point in V_1 has smaller x value than the point in V_2.

The relative minimum next to $(1, -1)$ must lie in V_1.

As we look in region $R(d) = \{ \underline{t} \in K_{2,0} : t^{(x)} \leq d , t^{(y)} \leq 1 , d \geq 1 \}$ and increasing d from 1 the next relative minimum must lie on a line through $\left(\frac{n(\omega + b')}{a'}, \frac{n(\bar{\omega} + b')}{a} \right) = M(n) \qquad n \geq 1$

If l is the distance from where the line through M (1) cuts the x axis, to the origin, then $\exists$ a point $\underline{\eta}$ lying on the line through M (1) in V_1 so that $1 < \eta^{(x)} < l$

and a point in V_1 lying on line through M (n) must have x parameter value at least $\frac{nl}{2}$

First relative minimum lies on a line through M (1) and is the unique point defined by $\left(\frac{\omega + b}{a} , \frac{\bar{\omega} + b}{a} \right)$

$$-1 < \frac{\bar{\omega} + b}{a} < 0 \quad \text{and} \quad \frac{\omega + b}{a} > 1$$

i.e. $$0 < -\bar{\omega} - b < a < \omega + b$$

the conditions for reduced ideals due to Hermite.

CHAPTER 4

A Description and Explanation of Voronoi's Algorithm

4.1 Voronoi (23) considers a 3-dimensional lattice, with general points $(\xi \pm i\eta, \zeta)$ and then transforms it into the real lattice S with general point (ξ, η, ζ). All points of S lie on lines parallel to the line through the points O (0, 0, 0) and I (1, 0, 1) and these lines, or "parallels" cut the $\xi - \eta$ plane in a 2-dimensional lattice T. We know (Delone and Faddeev (13), p.p. 459-464) that T has a basis $\underline{x}$, $\underline{y}$ such that triangles formed by the origin with pairs of $\underline{x}$, $\underline{y}$, $\underline{y}$-$\underline{x}$, -$\underline{x}$, -$\underline{y}$, $\underline{x}$-$\underline{y}$ taken cyclically are all acute-angled. Of these six triangles we choose that one which covers the negative ξ-axis, and suppose the basis points are $\underline{x}$ and $\underline{y}$. Let $\underline{z}$, (z_1, z_2) be a point of T. The lattice point of S, which lies on the parallel through $\underline{z}$ and has least positive ζ-coordinate, is called the pinhead of $\underline{z}$: let it be $\underline{z}$ + t(z) OI, and then we have $0 < t(z) < 1$. If $z \neq 0$, then $t(z) \neq 0$ since the ζ coordinate of the pinhead must be irrational.

Since - z - t(z) OI is a point of S we have that t(-z) = 1-t(z). The projection of $\underline{z}$ + t(z) OI onto T is $(z_1 + t(z), z_2)$ and is denoted by $\underline{z}'$. We denote by $|\underline{z}|$ the distance of $\underline{z}'$ from O, i.e. $|\underline{z}| = (z_1^2 + z_2^2)^{\frac{1}{2}}$. Since we assume that I is a relative minimum in the following proof, we have $|\underline{z}'| \geq 1$ for every $\underline{z}$ in T.

The next relative minimum is that pinhead $\underline{z}'$ for which $|\underline{z}'|$ is least. Voronoi's theorem states that it is one of the pinheads $A = \{\underline{x}', \underline{y}', (-\underline{x})', (-\underline{y})', (\underline{x}-\underline{y})', (\underline{y}-\underline{x})', (\underline{x}+\underline{y})'\}$. Since a proof of this theorem was not available to us, we give an independent proof. In the following sections $\underline{z}'$ will mean both the pinhead of $\underline{z}$, and the projection of the pinhead onto the $\xi - \eta$ plane as no ambiguity arises.

4.2

Lemma 4.1 $\min (|\underline{z}'|^{2}, |(-\underline{z})'|^{2}) < |\underline{z}|^{2}$ if $z_1 \le -\frac{1}{2}$

$< z_2^{2} + \frac{1}{4}$ if $-\frac{1}{2} \le z_1 \le 0$

Proof We have $(z_1 + t)^2 \lesseqgtr (- z_1 - t + 1)^2$ according as $t \lesseqgtr \frac{1}{2} - z_1$

Hence if $z_1 \le -\frac{1}{2}$ we have

$$\min ((z_1 + t)^2, (- z_1 - t + 1)^2) \le (z_1 + t)^2 < z_1^{2} \text{ for}$$

$0 < t < 1$

If $-\frac{1}{2} \le z_1 \le 0$ we have

$$\min ((z_1 + t)^2, (-z_1 - t + 1)^2) \le \max (z_1^{2}, \tfrac{1}{4}) = \tfrac{1}{4}$$

Now $\min (|\underline{z}'|^{2}, |(-\underline{z})'|^{2}) = \min ((z_1 + t(z))^2 + z_2^{2}, (- z_1 - t(z) + 1)^2 + z_2^{2})$

$$= z_2^{2} + \min ((z_1 + t(z))^2, (-z_1 - t(z) + 1)^2)$$

whence the result follows.

Since $|\underline{z}'|$ and $|(-\underline{z})'|$ are both greater than 1 we have

$$|\underline{z}|^{2} > 1 \qquad \text{if} \qquad z_1 \le -\tfrac{1}{2} \qquad \ldots (1)$$

and

$$z_2^{2} > \tfrac{3}{4} \qquad \text{if} \qquad -\tfrac{1}{2} \le z_1 \le 0 \qquad \ldots (2)$$

If $\underline{z}$ makes an angle ω with the negative ξ-axis, then

$$\text{if} \qquad \omega \le \pi/3 \qquad |\underline{z}| \ge 1 \qquad \ldots (3)$$

$$\text{if} \qquad \omega > \pi/3 \qquad |\underline{z}|^{2} > \tfrac{3}{4} \qquad \ldots (4)$$

Now let $\underline{x} = (- x \cos\theta , x \sin\theta)$ and $\underline{y} = (-y \cos\phi , -y \sin\phi)$ where $x = |\underline{x}|$, $y = |\underline{y}|$, $0 < \theta$, $0 < \phi$, $\theta + \phi < \frac{\pi}{2}$

θ is the angle made by $\underline{x}$ with the negative ξ-axis, and ϕ the angle made by $\underline{y}$ with the same axis, $\underline{x}$ and $\underline{y}$ being on opposite sides of this axis.

From (4) we have

$$x \; , \; y \quad > \quad \frac{3}{2} \qquad \ldots (5)$$

Also if $\theta \geq \pi/_3$ then from (5) $x > \cos\theta$

while if $\theta < \frac{\pi}{3}$ then (3) gives $x > 1$ and again $x > \cos\theta$

Thus $x > \cos\theta$ $\qquad \ldots (6)$

We now show that if $\theta \in \left] \frac{\pi}{3} , \frac{\pi}{2} \right[$ then

$$x - \cos\theta \quad > \quad \frac{1}{2} \qquad \ldots (7)$$

In the interval $\frac{\pi}{3} < \theta < \frac{\pi}{2}$ we have $| z_2 | > \frac{3}{2}$

i.e. $x \geq \dfrac{\sqrt{3}}{2 \sin\theta}$

Hence $x - \cos\theta \geq \dfrac{\sqrt{3}}{2\sin\theta} - \cos\theta$

Now $\dfrac{\sqrt{3}}{2\sin\theta} - \cos\theta$ attains a minimum at $\theta = \pi/_3$

in the interval $\frac{\pi}{3} \leq \theta \leq \frac{\pi}{2}$ with value $\frac{1}{2}$

If $0 < \theta < \frac{\pi}{3}$ then $x \cos\theta - t(x) > \cos\theta$ since $\underline{x}'$ lie inside the unit circle, and thus $\underline{I}$ would not be a relative minimum.

Thus $\qquad x\cos\theta - t(x) > \cos\theta > 0 \quad \ldots (8)$

<u>Lemma 4.2</u> Let $a\underline{x} + b\underline{y}$ be a point of T, not belonging to A, then there exists a point $\underline{z} \in$ A, such that

$$|(a\underline{x} + b\underline{y})'| > |\underline{z}'| \qquad \ldots (9)$$

<u>Proof</u> Case (1) $a.b > 0$

If $a < 0$ then $(a\underline{x} + b\underline{y})_\xi$, the ξ -coordinate of $(a\underline{x} + b\underline{y})$, is greater than zero. Hence

$$\begin{aligned} |(a\underline{x} + b\underline{y})'| &> |a\underline{x} + b\underline{y}| \\ &> (x^2 + y^2)^{\frac{1}{2}} \end{aligned}$$

since $\underline{x}$, $\underline{y}$ are sides of an acute angled triangle.

Thus $|(a\underline{x} + b\underline{y})'| > \mathrm{Min}\,(\cancel{x}^2, y^2) + \frac{1}{4}$ and at least one of the points $\pm x$, $\pm y$ of A satisfies (9) by Lemma 4.1. If $a > 0$ we assume first that $ax\cos\theta + by\cos\phi > 1$

Then $|(\underline{ax} + \underline{by})'|^2 = |\underline{ax} + \underline{by}|^2 + t^2 - 2|\underline{ax} + \underline{by}|\, t \cos|\omega|$ ... (10)

where $t = t(\underline{ax} + \underline{by})$ and ω is the angle made by $\underline{ax} + \underline{by}$ with the negative ξ-axis.

Since $ax \cos\theta + by \cos\phi > 1$ we know that

$$|(\underline{ax} + \underline{by})'|^2 \geq a^2x^2 + b^2y^2 + 1 - 2ax\cos\theta - 2by\cos\phi + 2abxy\cos(\theta+\phi) \quad \ldots (11)$$

If we fix $\theta+\phi$, we find the maximum value of $ax\cos\theta + by\cos\phi$ to be $(a^2x^2 + b^2y^2 + 2abxy\cos(\theta+\phi))^{\frac{1}{2}}$ and hence, from (11), we have

$$|(\underline{ax} + \underline{by})'|^2 \geq (a^2x^2 + b^2y^2 + 2abxy\cos(\theta+\phi)^{\frac{1}{2}} - 1)^2 \quad \ldots (12)$$

If a or b ≥ 2 and $1 \leq x \leq y$ then from (12) and $0<\theta+\phi<\frac{\pi}{2}$ we have

$$|(ax + by)'|^2 \geq (\sqrt{5}-1)^2 x^2 > \frac{5}{4}x^2$$
$$> x^2 + \frac{1}{4}$$

and so by lemma 4.1 one of $\pm \underline{x}$ satisfies (9).

If $x < 1$ using (3) we must have $\theta > \frac{\pi}{3}$ and hence $\phi < \frac{\pi}{6}$ which implies, again by (3), that $y > 1$. We still have that $x > \frac{\sqrt{3}}{2}$. From (12) we derive

$$|(\underline{ax} + \underline{by})'|^2 \geq \text{Min}\left[((4x^2 + 1)^{\frac{1}{2}} - 1)^2, ((x^2 + 4)^{\frac{1}{2}} - 1)^2\right] \quad \ldots (13)$$

and both of these variables are less than $x^2 + \frac{1}{4}$.

Hence $|(\underline{ax} + \underline{by})'|^2 \geq x^2 + \frac{1}{4} \geq \text{Min}(|\underline{x}'|^2, |(-\underline{x})'|^2)$

and thus one of $\pm \underline{x}$ satisfies (9).

We now consider $ax\cos\theta + by\cos\phi < 1$

Since $|(\underline{ax} + \underline{by})'|$ is not less than the y coordinate of $\underline{ax} + \underline{by}$, we have

$$|(\underline{ax} + \underline{by})'|^2 \geq (ax\sin\theta - by\sin\phi)^2 \quad \ldots (14)$$

$$= a^2x^2 + b^2y^2 + 2abxy\cos(\theta+\phi) - (ax\cos\theta + by\cos\phi)^2$$

$$a^2x^2 + b^2y^2 + 2abxy\cos(\theta+\phi) - 1$$

and if a or b ≥ 2 we have

$$|(a\underline{x} + b\underline{y})'|^2 \geq 5\,\text{Min}(x^2, y^2) - 1$$
$$\geq \text{Min}(x^2, y^2) + \tfrac{1}{4}$$

and by lemma 4.1, one of the points $\pm\underline{x}$, $\pm\underline{y}$ satisfies (9).

Case (ii) a.b = 0

We assume without loss of generality that b = 0

If $a \leq -2$ then $|(a\underline{x})'| > ax$ ... (15)

since the ξ coordinate of $a\underline{x}$ is positive, hence

$$|(ax)'|^2 \geq a^2x^2 \geq 4x^2 > x^2 + \tfrac{1}{4}$$

since from (4) $x > \frac{\sqrt{3}}{2}$

Thus again lemma 4.1 gives us that one of $\pm\underline{x}$ satisfies (9).

If $a \geq 2$ and $x\cos\theta \geq \frac{1}{2}$ then $ax\cos\theta > 1$ and thus from (11)

$$|(a\underline{x})'|^2 \geq a^2x^2 - 2ax\cos\theta + 1 \qquad \text{... (16)}$$
$$= (ax - \cos\theta)^2 + (1 - \cos^2\theta)$$

Now $x < 1 \Rightarrow \cos\theta > \frac{1}{2}$

$\Rightarrow \theta < \frac{\pi}{3}$

$\Rightarrow x > 1$ a contradiction, thus $x > 1$ and so

$$|(a\underline{x})'|^2 \geq (ax - x\cos\theta)^2$$
$$\geq (a-1)^2x^2$$
$$\geq x^2$$
$$> |x'|^2 \text{ since } x > 1$$

and so $\underline{x}$ satisfies (9).

If $x\cos\theta < \frac{1}{2}$ then $\theta > \frac{\pi}{3}$

$$|(ax)'|^2 \geq a^2x^2\sin^2\theta$$
$$\geq \left(\frac{\sqrt{3}}{2}\right)^2 a^2x^2$$

$$\geq 3x^2 \geq x^2 + \tfrac{1}{4}$$

and hence one of ± x satisfies (9).

Case (iii) a b < 0

We assume without loss of generality that b < 0.

The square of the perpendicular distance of the origin from the line $\underline{L}^{(b)} - t\underline{x} + b\underline{y}$ $(t \in \mathbb{R})$, is greater than $\frac{b^2}{2}$ Min $(y^2, |\underline{x} - \underline{y}|^2)$ This is so, since the triangle formed by the origin, $-\underline{y}$ and $\underline{x} - \underline{y}$ is acute-angled.

Thus $|(a\underline{x} + b\underline{y})'|^2 \geq \frac{b^2}{2}$ Min $(y^2, |\underline{x} - \underline{y}|^2)$ ... (17)

since $(a\underline{x} + b\underline{y})'$ lies on the opposite side of L(b) to the origin.

Hence if b ≤ - 2 then

$$|(a\underline{x} + b\underline{y})'|^2 \geq 2 \text{ Min } (y^2, |\underline{x} - \underline{y}|^2)$$
$$\geq \text{Min } (y^2, |\underline{x} - \underline{y}|^2) + \tfrac{1}{4} \text{ by (3) and (4)}$$

and so by lemma 4.1, one of $\pm\underline{y}$, $\pm(\underline{x} - \underline{y})$ satisfies (9).

Thus b can only be - 1

If a ≥ 3 and t $(a\underline{x} - \underline{y})$ = 1 then

$$|(a\underline{x} - y)'|^2 \geq \left[(a - 1)\underline{x} - 1 \cos\theta\right]^2 + |\underline{x} - \underline{y}|^2 \quad \text{... (18)}$$

This is so, since $(a\underline{x} - \underline{y})'$ is at a distance from the origin greater than the distance of the projection of $(a\underline{x} - \underline{y})$ onto L(-1). Also the angle subtended at $\underline{x} - \underline{y}$ by $a\underline{x} - \underline{y}$ (a ≥ 2) and the origin is obtuse. (see diagram 4.1)

Thus from (18) we see,

$$|(a\underline{x} - \underline{y})'|^2 \geq \left[(a - 2)\,\underline{x} + (x - 1 \cos\theta\,)\right]^2 + |\underline{x} - \underline{y}|^2$$

(6) gives x > cos θ > 1 cos θ and so

$$|(a\underline{x} - \underline{y})'|^2 \geq |(a - 2)\underline{x}|^2 + |\underline{x} - \underline{y}|^2$$
$$\geq x^2 + |\underline{x} - \underline{y}|^2$$

Again lemma 4.1 and (3, (4) give that one of $\pm\underline{x}$, $\pm(\underline{x} - \underline{y})$ satisfies (9).

This leaves us with the point $2\underline{x} - \underline{y}$.

If $(2\underline{x} - \underline{y})_{\xi} = -(2x \cos\theta - y \cos\phi) \geq 0$ then

$$|(2\underline{x} - \underline{y})'|^2 > |2\underline{x} - \underline{y}|^2 > |\underline{x} - \underline{y}|^2 + x^2 \qquad \ldots (19)$$

because the angle subtended at $\underline{x}$ by the origin and $2\underline{x} - \underline{y}$ is obtuse. Thus lemma 4.1 with (3) (4) give that one of $\pm \underline{x}$, $\pm (\underline{x} - \underline{y})$ satisfy (9). So we assume that $2x \cos\theta - y \cos\phi > 0$. Let $l = t(2\underline{x} - \underline{y})$, B is the point $(2\underline{x} - \underline{y})$, E is $(\underline{x} - \underline{y})$, α is acute since it is equal to one of the angles in the fundamental triangle formed by the origin, $\underline{x}$ and $\underline{y}$.

$t = t(\underline{x} - \underline{y})$ hence $1 - t = t(\underline{y} - \underline{x})$.

The projection of the point, a distance of $1 - t$ in the $\xi < 0$ direction from E, onto the line BE, is the point D. The projection of $(2\underline{x} - \underline{y})$ onto BE is the point C.

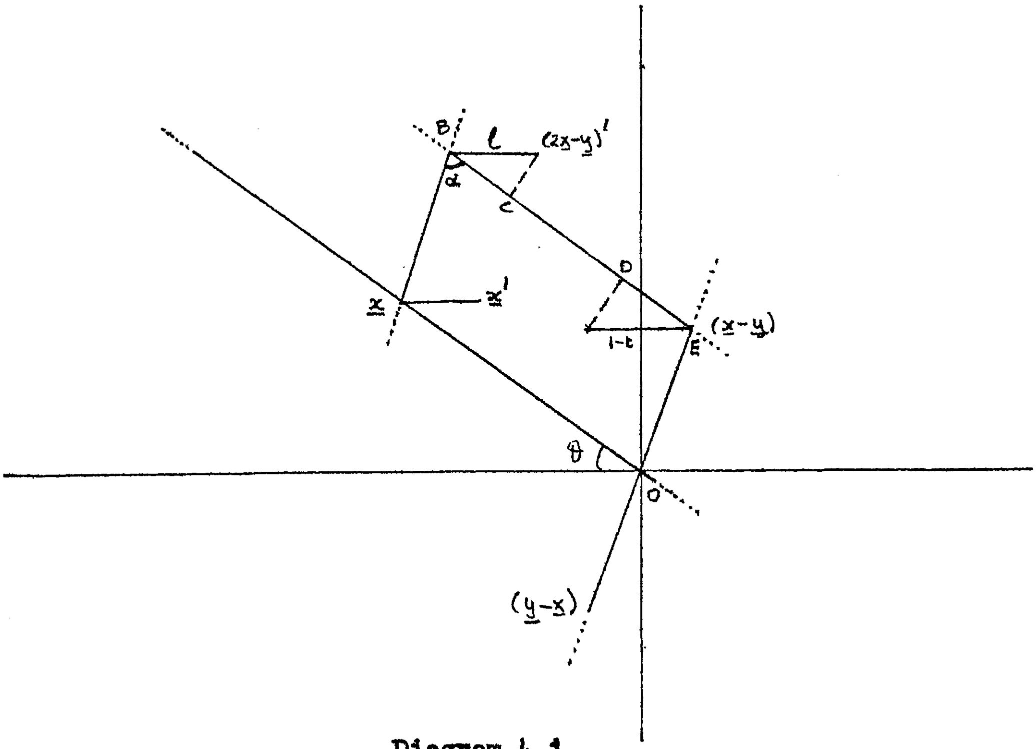


Diagram 4.1

Since OEC = $\pi - \alpha > \frac{\pi}{2}$ we have

$$OC^2 > OE^2 + EC^2 = |\underline{x} - \underline{y}|^2 + (x - l \cos \theta)^2$$

If $(x - l \cos \theta)^2 \geq \frac{1}{4}$ then $OC^2 > |\underline{x} - \underline{y}|^2 + \frac{1}{4}$ ... (20)

and since the angle subtended at C by $(2\underline{x} - \underline{y})'$ and O is obtuse then

$$|(2\underline{x} - \underline{y})'|^2 > |\underline{x} - \underline{y}|^2 + \frac{1}{4}$$

which from lemma 4.1 proves that one of $\pm (\underline{x} - \underline{y})$ satisfies (9).

Thus $(x - l \cos \theta)^2 < \frac{1}{4}$ and by (6) $x > \cos \theta > l \cos \theta$

and so $x < \frac{1}{2} + l \cos \theta$ ... (21)

(7) puts a further restriction that $0 < \theta < \frac{\pi}{3}$ and hence

$1 < x < \frac{1}{2} + l \cos \theta < \frac{3}{2}$ ... (22)

by (21) and (3).

Now $|\underline{x}'_{\xi}| = |x \cos \theta - t(x)|$

$= x \cos \theta - t(x)$ from (8)

$\leq l \cos \theta + \frac{1}{2} - t(x)$ ... (23) from (21)

If $t(x) \geq \frac{1}{2}$ then

$$|\underline{x}'_{\xi}| < l \cos \theta < \cos \theta$$

which would place $\underline{x}'$ inside the unit circle, contradicting the fact that

$\underline{I}$ is a relative minimum.

Thus $t(x) < \frac{1}{2}$

If $l \leq t(x)$ then $l < \frac{1}{2}$ which is impossible since by (32) we must have

$1 < x < \frac{1}{2} + \frac{1}{2} = 1.$

Thus $l > t(x)$ and hence

$t(\underline{x} - \underline{y}) = l - t(x)$

So $t(\underline{y} - \underline{x}) = 1 - l + t(x)$

and ED $= (1 - l + t(x)) \cos \theta$

CB $= l \cos \theta$

CD $=$ EB $-$ ED $-$ CB

$= x - (1 + t\,(x)) \cos\theta$

Hence OC $<$ OD $\Leftrightarrow$ $x > (1 + t\,(x)) \cos\theta$

But $x \cos\theta > \cos\theta + t\,(x)$ by (8),

and thus $x > \cos\theta + t\,(x) \geq (1 + t\,(x)) \cos\theta$

If OC $<$ OD then $|(\underline{y} - \underline{x})'| < |(2\underline{x} - \underline{y})'|$

and so $\underline{y} - \underline{x}$ satisfies the conditions of the lemma.

The proof is similar in the case when $a < o$.

The previous lemma constitutes a proof of Voronoi's Theorem.

We now consider $(\underline{x} + \underline{y})'$ in more detail.

4.3 Let $\rho(z) = \text{Min}\,(|\underline{z}'|, |(-z)'|$ where $\underline{z} \in T$.

Lemma 4.3 If $\rho(\underline{x} - \underline{y}) < \rho(\underline{x})$, then

$$\text{Min}\,(\rho(\underline{y}), \rho(\underline{x} - \underline{y})) < |(\underline{x} + \underline{y})'| = \rho(\underline{x} + \underline{y})$$

Proof $(\underline{x} + \underline{y})_\xi = (\underline{x})_\xi + (\underline{y})_\xi$ and since one of $\theta, \phi < \frac{\pi}{2}$

then $x \cos\theta + y \cos\phi > \frac{\sqrt{3}}{2} \cdot \sqrt{2} > 1$

Hence $|(-\underline{x} - \underline{y})'| > |(-\underline{x} - \underline{y})| = |(\underline{x} + \underline{y})| > |(\underline{x} + \underline{y})'|$

and thus $\rho(\underline{x} + \underline{y}) = |(x + y)'|$

Let $l = t\,(\underline{x})$ and $m = t\,(\underline{x} - \underline{y})$

We first look at the case $\rho(x) = |\underline{x}'|$ and $\rho(\underline{x} - \underline{y}) = |(\underline{x} - \underline{y})'|$

There are three cases to consider

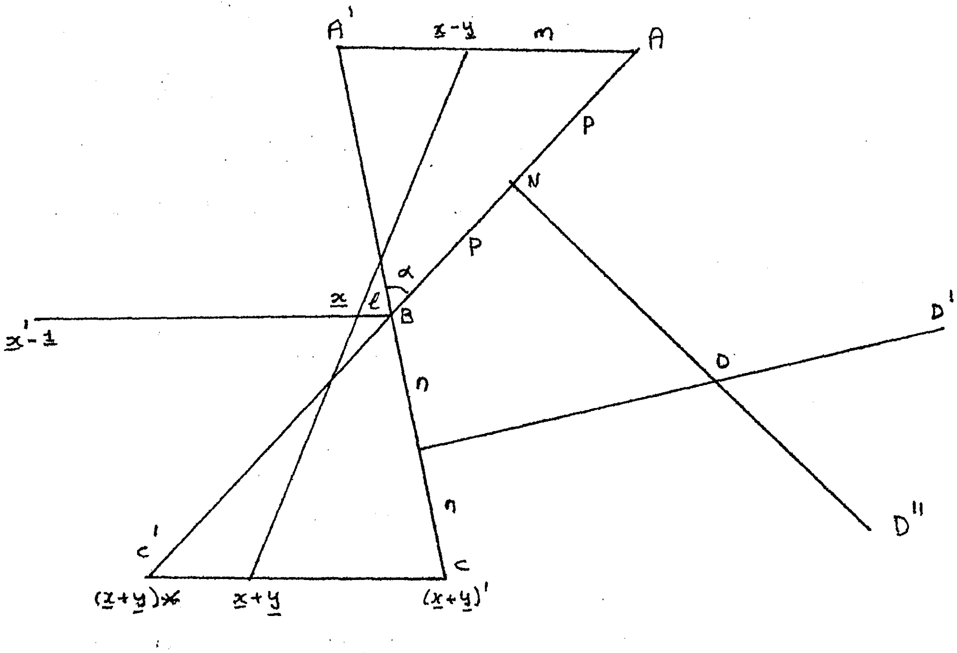
i) $l < \frac{m}{2}$ ii) $\frac{m}{2} \leq l < \frac{1 + m}{2}$ iii) $l \geq \frac{1 + m}{2}$

Since $t\,(\underline{x} + \underline{y}) \equiv 2\,l - m \pmod 1$ we have respectively

$$t\,(\underline{x} + \underline{y}) = 2 + l - m + 1,\ 2\,l - m,\ 2\,l - m - 1$$

In the following section, let $(\underline{x} - \underline{y})'$, $\underline{x}'$ be denoted by A, B respectively. Let $(\underline{x} + \underline{y})^*$ be the point where the line AB cuts the line through $\underline{x} + \underline{y}$ parallel to the ξ - axis. Let $\underline{1}$ represent the projection of OI onto the $\xi - \eta$ plane.

(i) $1 < \frac{m}{2}$. In this case $C = (\underline{x} + \underline{y})' = (x + y) * + \underline{1}$



A'
$\underline{x} - \underline{y}$
m
A
p
N
p
α
$\underline{x}$
ℓ
B
$\underline{x}' - \underline{1}$
D'
D
n
n
C'
C
D''
$(\underline{x}+\underline{y})*$
$\underline{x}+\underline{y}$
$(\underline{x}+\underline{y})'$

Diagram 4.2

In diagram 4.2 $A' = (x - y)' - \underline{1}$, $C' = (x + y) *$, $BC' = AB$ is of length $(- \underline{y})' = 2p$, since $t(- y) = m - 1$ and $A'B = BC$ is of length $\underline{y}' = 2n$ since $t(y) = 1 - m + 1$ N is the mid-point of AB and NDD'' is the perpendicular bisector of AB. DD' is the perpendicular bisector of BC.

α = angle $A'BA < \frac{\pi}{3}$ since $A'A = 1$, $AB > 1$, and $A'B > 1$

Now if $\rho(\underline{x} + \underline{y}) < \rho(\underline{x} - \underline{y})$ the origin must lie in the sector D'DD'' since then we have $\rho(x + y) < \rho(x)$ and $\rho(x - y) < \rho(x)$. The perpendicular distance of C to ND is $p + 2n \cos\alpha \geq p + n$

Hence the distance of C to the origin $\geq$ perpendicular distance of C to ND

$$\geq \text{Min}(2p, 2n)$$
$$= (\underline{y})$$

(ii) $\frac{1 + m}{2} \geq 1 > \frac{m}{2}$. In this situation $(\underline{x} + \underline{y})' = (\underline{x} + \underline{y})*$ and since $\rho(\underline{x}) > \rho(\underline{x} - \underline{y})$ the origin lies on the opposite side from $\underline{x}'$of the perpendicular bisector of AB and hence (x

$$\rho(\underline{x} + \underline{y}) = |(\underline{x} + \underline{y})*| > \rho(\underline{x}) > \rho(\underline{x} - \underline{y})$$

iii) $1 \geq \frac{1 + m}{2}$. Hence $(\underline{x} + \underline{y})' = (\underline{x} + \underline{y})* - \underline{1}$. Let H be the point $\underline{x}' - \frac{1}{2}. \underline{1}$.

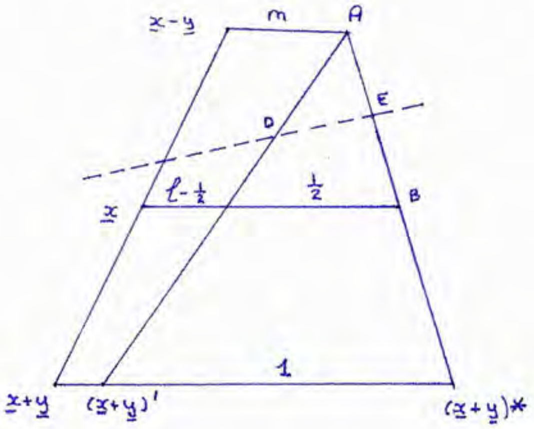


Diagram 4.3

Since $1 > \frac{1}{2}$ and $(\underline{x} + \underline{y})'$ lies on the line joining $(\underline{x} - \underline{y})'$ to $\underline{x} + (1 - \frac{1}{2}).\underline{1}$ i.e. H; and $AB \geq 1$ since $t(y) = 1 - m$ and so $AB = |\underline{y}'| \geq 1$, then the perpendicular bisector DE, of AB cuts the line joining A to H internally at D, since it cannot cut BH internally.

Since $\rho(\underline{x} - \underline{y}) < \rho(\underline{x})$ the origin must lie on the same side of DE as A. Also the ξ -coordinate of H must be negative or otherwise $|\underline{x}'| > |(-\underline{x})'|$ With the origin in this position we must have

$$\rho(\underline{x} - \underline{y}) < \rho(\underline{x} + \underline{y})$$

We now consider the case where $\rho(\underline{x}) = |(-\underline{x})'|$ and $\rho(\underline{x} - \underline{y}) = |(\underline{x} - \underline{y})|$ $(\underline{x} + \underline{y})*$ is $\underline{x} + \underline{y} + (21 + m). \underline{1}$.

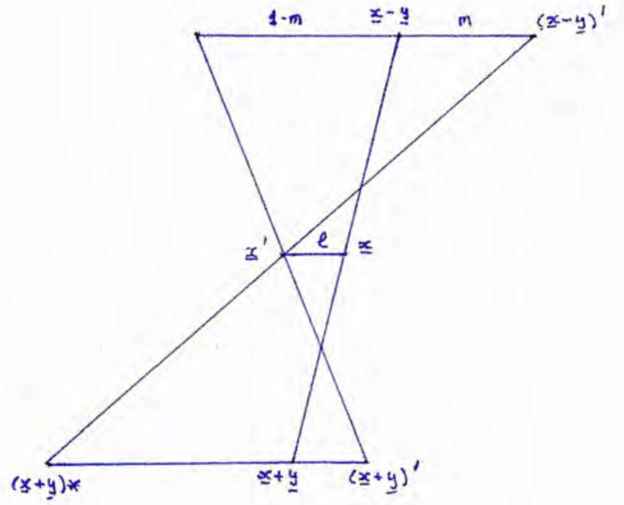
Since $\rho(x) = |(-x)'|$ we have $1 < \frac{1}{2} - x \cos \theta$ and $\theta > \frac{\pi}{3}$

and since $\rho(\underline{x} - \underline{y}) = |(x - y)'|$ we have $m < \frac{1}{2} + x\cos\theta - y\cos\phi$

Hence $21 + m < \frac{3}{2} - \cos\theta . x - y\cos\phi$

Now since $\theta > \frac{\pi}{3}$ then $\phi < \frac{\pi}{6}$ and so $y > 1$ and hence

$21 + m < 1$ which implies $(\underline{x} + \underline{y})' = (x + \underline{y})* + \underline{1}$ and we have a situation analagous to (i) of the previous section.



$1-m$
$\underline{x}-\underline{y}$
m
$(\underline{x}-\underline{y})'$
$\underline{x}'$
ℓ
$\underline{x}$
$(\underline{x}+\underline{y})*$
$\underline{x}+\underline{y}$
$(\underline{x}+\underline{y})'$

Diagram 4.4

Similar configurations occur in the remaining two possibilities

i.e. i) $\rho(\underline{x}) = |\underline{x}'|$ and $\rho(\underline{x} - \underline{y}) = |(\underline{y} - \underline{x})'|$

and ii) $\rho(\underline{x}) = |(-\underline{x})'|$ and $\rho(\underline{x} - \underline{y}) = |(\underline{y} - \underline{x})'|$

and lemma 4.3 is proved.

A similar statement may be proved if $\rho(\underline{y}) > \rho(\underline{x} - \underline{y})$ thus we need only consider $(\underline{x} + \underline{y})'$ if $\rho(\underline{x} - \underline{y})$ is greater than both $\rho(\underline{x})$ and $\rho(y)$.

When $t(\underline{x}) + t(\underline{y}) > 1$ the pinhead of $\underline{x} + \underline{y}$ lies on the parallel through $\underline{x} + \underline{y}$ at a distance $t(\underline{x}) + t(y) - 1$ from that point. Let

A, A', B, B', C, C' denote respectively $\underline{x} + \underline{y}$, $(\underline{x} + \underline{y})'$, $\underline{x}$, $\underline{x}'$, $\underline{y}$, $\underline{y}'$. The angle ABO (ACO) = $\pi - (\theta + \phi) > \frac{\pi}{2}$ and hence the perpendicular from O to AB (AC) cut AB (AC) on the opposite side of OB(OC) from A. Also we have that $t(\underline{x}) + t(\underline{y}) - 1$ is less than both $t(\underline{x})$ and $t(\underline{y})$. Hence the perpendicular from O to A'B' (A'C') cuts the line at E (F) on the opposite side of OB (OC) to A'. Also A'B' > AB = y .

Now B'E (C'E) < perpendicular distance of B' (C') to line OB (OC)

$$= d_B \ (d_C) \text{ say}$$

If we prove that either $d_B < \frac{1}{2}y$ or $d_C < \frac{1}{2}x$ then we will have

$$|(x + y)'| > \text{Min} \ (\rho(\underline{x}), \rho(\underline{y})) \qquad \dots (24)$$

There are three possibilities;

If $\theta > \frac{\pi}{3}$ then $x > \frac{\sqrt{3}}{2 \sin\theta}$ and d_C the distance of BC' from OC is less than $\sin\phi < \sin(\frac{\pi}{2} - \theta) = \cos\theta$.

Now $\frac{x}{2} - d_C \geq \frac{\sqrt{3}}{2 \sin\theta} - \cos\theta$ which has a minimum value zero in the interval $\frac{\pi}{3} \leq \theta \leq \frac{\pi}{2}$ at $\theta = \frac{\pi}{3}$

Hence $\frac{x}{2} > d_C$ and $\rho(\underline{y}) < |(\underline{x} + \underline{y})'|$

If $\theta < \frac{\pi}{6}$ and $\phi \leq \frac{\pi}{3}$. Then $d_B < \frac{1}{2}$ and $y > 1$ and so $\rho(\underline{x}) < |(\underline{x} + \underline{y})'|$

Finally we have the case when θ, ϕ both lie in $[\frac{\pi}{6}, \frac{\pi}{3}]$.

Now $x \cos\theta - t(x) > \cos\theta$ and $y \cos\phi - t(y) > \cos\phi$ by (8)

i.e.

$$x > \frac{t(\underline{x})}{\cos\theta} + 1 , \qquad y > \frac{t(\underline{y})}{\cos\phi} + 1$$

We may assume that $2t(y) \sin\phi > x$, $2\,t(x) \sin\theta > y$, for otherwise (24) would be satisfied.

Hence $2t(y) \cos\theta > \frac{t(\underline{x})}{\cos\theta} + 1$, $2t(x) \cos\phi > \frac{t(\underline{y})}{\cos\phi} + 1$

whence $\sqrt{3}t(y) > \frac{2t(\underline{x})}{\sqrt{3}} + 1$, $\sqrt{3}t(x) > \frac{2t(\underline{y})}{\sqrt{3}} + 1$

adding we get $\left(\sqrt{3} - \frac{2}{\sqrt{3}}\right)(t(x) + t(y)) > 2$.

i.e. $t(\underline{x}) + t(\underline{y}) > 2 . \sqrt{3}$, a contradiction since $t(\underline{x}) + t(\underline{y}) < 2$.

Hence we only consider the case when $t(x) + t(y) < 1$.

If $a = (\bar{\phi})_{\xi}$ and $c = (\bar{\psi})_{\xi}$ then $(\underline{x} + \underline{y})$ is the projection $\bar{\phi} + \bar{\psi}$ onto the $\xi - \eta$ plane and thus $(\bar{\phi} + \bar{\psi})_{\xi} = a + c$.

If $a + c > \frac{1}{2}$ then the projection of $\underline{1} - (\bar{\phi} + \bar{\psi})$ onto the $\xi - \eta$ plane is closer to the origin than is the projection of $(\bar{\phi} + \bar{\psi})$.

Hence $|(\underline{x} + \underline{y})'| > |(-\underline{x} - \underline{y})'|$, which was rejected by lemma 4.2.

We have thus proved

Lemma 4.4 Unless the conditions

i) $\rho(\underline{x}) < \rho(\underline{x} - \underline{y})$ ii) $\rho(\underline{y}) < \rho(\underline{x} - \underline{y})$

iii) $t(\underline{x}) + t(\underline{y}) < 1$ iii) $(\bar{\phi})_{\xi} + (\bar{\psi})_{\xi} < \frac{1}{2}$

all hold, then there is a point $\underline{z}$, $\underline{z} \in \{\pm\underline{x}, \pm\underline{y}, \pm(\underline{x} - \underline{y})\}$ such that $|(\underline{x} + \underline{y})'| > |\underline{z}'|$

4.4 We now suppose that the cubic field $K(\theta)$ is generated by one of the zeros $\alpha, \beta \pm i\gamma$ of the polynomial $p(x) = x^3 - qx - n$. Starting with the lattice $S = [1, \phi, \psi] = \left[1, \frac{m+m'\theta+m''\theta^2}{\sigma}, \frac{n+n'\theta+n''\theta^2}{\sigma}\right]$ the lattice T will have basis elements

$$\underline{x} = \left(\frac{m'(\beta-\alpha) + m''(\beta^2-\gamma^2-\alpha^2)}{\sigma}, \frac{\gamma(m'-m''\alpha)}{\sigma}\right) = (\xi_1, \eta_1)$$

$$\underline{y} = \left(\frac{n'(\beta-\alpha) + n''(\beta^2-\gamma^2-\alpha^2)}{\sigma}, \frac{\gamma(n'-n''\alpha)}{\sigma}\right) = (\xi_2, \eta_2)$$

We see that
$$\xi_1\eta_2 - \xi_2\eta_1 = (m'n''-m''n')\left(\frac{\gamma((\alpha-\beta)^2+\gamma^2)}{\sigma}\right)$$
$$= (m'n''-m''n').\,Z \quad \text{say}$$

Thus $\frac{\eta_1}{\xi_1} < \frac{\eta_2}{\xi_2}$ if and only if $m'n''-m''n' > 0$

If $m'n'' - m''n'$ is initially positive, then after every transformation performed on the basis, with positive discriminant, the new value of $m'n'' - m''n'$ will still be positive. In the case when $m'n'' - m''n' < 0$ we alter the basis to $[1, \psi, \phi]$ which satisfies the condition.

To use Voronoi's algorithm we have to find a basic vector pair for the lattice T which produces an acute triangle with the origin covering the negative ξ axis. First we have to produce a basis which gives an acute triangle with the origin, the second condition is then satisfied by using a suitable transformation.

T has a basis $\underline{x}, \underline{y}$, the necessary and sufficient conditions that the triangle is acute are

i) $\underline{x} . \underline{y} > 0$

ii) $\underline{x} . (\underline{x} - \underline{y}) > 0$

iii) $\underline{y} . (\underline{y} - \underline{x}) > 0$

i.e. all three angles of the triangle have positive cosines.

Now $\underline{x} . \underline{x} = \gamma\left((\alpha-\beta)^2+\gamma^2\right)\left(m'^2 + m'm''\alpha + m''^2(\alpha^2-q)\right)$

$= Z . A$ say

$\underline{x} . \underline{y} = \gamma\left((\alpha-\beta)^2+\gamma^2\right)\left(m'n' + (m'n''+m''n')\frac{\alpha}{2} + m''n''(\alpha^2-q)\right)$

$= Z . B$ say

and $\underline{y} . \underline{y} = Z . \left(n'^2 + n'n''\alpha + n''^2(\alpha^2-q)\right)$

$= Z . C$ say

Without loss of generality, these conditions may be restated as

i) $B > 0$ ii) $A > B$ iii) $C > B$

because of the fact that $Z > 0$

If $B < 0$, by post-multiplying the basis by the matrix

$$H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & 0 \end{bmatrix}$$

the basis is changed to $[1, -\psi, \phi]$ which gives us $B > 0$ and det $H = +1$

If $A < B$ by setting $d = \left[\frac{B}{A}\right]$ and past-multiplying by a matrix

$$J = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -d \\ 0 & 0 & 1 \end{bmatrix}$$

we have $A > B$, and det $J = +1$. Similarly if $C < B$.

By repeated multiplication of the basis by matrices such as H and J, we eventually arrive at a basis which satisfies conditions i), ii), iii). This is so, because on each multiplication B is decreased by a value greater than the minimum length of a vector in the lattice, and is positive. (this is the method of reduction of a quadratic form)

By multiplying the newly found basis by matrices Ii, $(i = 1, .. , 6)$, the six triangles formed by the respective basis elements form the first reduced Hexagon of Zelling.

Here the matrices are defined by

$$I_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad I_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & 0 \end{bmatrix} \qquad I_4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & -1 \\ 0 & 1 & 0 \end{bmatrix}$$

$$I_5 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 1 \end{bmatrix} \qquad I_6 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{bmatrix}$$

Two of the six triangles formed by the six basis and the origin, cover the ξ - axis, one the positive ξ - axis, the other the negative. However we know for these that

$$\frac{\eta_1}{\xi_1} < \frac{\eta_2}{\xi_2}$$

and so if the triangles cross the negative ξ - axis then

$$\frac{\eta_1}{\xi_1} < 0 \qquad \frac{\eta_2}{\xi_2} > 0 \qquad \xi_1 , \xi_2 < 0$$

thus $\quad \eta_1 > 0 \qquad \eta_2 < 0$

Thus the required vector pair is that one whose first element has positive η coordinate and whose second element has negative η - coordinate.

If $\quad b = \eta$ coordinate of $\phi \quad : \phi(\eta)$

$\quad\quad d = \eta$ coordinate of $\psi \quad : \psi(\eta)$

Then the required basis is that one obtained from post-multiplication by I_i, where i is such that $b_i > 0 \quad d_i < 0$ and

$$(b_i, d_i, i) = ((b, d, 1), (-b, -d, 2), (b-d, b, 3), (-b + d, -b, 4), (d, -b + d, 5), (-d, b-d, 6))$$

Now suppose at this stage we have a basis $[1, \phi_1, \psi_1]$ we require the pinheads corresponding to points ϕ_1 , ψ_1

To do this we find integer l, m so that

$$0 < \phi_1(\xi) + l < 1$$
$$0 < \psi_1(\xi) + m < 1$$

and by setting the new basis as $[1, \phi_1 + l, \psi_1 + m] = [1, \bar{\phi}, \bar{\psi}]$

Now we use Voronoi's theorem which states that the first relative minimum of S is that one of the seven given below, which is the minimum distance from the ζ - axis

$$\bar{\phi} \quad \text{or} \quad 1 - \bar{\phi} \qquad \text{denoted by } \theta_0$$

$$\bar{\psi} \quad \text{or} \quad 1 - \bar{\psi} \qquad \text{denoted by } \theta_1$$

$(-1)^t (\bar{\phi} - \bar{\psi})$ or $(1 - (-1)^t (\bar{\phi}-\bar{\psi})$denoted by θ_2

where $t = 0$ if $\quad \bar{\phi} (\zeta) \quad > \quad \bar{\psi} (\zeta)$

$\qquad = 1$ otherwise

and $\bar{\phi} + \bar{\psi}$ denoted by θ_3, which need only be considered if

$$\rho (\theta_2) > \rho(\theta_0) \quad ; \quad \rho(\theta_1) > \rho(\theta_0)$$

and

$$\bar{\phi} (\zeta) + \bar{\psi} (\zeta) < 1$$

$$\bar{\phi} (\xi) + \bar{\psi} (\xi) < \tfrac{1}{2}$$

For θ_0 all we need check is if $a = \bar{\phi} (\xi) < \frac{1}{2}$ or not

since $(1 + \bar{\phi})(\xi) = 1 - a$

Thus $\quad \theta_0 = \bar{\phi} \quad$ if $\quad a < \frac{1}{2}$

$\qquad\qquad = 1 - \bar{\phi}$ if otherwise

similarly $\theta_1 = \bar{\psi} \quad$ if $c = \bar{\psi} (\xi) < \frac{1}{2}$

$\qquad\qquad = 1 - \bar{\psi}$ otherwise

$\qquad \theta_2 = (\bar{\phi} - \bar{\psi})(-1)^t \quad$ if $(a - c)(-1)^t < \frac{1}{2}$

$\qquad\qquad = 1 - (\bar{\phi} - \bar{\psi})(-1)^t$ otherwise

$\qquad \theta_3 = \bar{\phi} + \bar{\psi}$

Then we find i, j, k, l from 0, 1, 2, 3 such that

$$\rho (\theta_i) < \rho (\theta_j) < \rho (\theta_k) < \rho (\theta_\ell)$$

and then set $[1, \theta_i , \theta_\ell]$ as the reduced basis of S, and where is the first relative minimum of S.

By dividing the lattice by θ_i and considering the lattice $\left[1, \frac{\theta_j}{\theta_i} , \frac{1}{\theta_i}\right]$ we may repeat the process and in this way produce a sequence of lattices S_t with first relative minimum $\theta^{(t)}_{i_t}$ which will furnish us with the relative minima of S. i.e. $\vartheta_{i_1}^{(1)}, \vartheta_{i_1}^{(1)}\, \vartheta_{i_2}^{(2)}, \dots$

4.5 We now show how Voronoi's algorithm is actually used in the computation of the class number of a given field.

We first find all ideals with norms less than the Minkowski-Davenport Bound (Davenport (9)) B.

i) Now suppose the field has basis $[1, \vartheta, \lambda]$ where $\lambda = \frac{\vartheta^2 + j\vartheta + k}{\text{index}}$ for some integral j , k, and where 'index' is the index of the defining polynomial of the field K(ϑ). Then any ideal of norm n can be represented in the form $\mathfrak{a} = [a, b\vartheta + c, d\lambda + e\vartheta + f]$ where a, b, c, d, e, f are rational positive integers and a x b x d = n. From the additivity property of ideals and since $a\vartheta$, $a\lambda$ belong to the ideal we may redefine the above representation so that $0 \leq b \leq a$ $0 \leq d \leq a$ and also $0 \leq e \leq b$ and $0 \leq c, f \leq e$.

We also have that $a \geq \sqrt[3]{n}$. Now $\mathfrak{a}$ is the highest common factor of three numbers a, $b\vartheta + c$, $d\lambda + e\vartheta + f$ and hence

$$n \mid a^3,\ n \mid \text{Norm}(b\vartheta + c) \text{ and } n \mid \text{Norm}(d\lambda + e\vartheta + f)$$

ii) We now vary n between the bound $2 \leq n \leq B$ and for each n produce a set of values for a, b, c, d, e, f - we still do not know if the form $\mathfrak{a} = [a, b\vartheta + c, d\lambda + e\vartheta + f]$ is in fact an ideal - we have implicitly the additive rule - we must now check if the totality of linear combinations $\mathfrak{a}$ when multiplied by any integer of the field give a subset of $\mathfrak{a}$.

This is simply done by checking if $a\lambda$, $a\vartheta$, $b\vartheta^2 + c\vartheta$, $b\lambda\vartheta + c\lambda$, $d\lambda\vartheta + e\vartheta^2 + f\vartheta$, $d\lambda^2 + e\lambda\vartheta + f\lambda$ all belong to $\mathfrak{a}$.

When all these conditions have been satisfied, then the ideal is added to the list of ideals to be considered by Voronoi's algorithm.

Once we have an ideal $\left[a, b\theta + c, d\lambda + e\theta + f\right]$ we have to divide the three basis elements by a to put it in the form which is used in the calculation i.e. a fractional ideal containing 1 as its minimal positive rational member. So we consider

$$\left[1 , \frac{b\theta + c}{a} , \frac{d\lambda + e\theta + f}{a}\right]$$

Once we have all ideals with norm less than B in the form, we find the number of different lattice loops evolved in the process of the algorithm and this furnishes us with the class number of the field.

4.6 We now produce a check on the unit produced by Voronoi's algorithm.

Consider the field generated by a zero of the polynomial $P(x) = x^3 - ax^2 + bx - 1$ with negative discriminant and the roots of $P(x) = 0$ are $\alpha, \beta \pm i\gamma$ Let the unit ε represent this triad.

Since $\alpha(\beta^2+\gamma^2) = 1$ we can assume $\alpha > 1$ for we can choose between ε, and ε^{-1} (ε^{-1} represents the triad $\alpha^{-1}, \alpha\beta \pm i\alpha\gamma$)

$$\begin{aligned} \text{Define } S(\varepsilon) &= (\alpha-\beta)^2 + \gamma^2 \\ &= \alpha^2 - 2\alpha\beta + \alpha^{-1} \end{aligned}$$

Thus $S(\varepsilon^{-1}) = \alpha^{-2} - 2\beta + \alpha$ and hence

$$\begin{aligned} S(\varepsilon) - S(\varepsilon^{-1}) &= \alpha^2 - 2\alpha\beta + \alpha^{-1} - \alpha^{-2} + 2\beta - \alpha \\ &= (\alpha-1)\,\alpha^{-2}\,(\alpha^3 - 2\beta\alpha^2 + 1) \end{aligned}$$

We have that $\alpha(\beta^2+\gamma^2) = 1$ hence $\beta < \alpha^{-\frac{1}{2}}$ and so

$$\begin{aligned} S(\varepsilon) - S(\varepsilon^{-1}) &> (\alpha-1)\,\alpha^{-2}\,(\alpha^{\frac{3}{2}} - 1)^2 \\ &> 0 \end{aligned}$$

So $S(\varepsilon) > S(\varepsilon^{-1})$ and $S(\varepsilon^{n}) > S(\varepsilon^{-n})$, where n is a rational integer greater than 1.

We consider $S(\varepsilon^{-n})$ in more detail. Suppose ε^{-n} represents the triad of algebraic numbers α^{-n} , $\omega + i\eta$ where

$\alpha^{-n}(\omega^2 + \eta^2) = 1$ $\qquad$ $\omega \pm i\eta = (\beta \pm i\gamma)^{-n}$

Thus $\omega^2 + \eta^2 = \alpha^n$ and so $\omega < \alpha^{\frac{n}{2}}$

$$\begin{aligned} S(\varepsilon^{-n}) - S(\varepsilon^{-1}) &= (\alpha^{-n} - \omega)^2 + \eta^2 - \alpha^{-2} + 2\beta - \alpha \\ &= \alpha^{-2n} - 2\alpha^{-n}\omega + \alpha^{n} - \alpha^{-2} + 2\beta - \alpha \\ &> \alpha^{n} - \alpha - 2\alpha^{-\frac{n}{2}} - \alpha^{-2} \end{aligned}$$

If $\alpha > 1$ then

$$\begin{aligned} S(\varepsilon^{-n}) - S(\varepsilon^{-1}) &> \alpha^{2} - \alpha - 2\alpha^{-1} - \alpha^{-2} \\ &= \alpha^{-2}(\alpha^4 - \alpha^3 - 2\alpha - 1) \end{aligned}$$

Now if $\alpha > 1{\cdot}795$

$$S(\varepsilon^{-n}) > S(\varepsilon^{-1})$$

Artin (1) gives us the lemma

$|\alpha^3| > \frac{D}{4} - 6$ $\qquad$ where D is the discriminant of the polynomial P, and thus is not greater than Δ the discriminant of the field generated by P.

Hence if $|D| > 47$ then $\alpha > 1.795$, and thus in every cubic field with discriminant less than -47 (so that in fact $\Delta \leq -59$), $S(\varepsilon)$ where ε represents a unit of the field, takes a minimum value at the fundamental unit of the field, with real part in the interval $0 < \alpha < 1$.

Now given an algebraic integer $p\theta^2 + q\theta + r$ of $K(\theta)$ we have $S(p\theta^2 + q\theta + r) = S(\theta)\{(p(\alpha+\beta)+q)^2 + p^2\gamma^2\}$ where now $\alpha, \beta \pm i\gamma$ are the zeros of the polynomial satisfied by θ

Hence if we find a unit ε (as was done using Voronoi's algorithm), we can produce all p, q which satisfy

$$(p(\alpha+\beta)+q)^2 + p^2\gamma^2 < \frac{S(\varepsilon)}{S(\theta)}$$

and then exhaust all the possible units $p\theta^2 + q\theta + r$ eventually giving us the fundamental unit of the field.

Using this technique, the fundamental units obtained by Voronoi's algorithm for the first hundred complex cubic fields, were checked, and found to be correct.

4.7 Only seven of the fields considered had a non-cyclic group of ideals. These are the following fields, identified by their discriminant and generating polynomial equation.

i) -6571 generated by $\theta^3 - 14\theta^2 + 56\theta - 39 = 0$

The class number of this field is 4, and the group of ideals is the product of two cyclic groups of order 2, which are generated by ideals $[2, \theta + 1, \theta^2 + 1]$ and $[3, \theta, \theta^2]$

ii) -6883 generated by $\theta^3 - 17\theta^2 + 77\theta - 36 = 0$

The field has class number 4, and the group of ideals is the product of two cyclic groups of order 2 generated by ideals $[2, \theta, \theta^2]$ and $[3, \theta, \theta^2]$

iii) -11003 generated by $\theta^3 - 3\theta^2 + 17\theta - 14 = 0$

The field has class number 8, and the group of ideals is the product of a cyclic group of order 4 and a cyclic group of order 2.

The group of order 4 is generated by ideal $[2, \theta, \theta^2]$ and the group of order 2 is generated by ideal $[7, \theta + 3, \theta^2 + 5]$

iv) -12763 generated by $\theta^3 - 11\theta^2 + 41\theta - 30 = 0$

The group of ideals is the product of a cyclic group of order 4 and a cyclic group of order 2.

The group of order 4 is generated by ideal $[2, \theta, \theta^2]$ and the group of order 2 is generated by ideal $[3, \theta, \theta^2]$

v) -16871 generated by $\theta^3 - 12\theta^2 + 47\theta - 35 = 0$

The group of ideals is the product of two cyclic groups of order 2 generated by ideals $[5, \theta, \theta^2]$ and $[5, \theta + 1, \theta^2 + 4]$

vi) -17231 generated by $\theta^3 - 6\theta^2 + 23\theta - 9 = 0$

The group of ideals is the product of two cyclic groups of order 2, generated by $[3, \theta, \theta^2]$ and $[3, \theta + 1, \theta^2 + 2]$

vii) -18923 generated by $\theta^3 - 9\theta^2 + 35\theta - 26 = 0$

The group of ideals is the product of a cyclic group of order 4 and a cyclic group of order 2.

The cyclic group of order 4 is generated by $[2, \theta, \theta^2]$ and the cyclic group of order 2 is generated by $[5, \theta + 2, \theta^2 + 1]$

PART II

A description of the programs used in the calculation of the complex cubic number fields, their fundamental units and class numbers

CHAPTER 5

The field calculation - TABLE

First the subroutines are described, and then finally the main routine.

BASIS (I2, KT, KS)

$P(x) = x^3 - I3x^2 + I4x - I5$ has zeros θ, ϕ, ψ and we are concerned with the field $K(\theta)$. This routine has a dual purpose, i) given the index of the polynomial I2, to find an integral basis of the field $\left[1, \theta, \frac{\theta^2+KT\theta+KS}{I2}\right]$ or ii) to check if I2 divides the index of P by checking there exists the module $\left[1, \theta, \frac{\theta^2+KT\theta+KS}{I2}\right]$ contained in the ring of integers. This is done by considering the coefficients IA, IB, IC of the monic polynomial satisfied by $\xi = \frac{\theta^2+KT\theta+KS}{I2}$ $\quad 0 \leq KT, KS \leq I2 - 1$ as described in 1 § 5 (ii), checking if any such ξ is an algebraic integer. If no such integer exists, i.e. I2 does not divide the index of P, we transfer this fact to the main program by returning KT as - 1. The routine also returns $IH = \Sigma\theta^2$, $IJ = \Sigma\theta^2\phi^2$ and $IK = \Sigma\theta^2\phi$ which are used in two of the following subroutines INDEX 2 and CHECK.

INDEX 1 (M)

$P(x) = x^3 - IAx^2 + IBx - IC$, and IN divides the index of P. All these variables are obtained via common store. Using the theory described in 1 § 5 (i) the routine finds whether the prime number M divides the index of P or not. We know $M \not| IN$; by varying JT between 0 and M-1 and by setting I = P'(JT) and K = P(JT) (P'(x) the derivative of P(x)), we see that M divides the index if $M \mid I$ and $M^2 \mid K$ and if this is so we replace IN by IN x M, making IN one step closer to the actual value of the index of P.

INDEX 2 (JM, M)

Again $P(x) = x^3 - IAx^2 + IBx - IC$ and IN divides the index of P. $JM = M^q$ for some rational integral q and $JM \mid IN \times M$ but $JM \nmid IN$. By calling BASIS JM, KT, KS we know that JM divides the index of P if and only if $KT \neq -1$ and in this case we replace IN by IN x M. This routine is used mostly in finding if the index of P contains a squared factor.

INDEX 3 (M)

θ, P and M are the same as in previous subroutines. This routine using the theory of 1 § 5 (iii), checks if any of the M numbers $\xi = \frac{\theta + I}{M}$ $1 \leq I \leq M$ are algebraic integers by considering the equation $x^3 - LAx^2 + LBx - LC = 0$ satisfied by ξ. IN is the same as in the previous subroutines. If one such integer does exist, then we know that M^3 divides the index of P and in this case we return IN as zero. We need not return the basis of the integral ring of the field, since if M^3 does divide the index of the polynomial, then the index is greater than 6, and the polynomial may be discarded.

CHECK (I1, I2, I3, I4, I5, R1, R2, R3, KT, KS, J3, J4, J5, Y1, Y2, Y3, MQ)

We are given a polynomial $P(x) = x^3 - I3x^2 + I4x - I5$ with zeros R1, $R2 \pm iR3$, one of which generates the field $K(\theta)$ with discriminant $-$ I1 and integral basis $\left[1, \theta, \lambda = \frac{\theta^2 + KT\theta + KS}{I2}\right]$. Q(x) is another polynomial $x^3 - J3x^2 + J4x - J5$ with roots Y1, $Y2 \pm iY3$ and both polynomial P and Q generate fields with the same discriminant. This routine using the theory of 1 § 6 searches for a Tschirnhausen transformation between polynomials P and Q by finding approximate values RL, RM, RN so that:-

$$\phi = RL\,\lambda + RM\,\theta + RN$$

satisfies the equation $Q (\phi) = 0 \pm 0.001$. IL, IM, IN are the nearest integers to RL, RM, RN respectively. We check if $\eta = \text{IL}\,\lambda + \text{IM}\,\theta + \text{IN}$ satisfies $Q (\eta) = 0$ and if so then the two polynomials give rise to the same fields, and in this case MQ, which answers the question of whether P and Q are related thus, is returned as . TRUE ., if not then . FALSE .

The Main Program

TABLE

Initially the inter-related bounds are found for IA, IB and IC, which are such that the totality of polynomials $P(x) = x^3 - \text{IA}x^2 + \text{IB}x - \text{IC}$ give rise to all fields with negative discriminant greater than - 20,000.
In the three loops IA, IB, IC vary thus IA MIN ≤ IA ≤ IA MAX, IB MIN ≤ IB ≤ IB MAX, IC MIN ≤ IC ≤ IC MAX; and we consider each polynomial in turn. In section 2 we have fixed IA, IB, IC and we find the discriminant IDEM of P(x) and set IDET = - IDEM. We ensure that IDEM is negative so that P(x) has two complex roots, the roots being ALPHA, BETA ± i GAMMA (we shall refer to them as $\alpha, \beta \pm i\gamma$). These are calculated by the Newton Raphson method, and are used to find RIS = $S (\alpha, \beta, \gamma)$ and here, as throughout the program when we successively reduce IDET by dividing it by squares of factors of the index of P, we check that IDET < IS = RIS^2.
Section 3 contains the method by which the index of the polynomial is found. Subroutines INDEX 1, INDEX 2 and INDEX 3 are used after first finding the squared divisors of IDET, to calculate each factor of the index of P and then we divide IDET by the square of this factor. After the final value of the index has been found (INDEX) we check both that the index is less than 6 and that IDET ≤ 20,000.
Since the largest complex cubic discriminant is - 23, and since

$31^2 \times 23 = 22103$ the only index factors we need consider are the rational primes ≤ 29 and also 4, 8, 9, 25 as we may discard any polynomial with index greater than 6.

In Section 4, starting at K = 1, for each field produced, we set IDET in IDIS (K), INDEX, IA, IB, IC in IZ (1-4, K) and α, β, γ in ZZ (1 - 3, K) and then increment K by 1, and then manipulate the arrays so that the IDIS values are in increasing order.

In the last section, 5, we take all fields with the same discriminant, by considering the IDIS array, and using the subroutine CHECK find the actual number of different non-conjugate fields with that discriminant. Finally the program prints out one representative polynomial with its discriminant, index and roots for each non-conjugate field with discriminant less than - 20,000.

CHAPTER 6

The calculation of the fundamental unit and class number of a given field using program VORONOI.

First is given a description of the subroutines used in the above program except the major subroutine UNIT which comes at the end.

ICF (IJ, IK, IL, IH)

This routine calculates IH the h.c.f. of the absolute value of integers IJ, IK and IL by calculating

$$\text{h.c.f.}\ (\text{h.c.f.}\ (\,|IJ|\,,\ |IK|\,),|IL|)$$

ICF 2 does the same calculation but for double precision values.

BASIS is essentially the same routine found in Chapter 5.

SUB (I, J, K, L)

$\left[1,\ \phi = \dfrac{M1 + M2\theta + M3\theta^2}{IG},\ \psi = \dfrac{M1 + N2\theta + N3\theta^2}{IG}\right]$ form a basis of a given lattice, and $\Phi = Ax^2 + 2Bxy + Cy^2$ is the quadratic form which represents the vector pair defining the two dimensional lattice corresponding to the given basis. Chapter 4.

This routine produces a new basis for the lattice by pre-multiplying the vector $\begin{bmatrix}1\\ \phi\\ \psi\end{bmatrix}$ by the matrix $\begin{bmatrix}1 & 0 & 0\\ 0 & I & J\\ 0 & K & L\end{bmatrix}$

now $$\begin{bmatrix}1\\ \phi\\ \psi\end{bmatrix} = \frac{1}{IG}\begin{bmatrix}IG & 0 & 0\\ M1 & M2 & M3\\ N1 & N2 & N3\end{bmatrix} \times \begin{bmatrix}1\\ \theta\\ \theta^2\end{bmatrix}$$

Thus the new basis is of the form

$$\frac{1}{IG}\begin{bmatrix}1 & 0 & 0\\ 0 & I & J\\ 0 & K & L\end{bmatrix}\times\begin{bmatrix}IG & 0 & 0\\ M1 & M2 & M3\\ N1 & N2 & N3\end{bmatrix}\times\begin{bmatrix}1\\ \theta\\ \theta^2\end{bmatrix}$$

We redefine M1, M2, M3, N1, N2, N3 so that we have the new basis in the same form i.e. $\left[1, \frac{M1 + M2\theta + M3\theta^2}{IG}, \frac{N1 + N2\theta + N3\theta^2}{IG}\right]$

The associated binary quadratic form has also changed and the new values of A, B and C are

$$A \times I^2 + 2 \times B \times I \times K + C \times K^2$$

$$A \times I \times J + B \times (I \times L + J \times K) + C \times K \times L$$

$$A \times J^2 + 2 \times B \times L \times J + C \times L^2$$

respectively.

<u>MULT (J1, J2, J3, K1, K2, K3, L1, L2, L3)</u>

I1, I2 are obtained via common store; we have a field K(θ) generated by a zero of the polynomial $P(x) = x^3 - I1x - I2$. The routine multiplies the number $J1 + J2\theta + J3\theta^2$ by $K1 + K2\theta + K3\theta^2$ to give as the product the algebraic number $L1 + L2\theta + L3\theta^2$. <u>MULT 2</u> is a similar routine, but it uses double precision values.

<u>INVER (I, J, K, KDET)</u>

IQ, IN, N(3.3) in common store. This routine finds the inverse of the matrix $A = \begin{bmatrix} I & J & K\\ IN\cdot K & I+IQ\cdot K & J\\ IN\cdot J & IQ\cdot J+IN\cdot K & I+IQ\cdot K\end{bmatrix}$ and sets

$\frac{N}{KDET} = A^{-1}$ where N (1,J) J = 1,3 and KDET have no common factors.

Now if $\phi = I + J\theta + K\theta^2$ is an integer of K(θ), where $\theta^3 = IQ\,\theta + IN$

then $\frac{N(1,1) + N(1,2)\theta + N(1,3)\theta^2}{KDET}$ is the inverse ϕ^{-1} of ϕ in K (θ).

FACTOR

$P(x) = x^3 - IAx^2 + IBx - IC$, whose zeros AL, BE ± iGA generate the algebraic number field $K(\theta)$. The field has integral basis $[1, \theta, \lambda]$ where $\lambda = \frac{\theta^2 + KT\theta + KS}{INDEX}$, and has discriminant - IDET with Minkowski-Davenport bound MZ.

NORN (J) finds the norm of $s\theta + J$ where s is defined just before the call of this function. NORM (I, J, K) finds the norm of $\frac{I\theta^2 + J\theta + K}{INDEX}$.

The representations of θ^2, $\lambda\theta$, λ^2 in terms of λ and θ are know found

$$\theta^2 = IX\lambda + IY\theta + IZ$$
$$\lambda\theta = JX\lambda + JY\theta + JZ$$
$$\lambda^2 = KX\lambda + KY\theta + KZ$$

Ideals $\mathfrak{a}_i = [F, S\theta + J, T\lambda + U\theta + K]$ are stored in the array LIST. LIST (i, 1) = F, LIST (i, 2) = J, LIST (i, 3) = S, LIST (i, 4) = 0, LIST (i, 5) = K, LIST (i, 6) = U, LIST (i, 7) = T and LIST (i, 8) is the norm of the ideal.

For i = 1 we consider the integral ideal $[1, \theta, \lambda]$

Section 1 of the routine is a section of loops which generate all the possible values for F, S, J, T, U, K using the bounds and conditions discussed in 4 § (1), for all ideals with norm N less than or equal to the Minkowski bound MZ.

In Section 2 we see if the module $[F, S\theta + J, T\lambda + U\theta + K]$ (for convenience we will call it $[\delta_1, \delta_2, \delta_3]$) satisfies the multiplicity condition of ideals. i.e. let

$$\delta_i.\theta = MY(i, 1)\lambda + MY(i, 2)\theta + MY(i, 3)$$
$$\delta_i.\lambda = MY(i + 3, 1)\lambda + MY(i + 3, 2)\theta + MY(i + 3, 3)$$
$$i = 1, 2, 3$$

when we check if $MY(j, 1)\lambda + MY(j, 2)\theta + MY(j, 3)$ for j = 1, ..., 6 belongs to the module.

If this is so then we have in fact produced an ideal. We initially set ICO to 1 and in section 3 we increment ICO and fill the array LIST as described previously.

In this way we produce ICO different ideals with norm $\leq$ MZ which are now returned to the main program via common store, to be processed by subroutine UNIT to calculate both the fundamental unit of the field, and the number of non-equivalent classes.

MAIN PROGRAM

VORONOI

For each field K(θ), where $\theta^3 - \text{IA}\,\theta^2 + \text{IB}\,\theta - \text{IC} = 0$, IA, IB, IC are given together with the discriminant - IDET and INDEX, the index of the polynomial. Initially we set MARK to 1 and CLAS to zero. MARK will eventually give

$$\max_{\text{all ideal classes } \mathcal{C}_i} \left(\min_{\mathfrak{a}_j \in \mathcal{C}_i} (\text{Norm } \mathfrak{a}_j) \right)$$

and CLAS will be the class number of the field.

As an example of the use of this program, we will illustrate its operations by considering a specific field, the one generated by a zero of the polynomial $P(x) = x^3 - 2x^2 + 6x - 1$. IDET = 563 and INDEX = 1.

First, in Section 1, we calculate the roots AL, BE $\pm$ iGA of $P(x) = 0$ by the Newton Raphson Method.

In what follows references to the particular example will occur in braces $\{\ \}$ thus:-

$\{$AL = 0.17609 ... ; BE = 0.91195 ... ; GA = 2.20163 ... $\}$

In Section 2 the integral basis of the field is calculated by calling the subroutine BASIS

$\{$ in K(θ) basis is $[1, \theta, \theta^2]$ since INDEX = 1 $\}$

Then MZ the Minkowski Bound is obtained $\{$ MZ = 4 $\}$

For ease of calculation, we change the defining polynomial by the transformation $\phi = 3\theta$ - IA to form a new polynomial $\phi^3 -$ IQ ϕ = I = 0 with real root H. The index of this polynomial IG = 9x INDEX.

$\{$ IQ = -42 ; IN = -65 ; H = -1.47 ... ; H^2 = HHH = 2.16 ... $\}$

Subroutine FACTOR is now called, which gives all the ideals whose norms are not greater than MZ. They are ITAG in number and are set in the array LIST (1 - ITAG, 1 - 8).

$\{$ ITAG = 4 and

LIST (1, 1-8) = 1; 0,1,0; 0,0,1; 1 corresponding to ideal $[1, \theta, \theta^2]$ = I_1

LIST (2, 1-8) = 2; 1,1,0; 1,0,1; 2 corresponding to ideal $[2\ 1+\theta, 1+\theta^2]$ = I_2

LIST (3, 1-8) = 2; 0,2,0; 1,1,1; 4 corrsesponding to ideal $[2, 2\theta, 1+\theta+\theta^2]$ = I_3

LIST (4, i-8) = 4; 3,1,0; 3,0,1; 4 corresponding to ideal $[4, 3+\theta, 3+\theta^2]$ = I_4

and in the new variable the ideals become

$$I_1 = \left[1, \frac{6+3\phi}{9}, \frac{4+4\phi+\phi^2}{9}\right]$$

$$I_2 = \left[1, \frac{15+3\phi}{18}, \frac{13+4\phi+\phi^2}{18}\right]$$

$$I_3 = \left[1, \frac{12+6\phi}{18}, \frac{19+7\phi+\phi^2}{18}\right]$$

$$I_4 = \left[1, \frac{33+3\phi}{36}, \frac{31+4\phi+\phi^2}{36}\right]$$

after having been put in the form required for the application of the algorithm i.e. a fractional ideal which contains 1 as its smallest natural number. $\}$

UNIT (1) is then called which gives the fundamental unit of the field, (having transformed back to the old variable θ) viz $\dfrac{DD\ \theta^2 + DE\ \theta + DF}{DG}$

which is associated with prime principal ideals

$\left\{\left[1, \frac{6+3\phi}{9}, \frac{4+4\phi+\phi^2}{9}\right]\right.$ is the reduced form of I_1 and the lattice loop is:-

$$\begin{tikzcd} \left[1, \frac{3-3\phi}{9}, \frac{7+\phi+\phi^2}{9}\right] \arrow[d, bend left] \\ \left[1, \frac{7+\phi+\phi^2}{36}, \frac{12-12\phi}{36}\right] \arrow[u, bend left] \end{tikzcd}$$

Loop 1

and thus the fundamental unit is $\frac{3-3\phi}{9} \times \frac{7+\phi+\phi^2}{36} = \frac{\phi+2}{3} = \theta$

i.e. DD = DF = 0 DE = DG = 1 $\left.\right\}$

Now we call UNIT (2), ..., UNIT (ITAG) in turn corresponding to each of the lattices in LIST (2, -ITAG, 1-8), and we are eventually given CLAS the number of different lattice loops, and MARK.

The relevant information is then printed and we then consider the next field.

$\left\{\left[1, \frac{15+3\phi}{18}, \frac{13+4\phi+\phi^2}{18}\right]\right.$ has reduced form $\left[1, \frac{3-3\phi}{18}, \frac{16+\phi+\phi^2}{18}\right]$

which produces the loop

$$\begin{tikzcd} \left[1, \frac{3-3\phi}{18}, \frac{16+\phi+\phi^2}{18}\right] \arrow[d, bend left] \\ \left[1, \frac{7+\phi+\phi^2}{18}, \frac{6-6\phi}{18}\right] \arrow[u, bend left] \end{tikzcd}$$

Loop 2

The second ideal of the loop is the reduced form of I3

$\left[1, \frac{33+3\phi}{36}, \frac{31+4\phi+\phi^2}{36}\right]$ and has reduced form $\left[1, \frac{34+4\phi+\phi^2}{36}, \frac{3-3\phi}{36}\right]$

which leads on to Loop 1 as will be shown in detail at the end of the description of UNIT.

The results give us CLAS = 2 and MARK = 2, and so the cubic field K(θ)

generated by a zero θ of P has fundamental unit θ and class number 2.

UNIT (INK)

We consider the ideal

$$\left[1, \frac{\mathrm{LIST(INK,4)}\lambda + \mathrm{LIST(INK,3)}\theta + \mathrm{LIST(INK,2)}}{\mathrm{LIST(INK,1)}}, \frac{\mathrm{LIST(INK,7)}\lambda + \mathrm{LIST(INK,6)}\theta + \mathrm{LIST(INK,5)}}{\mathrm{LIST(INK,1)}}\right]$$

where $\lambda = \frac{\theta^2 + \mathrm{ISU}\,\theta + \mathrm{KH}}{\mathrm{INDEX}}$, in the field $K(\theta)$ where
$\theta^3 - \mathrm{IA}\,\theta^2 + \mathrm{IB}\,\theta - \mathrm{IC} = 0.$

Under the transformation $\phi = 3\theta - \mathrm{IA}$, $\phi^3 = \mathrm{IQ}\,\phi + \mathrm{IN}$ and the ideal becomes $\left[1, \frac{M1 + M2\,\phi + M3\,\phi^2}{\mathrm{IG}}, \frac{N1 + N2\,\phi + N3\,\phi^2}{\mathrm{IG}}\right]$

$\left\{\right.$ i.e. $\left[1, \frac{33 + 3\phi}{36}, \frac{31 + 4\phi + \phi^2}{36}\right]$ in the example $\left.\right\}$

RHO (U,V,W) defines the distance of $U + V\phi + W\phi^2$ from the real axis.
Now we enter a loop which is the consideration of Voronai's Algorithm.

STEP (I) We check that M2 x N3 - M3 x N2 > 0, and if not interchange the basis elements

$\{$ In the example $3 \times 1 - 0 \times 4 = 3 > 0$ $\}$

STEP (II) We calculate the values A, B, C (as described in Chapter 4)

$\{$ A = 9 ; B = 9.79.. ; C = 54.27.. $\}$

STEP (III) Check if B > 0, if not call subroutine SUB (0, -1, 1, 0) which alters basis from $[1, \phi', \psi']$ to $[1, -\psi', \phi']$

$\{$ B = 9.79 > 0 so original basis is left $\}$

STEP (IV) Check if A > B and C > B ; if B > A
we call subroutine SUB (1, -ID, 0, 1) where ID = $\left[\frac{B}{A}\right]$
and if C < B call SUB (1, 0, -ID, 1) where ID = $\left[\frac{B}{C}\right]$

and by repeated use of this section the three conditions A > B > 0, C > B are satisfied

{ A = 9, B = 9.79, ∴ A < B and so we call SUB (1, -1, 0, 1) to produce basis $\left[1, \frac{33+3\phi}{36}, \frac{-2+\phi+\phi^2}{36}\right]$; A = 9, B = 0.79, C = 43.69 }

STEP (V) We calculate RB = (M2 - M3 x H) RD = (N2 - N3 x H). Now one of the six pairs (RB, RD), (-RB, -RD), (RB-RD, RB), (RB + RD, -RB), (RD, -RB + RD), (-RD, RB - RD) and only one has positive first element and negative second. We find which and call the corresponding subroutine, no call to subroutine, SUB (-1, 0, 0, 1), SUB(1, 1, -1, 0); SUB (-1, -1, 1, 0) SUB (0, -1, 1, 1) : SUB (0, 1, -1, -1). This corresponds to finding which of the elements of the reduced Hexagon of Zelling cross the negative ξ axis (Chapter 4).

{ RB = 3.0 ; RD = 2.47 > 0 of the other possibilities RD > 0, RB - RD < 0 satisfy the above conditions so we call SUB (0, -1, 1, 1) to give a new basis
$$\left[1, \frac{-2+\phi+\phi^2}{36}, \frac{-35-2\phi+\phi^2}{36}\right] \Big\}$$

STEP (VI) Finds I, such that

$$0 < \frac{\text{M1} + \text{M2} \times \text{H} + \text{M3} \times \text{HHH}}{\text{IG}} - \text{I} < 1$$

and we reset M1 = M1 - I x IG, then we find a new value of I such that

$$0 < \frac{\text{N1} + \text{N2} \times \text{H} + \text{N3} \times \text{HHH}}{\text{IG}} - \text{I} < 1$$

and reset N1 = N1 - I x IG. This corresponds to finding the pinheads associated with the two basis elements.

$$\Bigg\{ \frac{-2 + \text{H} + \text{HHH}}{36} = -0.36 \qquad \text{I} = 1 \quad \text{new element} \quad \frac{34+\phi+\phi^2}{36} = \bar{\phi}$$

$$\frac{-35 - 2\text{H} + \text{HHH}}{36} = \frac{-29.9}{36} \qquad \text{I} = 1 \quad \text{new element} \quad \frac{1-2\phi+\phi^2}{36} = \bar{\psi}$$

in the notation of Chapter 4 }

STEP (VII) We calculate XA, XC where XA is the ξ coordinate of $\bar{\phi}$ and XC is the ξ coordinate of $\bar{\psi}$ and with the conditions described in Chapter 4 we choose two pinheads from the seven possible with reference to these values XA and XC and the distance RHO, i.e. we choose the pinheads with the smallest value of RHO.

$\{$ XA = -0.23   XC = -1.2

We have $\theta_0 = \bar{\phi} = \frac{34+\phi+\phi^2}{36}$ since XA $< \frac{1}{2}$ $\rho_0 = 336.1$

$\theta_1 = \bar{\psi} = \frac{1-2\phi+\phi^2}{36}$ since XC $< \frac{1}{2}$ $\rho_1 = 1909.1$

$\theta_2 = 1-\bar{\phi}+\bar{\psi} = \frac{3-3\phi}{36}$ since 1 - XA + XC $< \frac{1}{2}$ and $\bar{\phi}-\bar{\psi} > 0$

hence $\rho_2 = 393.2$

It was not necessary to calculate θ_3 since $\rho_2 < \rho_1$

The reduced basis is $\left[1, \frac{34+\phi+\phi^2}{36}, \frac{3-3\phi}{36}\right]$ $\}$

STEP (VIII)

We have a reduced basis $\left[1, \frac{\text{M1} + \text{M2}\,\phi + \text{M3}\,\phi^2}{\text{IG}}, \frac{\text{N1} + \text{N2}\,\phi + \text{N3}\,\phi^2}{\text{IG}}\right]$ where M1, M2, M3, N1, N2, N3, IG have no common factor because of the use of subroutine ICF.

Setting N initially at 1 we define $\phi_N = \frac{\text{M1} + \text{M2}\,\phi + \text{M3}\,\phi^2}{\text{IG}}$ and then increment N and divide the lattice by ϕ_{N-1} (the ϕ_N are stored in arrays IAN and NP) and repeat the process to find a reduced basis for the new lattice. The division is produced by multiplying the lattice by ϕ_{N-1}^{-1}, ϕ_{N-1}^{-1} being obtained by the subroutine INVER, until we eventually produce a loop of lattices which has either not occurred previously or one which has. With the production of each new loop we set ITEST (1-7, ITIB) to be M1, M2, M3, N1, N2, N3, IG, the first reduced lattice values of the loop. ITIB was initially set to zero and incremented each time a new lattice loop is found. MARK is set to the norm of the initial lattice of the new loop.

At the end of each reduction process we first check if the lattice has occurred in a previous loop, by comparing M1, M2, M3, N1, N2, N3, IG with ITEST (1-7, 1-ITIB). If such an occurrence happens the completion of the loop will give us no new information so we return to the main program.

If not we must check if a new loop has been produced, this is done by comparing M1, M2, M3, N1, N2, N3, IG with the previous bases of lattices in the loop, which have been stored in IAN (1 − 3, 1 − (N − 1)) JAN (1− 3, 1 − (N-1)) and NP (1 − (N − 1)). If the initial lattice of the loop is the integral lattice of the field we enter Section 2 otherwise we return. This section calculates the fundamental unit of the field by multiplying the ϕ_i 's together. Since some of the units get rather large (some coefficients as large as 10^{30}), it is necessary to use double precision. It is also necessary then to transform the unit to the original representation by the transformation $\theta = \frac{\phi + I A}{3}$. As a safeguard on the number of lattices in the loop we required N < 99, but none of the loop did reach this number.

{ We now conclude the description of the example.

$\left[1, \frac{34+\phi+\phi^2}{36}, \frac{3-3\phi}{36}\right]$ is the reduced basis. We devide the lattice by $(34+\phi+\phi^2)/36$ to obtain the new lattice

$$\left[1, \frac{7+\phi+\phi^2}{36}, \frac{19-11\phi+\phi^2}{36}\right]$$

Step I M2.N3 - M3.N2 = 12 > 0

Step II A = 43.69 ; B = 40.5 ; C = 181.3

Step III,IV A > B > 0 ; C > B so we leave original basis

Step V RB = 2.47 > 0 ; RD = -9.5 < 0 so we leave the basis unchanged.

Step VI $\quad \phi_1 = 0.213 \ldots \qquad \psi_1 = 1.03 \ldots$

$I_{\phi_1} = 0 \; ; \; I_{\psi_1} = -1$ thus

$\bar{\phi} = \phi_1 \; ; \quad \bar{\psi} = \psi_1 - 1$ and so the new basis is

$$\left[1 \, , \frac{7+\phi+\phi^2}{36} \, , \, \frac{-17-11\phi+\phi^2}{36} \right]$$

Step VII $\quad XA = -0.981 < \frac{1}{2} \; ; \; XC = -1.89 < \frac{1}{2}$

$\bar{\phi} - \bar{\psi} > 0 \qquad$ and $1 - XA + XC < \frac{1}{2}$

thus $\quad \theta_0 = \bar{\phi} \qquad \rho_0 = 1515.9 \ldots$

$\theta_1 = \bar{\psi} \qquad \rho_1 = 8608.9 \ldots$

$\theta_2 = 1 - \bar{\phi} + \bar{\psi} \qquad \rho_2 = 6291.97 \ldots$

and since $\rho_2 < \rho_1$ we need not calculate θ_3

and the reduced basis is $\left[1 \, , \frac{7+\phi+\phi^2}{36} \, , \, \frac{12-12\phi}{36} \right]$

But this basis occurred in the reduction of the integral lattice i.e. loop 1. And so we have the loop

$$\begin{tikzcd}
\left[1 \, , \frac{34+\phi+\phi^2}{36} \, , \, \frac{3-3\phi}{36}\right] \arrow[r] & \left[1 \, , \frac{7+\phi+\phi^2}{36} \, , \, \frac{12-12\phi}{36}\right] \arrow[d, bend left] \\
 & \left[1 \, , \frac{3-3\phi}{9} \, , \, \frac{7+\phi+\phi^2}{9}\right] \arrow[u, bend left]
\end{tikzcd}$$

CHAPTER 7

The Check of the Initial Table

Main Program - HASSE

Let P(1), ... P(35) denote the first 35 primes, P(35) = 149 being the final prime required since it is the smallest prime whose square is greater than 20,000. For a given value L, LMZ gives the index of the smallest prime whose square is greater than L. ITOT is initially set to zero but eventually gives the total cubic number fields with negative discriminant that are produced.

The first loop of the program sets J(1) = JJ x 4 and J(2) = J(1) + 3, so that as JJ takes the values 5 to 5000, the sets - J(1) and - J(2) then include all discriminants of cubic number fields which lie between -23 and -20,000. (All discriminants are ≡ 0 or 1 mod 4 (SCHUR (28)). Using the P's we may factorise any of the numbers J(1) and J(2) which occur. We set L = J(I), I = 1 or 2 and IB = -L, where IB is the possible field discriminant we are checking. Arrays INDEX (1 – 6) and JNDEX (1 — 6) are cleared; then by varying IJ from LMZ to 35 we find the first prime P(IJ) such that P(IJ) x x 2 > L and we reset LMZ to IJ, and MZ (which is the bound on the index of P required in factorising L) to IJ - 1. Q(1) has been set to 2 and Q(2) to 3, Q(3 – IP) will eventually contain all prime factors of L which are not equal to 2 or 3. We know that if L is less than 20,000 then L can have at most 4 such prime factors and hence IP ≤ 6. INDEX (I) will show to what power Q(I) divides L. First we find to what power Q(1) = 2 divides L by dividing L successively by 2 until it is prime to 2. Each time increasing INDEX (1) by 1 and a similar procedure is carried out for INDEX (2). Next IP is initially set to 2 and by varying

IJ between 3 and MZ we find if P(IJ) divides L and if so we set IP to IP + 1, Q(IP) to P(IJ), INDEX (IP) = 1 and L = L/Q(IP). We then see if Q(IP) still divides L; if so we set INDEX (IP) = INDEX (IP) + 1 and L = L/Q(IP) and repeat this process until L and Q(IP) are coprime. If the final value of L is not 1 then L is a prime which is greater than P(MZ) and so we set IP = IP + 1, Q(IP) = L and INDEX (IP) = 1.

By Theorem 2.1, we know that

$$\text{INDEX (I)} \le 3 \qquad \text{if } I \ge 3$$

and

$$\text{INDEX (1), INDEX (2)} \le 5$$

Hence if one of these conditions is not satisfied we reject IB as a cubic field discriminant.

Next, IDET, the associated quadratic discriminant of IB, is found. The relation

$$\text{IB} = \text{IDET * ITAL * * 2}$$

uniquely determines IDET and ITAL, where IDET is of the form a) $4m$, $m \equiv 2$ or $3 \bmod 4$ or b)m, $m \equiv 1 \bmod 4$. To find these values, we initially set ITAL = IDET = 1 and by varying M from 2 to IP set

$$\text{JNDEX (M)} = \frac{\text{INDEX (M) - MOD (INDEX (M), 2)}}{2} \qquad \text{(also for M = 1)}$$

$$\text{IDET} = \text{IDET * Q(M) * * MOD (INDEX (M) 2)}$$

$$\text{ITAL} = \text{ITAL * Q(M) * * JNDEX (M)}$$

For M = 1 (i.e. the case we 2 divides IB) we observe the following rules

$$\text{ITAL} = \text{ITAL * 2 * * JNDEX (1)}$$

$$\text{IDET} = \text{-IDET * 2 * * MULT}$$

where JNDEX (1) and MULT are given by the table

INDEX (1)	MULT	JNDEX (1)	
5	3	1	
4	2	1	
3	3	0	
2	2	0	if IDET $\not\equiv$ 1 mod 4
2	0	1	if IDET $\equiv$ 1 mod 4
1	no field		
0	0	0	

Now we check that the final value of IDET $\equiv$ 0 or 1 mod 4. Having obtained IDET we now find a defining polynomial x^2 - FIAx + FIB of the field with this discriminant. FIA and FIB are given by the formulae

$$\text{if IDET} \not\equiv 1 \bmod 4 \quad \text{then FIA} = 0 \quad \text{and} \quad \text{FIB} = \frac{-\text{IDET}}{4}$$

$$\text{if IDET} \equiv 1 \bmod 4 \quad \text{then FIA} = 1 \quad \text{and} \quad \text{FIB} = \frac{(1-\text{IDET})}{4}$$

If ITAL (f in Hasse's notation, the Führer of the field) is 1 we call subroutine NEG (IDET,ICL) which gives us ICL, the number of basis elements of the ideal group of index 3 in the quadratic field (if any).

The number of cubic fields with discriminant -IB is given by Theorem 2.2 as NOF = (3 * * ICL - 1)/2, and we then jump to the printout routine.

If ITAL > 1 we calculate ISEM, the number of primes $\neq$ 3 which divide ITAL. For each such prime we check the quadratic residue of condition of Theorem A i.e. if Q(I) divides ITAL, Q(I) $\neq$ 3 then we must have Q(I)$\equiv \left(\frac{\text{IDET}}{\text{Q(I)}}\right)$ mod 3.

LO = $\left(\frac{\text{IDET}}{\text{Q(I)}}\right)$ is the Kronecker symbol which is calculated by subroutine QUAD (IDET, Q(I)) and returned via common store.

Now IDEL (δ in Hasse's notation) is calculated by the rules if JNDEX (2) = 0 then IDEL = 0 ;

if IDET $\not\equiv$ 0 mod 3 and JNDEX (2) = 2 then IDEL = 1 ;

if IDET $\equiv \pm 3$ mod 9 and JNDEX (2) = 1 then IDEL = 1 ;

if IDET $\equiv -3$ mod 9 and JNDEX (2) = 2 then IDEL = 2 ;

otherwise there is no cubic field with discriminant IB.

By calling subroutine NEG (IDET, ICL), we obtain ICL, the number of basis elements of the ideal group of index 3 in K(θ) (e in Hasse's notation).

If ICL = 0 and IDET $\neq$ -3 then the corollary to Theorem 2.3 gives

$$\begin{aligned} NOF &= 2 ** (ISEM + IDEL - 1) && \text{if } IDEL \neq 2 \\ &= 3 * 2 ** ISEM && \text{if } IDEL = 2 \end{aligned}$$

In the case when IDET = - 3 or ICL > 0 we set SUM = 0, and by using subroutines QUAD and PROOT if either a prime Q divides ITAL and Q $\neq$ 3 or if 3 divides ITAL and IDET, we increment SUM by 1 and find IR (1, SUM) θ + IR (2, SUM) (Hasse's ρ_i). To find any remaining ρ_i's (i.e. if Q = 3 and the above conditions are not satisfied) subroutine SOLVE is used, and this also produces KOP (i,j) (the yij of Hasse). We fix Y(1) = 1 (Y(i) is the Yi of Hasse's notation) and vary Y(2), ..., Y(ISEM) between 1 and 2; if IDEL = 2 we let Y(ISEM + 1) vary between 0, 1, 2.

The series of loops produce all non proportional solutions of the equations

$$\sum_{i=1}^{ISEM+IDEL-1} KOP(i, k) * Y(i) \equiv 0 \bmod 3 \qquad 1 \leq k \leq ICL$$

IDI times. IDI = 2 ** (4 - ISEM) if IDEL $\neq$ 2

= 3 * 2 ** (4 - ISEM) if IDEL = 2

Thus the NOF solutions contain NOF/IDI non proportional solutions, and we reset NOF to this value. Finally we have that the number of cubic fields with discriminant IB is given by NOF = (3 ** ICL) * NOF .

QUAD (I,J)

This routine calculates the Kronecker symbol $\left(\frac{I}{J}\right)$ = K where I is the discriminant of the quadratic field K(θ) defined by the polynomial $x^2 - IAx + IB$. IA, IB are obtained from common store.

K is evaluated thus:-

if J divides I then we set K = 0

if the ideal (J) factorises in K(θ) then K = 1 otherwise K = -1

K is initially set at zero, and if J divides I we return this value. If not, K is set to -1 and we see if there is an L in the interval [1, J] such that $L^2 + IA * L + IB$ is divisible by J; if so then K is returned as +1.

HCF (IJ, IK, IH)

This routine calculates the h.c.f. of two integers IJ and IK in a method similar to that used in the routine ICF of the Voronoi program.

MULT (A,B,C,D,L,M,P)

A, B, C, D, are integers, θ satisfies $\theta^2 - IA\theta + IB = 0$. This subroutine calculates the integers L, M where

$$L + M\theta \equiv (A + B\theta)(C + D\theta) \mod P$$
$$0 \leq L, M \leq P - 1$$

EQV (IDET, I, J, K, L, M)

We have the field K(θ) as before and NORM (J) = Norm (θ + J). [I, θ + J] is an ideal in K(θ) and thus the numbers $\theta + J \pm (N * I)$ for integral N lie in the ideal. By varying N between 1 and K we may find a number $\theta + J + (N * I)$ whose norm when divided by I is prime to K. Such a number is θ + NN and the ideal $\left[\frac{N(\theta + NN)}{I}, \theta + NN\right]$ is equivalent to $[I, \vartheta + J]$. By a method similar to CUBE see below, we fixed integers L, M such that Norm $(L \vartheta + M) = \text{Norm}(\vartheta + KN)^3$ and $(L \vartheta + M)$ is equivalent to $[I, \vartheta + J]^3$.

TRIPLE (LT, IAN)

As before we have a field $K(\vartheta)$, where $\vartheta^2 - IA\,\vartheta + IB = 0$ and $NORM\,(J) = |\text{Norm}\,(\vartheta + J)|$

This subroutine finds the values of JB such that $[LT, \vartheta + JB]$ is a Gauss reduced ideal i.e.

$$- LT < 2 * JB + IA \leq LT < \frac{1}{LT} * NORM\,(JB)$$

or $\quad 0 \leq 2 * JB + IA < LT \quad$ if $LT * * 2 = NORM\,(JB)$

(LT is fixed having been read into the subroutine as a parameter).

We do this by allowing JB to vary between $\frac{-LT - IA + 1}{2}$ and $\frac{LT - IA}{2}$ and then checking the above inequalities.

IAN was initially set to zero, then after each value of JB is produced IAN is incremented by 1, I(IAN) is set to JB. Finally the array I is returned via common store, and the final value of IAN is returned as a parameter.

NEG (IDET, ICL)

We are given IDET, the discriminant of a quadratic field $K(\vartheta)$, where $IDET < 0$ and $\vartheta^2 - IA\,\vartheta + IB = 0$. The Minkowski bound of the field, viz. $IQ = \sqrt[2]{-IDET/3}$, is now calculated.

NORM (I) will give the absolute value of the norm of the algebraic integer $\vartheta + I$. We initially set ICL to zero and CLASNO to 1; where ICL will eventually give the number of basis elements of the ideal group of index 3 in the field, and CLASNO the class number of the field.

KEEP $(K, 1)\ \vartheta$ + KEEP $(K, 2)$, $K = 1, \ldots,$ ICL gives the basis elements of the ideal group, and if the field has a fundamental unit which is not unity, KEEP (ICL + 1, 1) ϑ + KEEP (KL + 1,2) will be that unit.

If IDET = -3 then we know that the field has no ideal group of index 3, and the fundamental unit of K(ϑ), (where $\vartheta^2 - \vartheta + 1 = 0$) is ϑ . Hence KEEP (1, 1) = 1 and KEEP (1, 2) = 0. (We assume that the field is such that ICL $\leq$ 2). If IDET $\neq$ -3 then we find CLASNO by finding the number of Gauss reduced pairs JA, JB for which

$$-JA < 2 * JB + IA \leq JA < \frac{1}{JA} * NORM (JB)$$

or $\quad 0 \leq 2 * JB + IA < JA$ if $JA ** 2 = NORM (JB)$

(See Gauss (14)). By a similar method to TRIPLE we let JA vary between 2 and IQ and for every value of JB found to satisfy the above inequalities, we increase CLASNO by 1. If 3 does not divide CLASNO then there does not exist an ideal group of index 3, hence ICL = 0. However if 3 | CLASNO we call CUBE (IDET, ICL) which calculates ICL and the values of KEEP (K, 1), KEEP (K, 2), K = 1, ICL .

<u>SOLVE (LM, LN, ITO, IZ)</u>

We set P = IR (3, ITO) ; N = NT (ITO) is the bound required in the search for variable JKJ found below. If P $\neq$ 3, we consider the two possibilities that IR (4, ITO) = $\left(\frac{IDET}{P}\right)$ is or is not equal to 1. When IR (4, ITO) = 1 we find an integer LIJ , 1 $\leq$ LIJ $\leq$ P such that N(ϑ + LIJ) $\equiv$ 0 mod P, and consequently the integer IX such that IX $\equiv$ LM ϑ + LN mod [P, ϑ + LIJ] i.e. IX $\equiv$ LN - LM * LIJ mod P.

Then we find JKJ $\ni$ (IR (2, ITO)) ** JKJ $\equiv$ IX mod P, (IR (2, ITO)) is the ρ_{ITO} in Hasse's notation, and we set KOP (IZ, ITO) = MOD (JKJ, 3) which is Hasse's variable $y_{ITO,IZ}$.

If IR (4, ITO) = 1 we raise ρ_{ITO} = IR (1, ITO) ϑ + IR (2, ITO) to the integer power JKJ, and checking that the result ICV ϑ + ICU is congruent to LM ϑ + LN mod P. Then, as previously, we set KOP (IZ, ITO) = MOD (JKJ, 3) If P = 3 we need to find the remaining ρ_i's and corresponding y_{ik}'s. We first change LM ϑ + LN into the equivalent form MM $\sqrt[2]{\text{IDET}}$ + MN. If IDEL = 2 we find J such that MN * J $\equiv$ 1 mod 9 and then let LL = MOD (J * M, 9).

$$\text{Then}\quad \text{KOP (IZ, SUM)} \;=\; \left[\frac{\text{LL} + 1}{3}\right] - 1$$

$$\text{and}\quad \text{KOP (IZ, SUM + 1)} \;=\; 3 + \text{LL} - \left[\frac{\text{LL} + 1}{3}\right],$$

the last two results coming from the way that 1 + 3 $\sqrt[2]{\text{IDET}}$ and 1 + $\sqrt[2]{\text{IDET}}$ form a complete set of residues.

i.e. $$\text{MM}\sqrt[2]{\text{IDET}} + \text{MN} \;\equiv\; (1 + 3\sqrt[2]{\text{IDET}}\,) ** \text{KOP (IZ, SUM)} * (1 + \sqrt[2]{\text{IDET}}\,) ** \text{KOP (IZ, SUM + 1)}$$

If IDEL = 1 however then we find J so that M N * J $\equiv$ 1 mod 3 and set KOP (IZ, SUM) $\equiv$ MN * J mod 3 since

$$\text{MM}\sqrt[2]{\text{IDET}} + \text{MN} \;\equiv\; (1 + \sqrt[2]{\text{IDET}}) ** \text{KOP (IZ, SUM)} \bmod 3$$

PROOT (P)

We have, as before, a field K(ϑ), ϑ^2 - IA ϑ + IB = 0 and LM ϑ + LN is a basis element of the ideal group of index 3 in K(ϑ) (PROOT is only called if such an ideal group does exist, or the field has a unit, and LM ϑ + LN is set to be the fundamental unit. SUM is passed to the routine via common store, where it is increased by 1 and then the routine calculates the primitive root of $\mathfrak{p}$ (P prime) IR (1, SUM) ϑ + IR(2, SUM) and also sets IR (3, SUM) = P and IR (4, SUM) = KS = $\left(\frac{\text{IDET}}{\text{P}}\right)$ (where the $(\;)$ denotes the Kronecker symbol). We assume that the value of SUM never exceeds 8.

The Euler function Φ of P in K(ϑ) is (P - 1)(P - KS) if P is prime. We set M = P - 1 and N = P - KS then Φ = M * N and M is the Euler function of P in the rational field. The case when P = 9 is also considered, if

KS $\neq$ 1 then N = 72 otherwise N = 36.

For prime P if KS = 1 we need only consider the rational primitive roots of P so we set N = 1, and these primitive roots are produced by examining numbers I to see which satisfy $1 \leq I \leq P - 1$ and

$$I^{P-1} \equiv 1 \bmod P \qquad I^{T} \not\equiv 1 \bmod P \qquad \forall T \text{ such that } 1 \leq T \leq P - 1$$

If KS = -1 or P = 9 then we let I, J vary independently between 1 and P and check if $(J\,\vartheta + I)^{N-1} \equiv L \bmod P$ where L is a rational integer and HCF (L, P) = 1 where $(J\,\vartheta + I)^{T} \not\equiv$ rational integer $1 \leq T \leq N - 1$.

CUBE (IDET, IEZ)

We consider the field K(ϑ), where $\vartheta^{2} - IA\,\vartheta + IB = 0$. IEZ, which will eventually give the number of basis elements of the ideal group of index 3, is set initially to zero; IBO, the Minkowski bound, is $\sqrt[2]{-IDET/3}$.

The program is divided into 3 main sections.

The first section considers the case when IDET $\equiv$ 1 mod 4. We let LT vary between 1 and IBO and call TRIPLE (LT, IAN) for each LT. IAN gives the number of Gauss-reduced ideals of the form $[LT,\ \vartheta + I(IAM)]$ where $1 \leq IAM \leq IAN$. To find members of the ideal group of index 3, we look for algebraic integers of K(ϑ) of norm LT * * 3, there being no integer of norm LT. The method is to look for integers LMS and I2 such that Norm (LMS ϑ + I2) = LT * * 3 = LTT. If LMS > 0 the minimum value of NORM (LMS ϑ + I2) for fixed LMS is (IB - $\frac{1}{4}$) * LMS * * 2 which occurs when I2 = -LMS/2.

Hence LMS $\leq 2 * LT * \dfrac{LT}{4*IB - 1} * * 0.5 = 2 * LT * \dfrac{LT}{IDET} * * 0.5 = JBO$

We let LMS vary between 1 and JBO and search for I2, a solution of the equation

$$I2 * (I2 + LMS) = LTT - LMS * * 2 * IB = LMT$$

R.H.C. ARY

i.e. I2 x I1 = LMT where I1 = I2 + LMS

Once a solution (LMS, I2) has been found we check if IX, the h.c.f. of LMS and I2, is not 1 and IX does not divide IDET. Otherwise we may ignore the solution as it simply involves rational multiples of a previous solution. Then we check to see if it belongs to one of the IAN ideals, and if so we have found one member of the ideal group of index 3. We then increase IEZ by 1 and set ICU (IEZ, 1) = LMS, ICU (IEZ, 2) = IZ, ICU (IEZ, 3) = LT and ICU (IEZ, 4) = I (IG). In other words, we have an ideal [LT, ϑ + I(IG)] which when cubed is equivalent to (LMS ϑ + I2).

The second section contains similar operations to the first except instead we consider the case IDET $\equiv$ 0 mod 4. We let LT vary from 2 to IBO, and for each LT, LMS varies from 2 to JBO and for each LMS set I2 $= \sqrt[4]{\text{LTT-LMSxx2xIB}}$ and check if Norm (LMS ϑ + I2) = LTT, and continue as in section 1.

In section 3 we check that the number of basis elements of the ideal group index 3 is either 1 or 2 (otherwise a diagnostic is printed and the program stops). If, the number of basis elements KE is 2 i.e. we have 1 < IEZ $\leq$ 8, we produce a Gauss reduced ideal equivalent to [ICU (1,3), ϑ + ICU (1,4)]xx2, $\mathfrak{J}$ say. We check this ideal against the list of ideals [ICU (K, 3), ICU (K, 4) + ϑ], 2 $\leq$ K $\leq$ IEZ, and the first one not equal to $\mathfrak{J}$ say K = K', we take as the provisional second basis element of the ideal group. [ICU (1, 3), ϑ + ICU (1, 4)] is provisionally taken to be the first basis element. If the second basis element is not prime to ITAL, we call EQV (IDET, KU (K', 3), ICU (K', 4), ITAL, KEEP (2,1), KEEP (2,2)), otherwise we set KEEP (2,1) = ICU (K', 3) and KEEP (2,2) = ICU (K', 4). If ICU (1, 3) is not prime to ITAL we call the subroutine EQV (IDET, ICU (1,3), ICU (1,4), ITAL, KEEP (1,1), KEEP (1,2)) or otherwise set KEEP (1,1) = ICU (1,3) and KEEP (1,2) =ICU (1,4).

Hence [KEEP (1,1), θ + KEEP (1,2)] (and [KEEP (2,1), θ + KEEP (2,2)] if KE = 2) are basis elements for the ideal group of index 3, which are prime to ITAL.

REFERENCES

1. E. Artin, 'Theory of Numbers' (Göttingen, 1959)

2. P. Bachmann, 'Allgemeine Arithmetik der Zahlkorper' (Leipzig, 1905)

3. P. Bachmann, 'Die Arithmetik der quadratischen Formen' (Leipzig, 1892)

4. G. Bergmann, 'Zur numerischen Bestimmung einer Einheitsbasis', Math. Annalen 166, 103-105 (1966)

5. G. Bergmann, 'Beispiel numerischen Einheits bestimmung', Math. Annalen 167, 143-168 (1966)

6. L. Bernstein and H. Hasse, 'An explicit formula for the units of an algebraic number field of degree n ≥ 2', Pacific J. Math. 30 (1969), 293-365.

7. W.E.H. Berwick, 'The classification of Ideal Numbers that depend on a cubic irrationality', Proc. London Math. Soc. (2) 12 (1914), 393-429.

8. J.W.S. Cassels, 'An introduction to the geometry of numbers', Berlin-Göttingen-Heidelberg, 1959)

9. H. Davenport, 'On the product of three homogeneous linear forms III', Proc. London Math. Soc. (2) 45 (1939), 98-125.

10. H. Davenport and H. Heilbronn, 'On the density of discriminants of cubic fields', Bull. London Math. Soc., 1 (1969), 345-348.

11. R. Dedekind, 'Ueber die Anzahl der Ideal klassen in reinen kubischen Zahl körpern', Journal f.d. reine und angew. Math. 121 (1900), 40-123.

12. B.N. Delone and D.K. Fadeev, 'Theory of Irrationalities of the third degree', Acad. Sci, U.R.S.S. Trav. Inst. Math. Stekloff, 11 (1940), (also Translations of the Amer. Math. Soc. Vol).

13. L.E. Dickson, 'History of the Theory of Numbers', (New York, 1952).

14. J.C.F. Gauss, 'Disquisitiones Arithmeticae', (New Haven, 1966).

15. H.J. Godwin and P. A. Samet, 'A table of real cubic fields', Journal London Math. Soc. 34 (1959), 108-110.

16. H.J. Godwin, 'The determination of units in totally real cubic fields', Proc. Camb. Phil. Soc. 56(4) 1960, 318-321.

17. H.J. Godwin, 'The determination of the class number of totally real cubic fields', Proc. Camb. Phil. Soc. 57(4) 1961, 728-730.

18. H.J. Godwin, 'On quartic fields of signature one with small discriminant', Quart. J. Math. Oxford (2), 8 (1957), 214-22.

19. H.J. Godwin, 'Real quartic fields with small discriminant', Journal London Math. Soc. 31 (1956), 478-485.

20. H.J. Godwin, 'On totally complex quartic fields with small discriminant', Proc. Camb. Phil. Soc. 53 (1957), 1-4.

21. H.J. Godwin, 'On relations between cubic and quartic fields', Quart. J. Math. Oxford (2), 13 (1962), 206-12.

22. H.J. Godwin, 'The determination of fields of small discriminant with a given subfield', Math. Scand. 6 (1958), 40-46.

23. H. Hasse, 'Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage', Math. Z. 31 (1930) 565-582.

24. C.G.J. Jacobi, 'Allgemeine Theorie der Ketterbruchähnlichen Algorithmen in welchen jede Zahl aus drei vorgehenden gebildet wird', Journal f.d. reine und angew. Math. 69 (1868), 29-64.

25. E. Landau, 'Vorlesungen über Zahlentheorie', (New York, 1947).

26. G.B. Mathews, 'On the reduction and classification of binary cubics which have a negative discriminant', Proc. London Math. Soc. (2), 10 (1912), 128-138.

27. H. Minkowski, 'Geometrie der Zahlen' (New York, 1953).

28. I. Schur, 'Elementarer Beweis eines Satzes von L. Stickelberger', Math. Z. 29 (1928) 464-5.

29. J. Sommer, 'Introduction a la theorie des nombres algebriques' (Paris, 1911)

30. L.W. Reid, 'Tafel der Klassenzahlen fur kubische Zahlkörper', Amer. Jour. Math., Vol. 23 (1901), 68-84.

31. G.F. Voronoi, 'On the generalisation of the algorithm of continued fractions' Doctoral Thesis, Warsaw 1896.

32. J.V. Uspensky, 'A method for finding units in cubic orders of negative discriminant', Trans. Amer. Math. Soc. 33 (1931), 1-22.

33. E.I. Zolotareff, 'On an indeterminate equation of the third degree'.