1990

Some examples in low-dimensional algebraic number theory

Robert Allen Supencheck
San Jose State University

Follow this and additional works at: https://scholarworks.sjsu.edu/etd_theses

---

Recommended Citation

Supencheck, Robert Allen, "Some examples in low-dimensional algebraic number theory" (1990). *Master's Theses*. 3296.

DOI: <https://doi.org/10.31979/etd.ux7a-p7hs>

https://scholarworks.sjsu.edu/etd_theses/3296

This Thesis is brought to you for free and open access by the Master's Theses and Graduate Research at SJSU ScholarWorks. It has been accepted for inclusion in Master's Theses by an authorized administrator of SJSU ScholarWorks. For more information, please contact scholarworks@sjsu.edu.

INFORMATION TO USERS

The most advanced technology has been used to photograph and reproduce this manuscript from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

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

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

U·M·I

University Microfilms International
A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
313 761-4700 800 521-0600

Order Number 1340549

Some examples in low-dimensional algebraic number theory

Supencheck, Robert Allen, M.S.

San Jose State University, 1990

U·M·I

300 N. Zeeb Rd.
Ann Arbor, MI 48106

**SOME EXAMPLES IN LOW-DIMENSIONAL
ALGEBRAIC NUMBER THEORY**

A Thesis

Presented to

The Faculty of the Department of Mathematics

San Jose State University

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

By

Robert Allen Supencheck

May, 1990

APPROVED FOR THE DEPARTMENT OF MATHEMATICS

Dr. Hugh Edgar

Dr. Brian Peterson

Dr. Roger Alperin

APPROVED FOR THE UNIVERSITY

ABSTRACT

SOME EXAMPLES IN LOW-DIMENSIONAL ALGEBRAIC NUMBER THEORY

by Robert A. Supencheck

This thesis presents some recent results in algebraic number theory. In particular, low-degree extensions of the rational numbers will be utilized. The first chapter presents a correction of an article by C. E. van der Ploeg [14] which proves the identity

$$\sqrt{5} + \sqrt{22 + 2\sqrt{5}} = \sqrt{11 + 2\sqrt{29}} + \sqrt{16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}}}.$$

This article contained quite a few typographical errors, which will be corrected in the first chapter. The second and third chapters present some solutions to the equation $\alpha\beta\gamma = \alpha + \beta + \gamma$. In chapter 2 a solution to the equation $a + b + c = abc = 1$ in a cyclic cubic extension of the rational numbers will be shown to exist. Also in chapter 2, all the integral points on the curves $Y^2 = -4X^3 + X^2 + 18X - 31$, and $Y^2 = X^3 + X^2 - 72X - 496$ will be determined. In chapter 3, solutions to the equation $\alpha\beta\gamma = \alpha + \beta + \gamma$, where α , β , and γ are units in the rings of integers of some low-degree extensions of the rational numbers, will be found.

ACKNOWLEDGEMENTS

Although I, as a human being, am limited to finitude, nonetheless I feel an infinite amount of gratitude to Professors Hugh Edgar, Brian Peterson, and Roger Alperin. To Professor Edgar, I am grateful for his tireless assistance with not only advising me and proofreading this thesis, but also for providing me with the basis for this thesis. To Professor Peterson, I am grateful for his patience and detailed proofreadings of the rough drafts of this thesis. To Professor Alperin, I am grateful for his helpful suggestions and for motivating me.

CONTENTS

Abstract	iii
Acknowledgements	iv
Chapter	
1. Shanks's Identity	1
2. A Solution to $abc = a + b + c = 1$ in a Cyclic Cubic Rational Extension	14
3. Unit solutions to $\alpha + \beta + \gamma = \alpha\beta\gamma$ in Rings of Integers of Low-Degree Rational Extensions	26
Bibliography	46

CHAPTER 1

Shanks's Identity

This chapter presents an argument as to why the identity,

$$\sqrt{5} + \sqrt{22 + 2\sqrt{5}} = \sqrt{11 + 2\sqrt{29}} + \sqrt{16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}}},$$

holds. Daniel Shanks, when he published this identity [11], referred to it as an “incredible identity.” C. E. van der Ploeg [14] sought to make this identity more credible. However, the published version of his attempt contained many typographical errors in addition to some theoretical mistakes. This chapter will follow his line of argument, except for the following modifications (excluding the corrections of obvious typographical errors):

1. The statement of part (1) of the theorem, following Lazarus [7], has been changed from “K is a nonnormal quartic” to “K is a nonnormal quartic extension of Q containing a quadratic subfield,” and the proof of the theorem has been modified accordingly;
2. The proof of van der Ploeg's lemma has been altered to avoid

using Capelli's theorem, which was unnecessary, and another lemma has been presented before van der Ploeg's lemma in order to simplify the proof of his lemma; and

3. The two lattice diagrams presented below include a quadratic subfield which did not appear in van der Ploeg's article.

Before presenting van der Ploeg's argument, some definitions need to be given. If two extensions of the rational numbers are generated by different roots of the same minimal polynomial with rational coefficients, then the two extensions are *conjugates* of each other. *Normal extensions* of the rational numbers are those that coincide with all their conjugates, and *normal polynomials* are irreducible polynomials whose roots generate the same field. *Nonnormal extensions* of the rational numbers are, then, those that do not coincide with their conjugates. If two different polynomials have roots that generate the same set of conjugate fields, then these polynomials are *equivalent*.

The following theorem will be used to make Shanks's identity more credible.

THEOREM: The following are equivalent.

(1) K is a nonnormal quartic extension of $\mathbb{Q}$ containing a quadratic subfield.

(2) K has a nonnormal biquadratic minimal polynomial of the form $x^4 + ax^2 + b$ for $a, b \in \mathbb{Q}$.

(3) K is a quartic extension with normal closure whose Galois group is dihedral.

Proof: (1) $\Rightarrow$ (2): Let $\mathbb{Q}(\sqrt{t})$ be a quadratic subfield of K , where t is some squarefree element of $\mathbb{Z}$. Then $K = \mathbb{Q}(\sqrt{\alpha})$ for some $\alpha \in \mathbb{Q}(\sqrt{t})$, with α squarefree over $\mathbb{Q}(\sqrt{t})$. Because $\mathbb{Q}(\sqrt{t})$ is a vector space over $\mathbb{Q}$ with $\{1, \sqrt{t}\}$ as a basis, $\alpha = r + s\sqrt{t}$ for some $r, s \in \mathbb{Q}$, and the minimal polynomial for $\sqrt{\alpha}$ over $\mathbb{Q}(\sqrt{t})$ is $x^2 - \alpha = x^2 - (r + s\sqrt{t})$, and that for $\sqrt{\alpha}$ over $\mathbb{Q}$ is $x^4 - 2rx^2 + (r^2 - s^2t) = [x^2 - (r + s\sqrt{t})] \cdot [x^2 - (r - s\sqrt{t})]$. This biquadratic polynomial is irreducible with respect to $\mathbb{Q}$, and nonnormal by assumption on K .

(2) $\Rightarrow$ (3): By assumption, K is generated over $\mathbb{Q}$ by a root of $f(x) = x^4 + ax^2 + b$ for $a, b \in \mathbb{Q}$. By setting $d = a^2 - 4b$, the roots of this biquadratic polynomial are $\pm\sqrt{\alpha}$ and $\pm\sqrt{\beta}$ with $\alpha = \frac{-a + \sqrt{d}}{2}$, and

$\bar{\alpha} = \frac{-a - \sqrt{d}}{2}$. According to the assumption of nonnormality,

$$K = \mathbb{Q}(\sqrt{\alpha}) \neq \mathbb{Q}(\sqrt{\bar{\alpha}}), \text{ i. e., } \sqrt{\bar{\alpha}} \notin K.$$

The Galois group of K can be found by following Hungerford [6],

p. 273. The roots of the resolvent cubic of $f(x)$ are a , $2\sqrt{b}$, and $-2\sqrt{b}$.

Thus adjoining these roots to $\mathbb{Q}$ yields $\mathbb{Q}(\sqrt{b})$. Now $[\mathbb{Q}(\sqrt{b}):\mathbb{Q}] = 2$, oth-

erwise $\sqrt{b} = \sqrt{\alpha} \cdot \sqrt{\bar{\alpha}} = k$ for some $k \in \mathbb{Q} \Rightarrow \sqrt{\bar{\alpha}} = k/\sqrt{\alpha} \Rightarrow \sqrt{\bar{\alpha}} \in K$,

which contradicts the assumption of K 's nonnormality. By proposition

4.11 (iv) on p. 273 of Hungerford [6], the Galois group of $f(x)$ is either D_4

or Z_4 . Because $f(x)$ is nonnormal, the Galois group of $f(x)$ is D_4 . Hence

K 's Galois group is the dihedral group D_4 .

(3) $\Rightarrow$ (1): Because the Galois group of K is a permutation group

which acts on the roots θ_1 , θ_2 , θ_3 , and θ_4 of the quartic which generates

K and its conjugates, and, by assumption, this group is isomorphic to D_4 ,

K 's Galois group, G , can be written as

$\{e, (1234), (13)(24), (1432), (13), (14)(23), (24), (12)(34)\}$ after any nec-

essary renumbering of the roots. This group contains only two nontrivial

subgroups that fix any of the roots of K 's minimal polynomial: $\{e, (13)\}$,

which fixes the roots θ_2 and θ_4 ; and $\{e, (24)\}$, which fixes the roots θ_1 and

θ_3 . By letting K be $Q(\theta_1) = Q(\theta_3)$, the conjugate of K , K' , is then $Q(\theta_2) = Q(\theta_4)$. Clearly K is nonnormal. The corresponding subgroups of D_4 that fix K and K' are both subgroups of $H = \{e, (13), (24), (13)(24)\}$. The index of H in G is 2, so H 's fixed field N^H is a quadratic extension of Q .

Q. E. D.

The next thing to do is to show when two nonnormal biquadratic polynomials have roots which generate the same quartic extensions of Q . This will be accomplished by working with their coefficients. Let $\alpha^2 + a\alpha + b = \beta^2 + a'\beta + b' = 0$ where $Q(\sqrt{\alpha}) = Q(\sqrt{\beta})$. If $d = a^2 - 4b$, then $\alpha = \frac{-a \pm \sqrt{d}}{2}$, and $Q(\sqrt{d})$ is the unique quadratic subfield of $Q(\sqrt{\alpha})$. Now $Q(\sqrt{\alpha}) = Q(\sqrt{\beta})$ if and only if $\beta = \gamma^2\alpha$ for some γ in $Q(\sqrt{d})$. Being an element of $Q(\sqrt{d})$, γ can be written as $u + v\alpha$, with $u, v \in Q$, since $Q(\sqrt{d}) = Q(\alpha)$. Hence $\beta = (u + v\alpha)^2\alpha$.

To find a' and b' in terms of a, b, u , and v , the fact that $a' = -(\beta + \beta')$ and $b' = \beta\beta'$ yields $a' = au^2 + 2(2b - a^2)uv + (a^3 - 3ab)v^2$, and $b' = (u^2 - auv + v^2b)^2b$. Letting $w = u - av$, if $x^4 + ax^2 + b$ and

$x^4 + (aw^2 + 4bvw + abv^2)x^2 + b(w^2 + awv + bv^2)^2$ are nonnormal and irreducible, then they are equivalent. The following lemmas will help to determine when such polynomials are nonnormal and irreducible.

LEMMA: If $f(x) = x^4 + ax^2 + b$ (where a and b are in $\mathbb{Q}$) is irreducible over $\mathbb{Q}[X]$ and if $d = a^2 - 4b$, then $f(x)$ is normal if and only if either $\sqrt{b}$ or $\sqrt{\frac{d}{b}} \in \mathbb{Q}$.

Proof: If $f(x)$ is irreducible, then its roots produce a pair of quartic extensions $\mathbb{Q}(\sqrt{\alpha})$ and $\mathbb{Q}(\sqrt{\bar{\alpha}})$, with $\alpha = \frac{-a + \sqrt{d}}{2}$ and $\bar{\alpha} = \frac{-a - \sqrt{d}}{2}$, which both contain the quadratic subfield $\mathbb{Q}(\sqrt{d})$. By definition, $f(x)$ is normal if and only if $\mathbb{Q}(\sqrt{\alpha}) = \mathbb{Q}(\sqrt{\bar{\alpha}})$, which means that $\alpha = \gamma^2 \bar{\alpha}$ for some γ in $\mathbb{Q}(\sqrt{d})$. Starting with the assumption that $f(x)$ is normal leads to $b = (\gamma \bar{\alpha})^2$. So $\sqrt{b} \in \mathbb{Q}(\sqrt{d})$ if $f(x)$ is normal. If $\sqrt{b} \in \mathbb{Q}(\sqrt{d})$, then $(\sqrt{b})^2 = \alpha \bar{\alpha} = \lambda^2$ for some $\lambda \in \mathbb{Q}(\sqrt{d})$. It follows that $\alpha = \frac{\lambda^2}{\bar{\alpha}} \Rightarrow \sqrt{\alpha} \in \mathbb{Q}(\sqrt{\bar{\alpha}})$, i. e., $f(x)$ is normal. Thus $f(x)$ is normal $\iff \sqrt{b} \in \mathbb{Q}(\sqrt{d})$.

Now $\sqrt{b} \in \mathbb{Q}(\sqrt{d}) \iff \sqrt{b} = u + v\sqrt{d}$ for suitable $u, v \in \mathbb{Q}$. But $b \in \mathbb{Q} \Rightarrow$ either u or v is equal to 0. Checking these possible values of

u and v , $v = 0 \iff \sqrt{b} \in \mathbb{Q}$, and $u = 0 \iff \sqrt{\frac{d}{b}} \in \mathbb{Q}$. Thus

$f(x)$ is normal $\iff$ either $\sqrt{b}$ or $\sqrt{\frac{d}{b}}$ is in $\mathbb{Q}$.

Q. E. D.

LEMMA: If $f(x) = x^4 + ax^2 + b$, where $a, b \in \mathbb{Q}$, and if $d = a^2 - 4b$,

then $f(x)$ is irreducible and nonnormal if and only if

$\sqrt{b}$, $\sqrt{d}$, and $\sqrt{\frac{d}{b}}$ are irrational.

Proof: If $f(x)$ is irreducible, then $\sqrt{d} \notin \mathbb{Q}$. If $f(x)$ is nonnormal,

then $\sqrt{b}$, $\sqrt{\frac{d}{b}} \notin \mathbb{Q}$, according to the lemma above.

If $\sqrt{d} \notin \mathbb{Q}$, then $f(x)$ has no rational root, so the only way $f(x)$ could be reducible would be for $f(x)$ to be the product of two quadratic polynomials, $g(x)$ and $h(x)$, both in $\mathbb{Q}[X]$, which are both irreducible with respect to $\mathbb{Q}[X]$. Let $g(x) = x^2 + rx + s$, and $h(x) = x^2 + tx + u$, with $r, s, t, u \in \mathbb{Q}$. Under the additional assumption that $\sqrt{b} \notin \mathbb{Q}$, such a factorization of $f(x)$ is not possible. This can be seen as follows (by equating coefficients): $g(x) \cdot h(x) = f(x) \Rightarrow r + t = 0 = ru + st$, $su = b$, and $rt + s + u = a$. So $r = -t$, which implies $t(s - u) = 0$. Because $b = su$

is not a square in $\mathbb{Q}$, $s \neq u$. Hence $t = r = 0$. Thus $g(x) = x^2 + s$, and $h(x) = x^2 + u$, and $a = s + u \Rightarrow u = a - s$. Substituting this expression for u into the equation for b yields the following quadratic equation:

$$s^2 - as + b = 0.$$

The assumption that $\sqrt{d} = \sqrt{a^2 - 4b} \notin \mathbb{Q}$ implies that s and u are not rational, which contradicts the assumption that they were. It follows that $f(x)$ is irreducible with respect to $\mathbb{Q}[X]$. Finally, with the assumption that $\sqrt{\frac{d}{b}} \notin \mathbb{Q}$, $f(x)$ is nonnormal by the previous lemma.

Q. E. D.

To find the quartic subfields of a normal extension, N , of degree 8 over $\mathbb{Q}$ with Galois group D_4 , let $N = \mathbb{Q}(\sqrt{\alpha}, \sqrt{\bar{\alpha}})$ with $\sqrt{\alpha}$ and $\sqrt{\bar{\alpha}}$ roots of a biquadratic polynomial $f(x) = x^4 + ax^2 + b$. Index $\sqrt{\alpha}$, $\sqrt{\bar{\alpha}}$, $-\sqrt{\alpha}$, and $-\sqrt{\bar{\alpha}}$ with 1, 2, 3, and 4, respectively, and use the permutation representation of D_4 :

$\{e, (1234), (13)(24), (1432), (13), (14)(23), (24), (12)(34)\}$. The quartic subfields of N are fixed by the 5 subgroups of D_4 of order 2:

Subgroup generator	Fixed field
(13)	$\mathbb{Q}(\sqrt{\alpha})$
(24)	$\mathbb{Q}(\sqrt{\alpha})$
(12)(34)	$\mathbb{Q}(\sqrt{\alpha} + \sqrt{\alpha})$
(14)(23)	$\mathbb{Q}(\sqrt{\alpha} - \sqrt{\alpha})$
(13)(24)	$\mathbb{Q}(\alpha + \sqrt{\alpha\alpha} - \alpha)$

The normal quartic subfield of N is $\mathbb{Q}(\alpha + \sqrt{\alpha\alpha} - \alpha)$ because this subfield is $\mathbb{Q}(\sqrt{b} + \sqrt{d}) = \mathbb{Q}(\pm\sqrt{b} \pm \sqrt{d})$. The field $\mathbb{Q}(\pm\sqrt{b} \pm \sqrt{d})$ is generated by the roots of $g(x) = x^4 - 2(d+b)x^2 + (d-b)^2$, where $d = a^2 - 4b$. The polynomial $g(x)$ is irreducible over $\mathbb{Q}$, hence, by the lemmas, $g(x)$ is normal. The conjugate pair of nonnormal quartic fields generated by the roots of $f(x)$ are $\mathbb{Q}(\sqrt{\alpha})$ and $\mathbb{Q}(\sqrt{\alpha})$. Their relationship to the other pair of nonnormal quartics $\mathbb{Q}(\sqrt{\alpha} + \sqrt{\alpha})$ and $\mathbb{Q}(\sqrt{\alpha} - \sqrt{\alpha})$ can be seen by setting $\beta = (\sqrt{\alpha} + \sqrt{\alpha})^2 = -a + 2\sqrt{b}$, and $\bar{\beta} = (\sqrt{\alpha} - \sqrt{\alpha})^2 = -a - 2\sqrt{b}$. Now β and $\bar{\beta}$ are the nonzero roots of the resolvent cubic of $f(x)$, $x^3 + 2ax^2 + dx$.

The roots of $f(x)$ can be expressed in terms of β and $\bar{\beta}$ as follows:

$\frac{1}{2}(\pm\sqrt{\beta} \pm \sqrt{\bar{\beta}})$. This can be seen from the fact that $\sqrt{\alpha} + \sqrt{\alpha} = \sqrt{\beta}$, and

$\sqrt{\beta} + \sqrt{\bar{\beta}} = 2\sqrt{\alpha}$. Now the lattice of subfields of N looks like this:

From the relationship between α , $\bar{\alpha}$, β , and $\bar{\beta}$, the quartic fields in the diagram above could have been written as: $Q(\sqrt{\bar{\beta}})$, $Q(\sqrt{\beta})$, $Q(\beta + \sqrt{\beta\bar{\beta}} - \bar{\beta})$, $Q(\sqrt{\beta} - \sqrt{\bar{\beta}})$, and $Q(\sqrt{\beta} + \sqrt{\bar{\beta}})$, respectively. This demonstrates the duality between the two nonnormal towers leading to N : either may be generated by the square roots of the nonzero roots of the resolvent cubic of the other's biquadratic minimal polynomial. Now if $K = Q(\sqrt{\alpha})$, then its dual $K^* = Q(\sqrt{\bar{\beta}})$, and $K^{**} = K$. The two minimal polynomials for K and K^* , respectively, may be written as $f(x) = x^4 + ax^2 + b$, and $f^*(x) = x^4 + 2ax^2 + d$, which are not dual because

$f^{**} \neq f$ even though their roots generate the same extensions.

To tie in the above discussion with Shanks's "incredible identities" [11], note that the two polynomials $(x^4 - x^3 - 3x^2 + x + 1, \text{ and } x^4 - x^3 - 5x^2 - x + 1)$ which Shanks uses to construct his incredible identities are equivalent to nonnormal biquadratic polynomials whose roots generate dual quartic fields. Shanks's incredible identities become immediate consequences of $\sqrt{\alpha} + \sqrt{\bar{\alpha}} = \sqrt{\beta}$, and $\sqrt{\beta} + \sqrt{\bar{\beta}} = 2\sqrt{\alpha}$ when the two polynomials he has given are written in biquadratic form.

Shanks's incredible identity is that $A = B$ where

$$A = \sqrt{5} + \sqrt{22 + 2\sqrt{5}} \text{ and}$$

$$B = \sqrt{11 + 2\sqrt{29}} + \sqrt{16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}}}. \text{ To see why}$$

$$A = B, \text{ let } \alpha = \frac{11 + \sqrt{5}}{2}. \text{ Now } \alpha\text{'s minimal polynomial is } x^2 - 11x + 29,$$

and that for $\sqrt{\alpha}$ is $x^4 - 11x^2 + 29$. Hence $\mathbb{Q}(\sqrt{\alpha})$ is a quartic extension

of $\mathbb{Q}$. Notice that $2\sqrt{\alpha} = A - \sqrt{5}$; $\sqrt{5} = \frac{A^2 - 17}{2(1+A)}$; hence, $\mathbb{Q}(\sqrt{\alpha}) = \mathbb{Q}(A)$

because both are extensions of $\mathbb{Q}$ of degree 4 and $\mathbb{Q}(\sqrt{\alpha})$ is a subfield of

$\mathbb{Q}(A)$. This means that $\sqrt{\alpha}$'s minimal polynomial is equivalent to that of

$\frac{A+1}{4}$, $x^4 - x^3 - 3x^2 + x + 1$. Setting $\beta = 11 + 2\sqrt{29}$, from the above, if $\beta = (\sqrt{\alpha} + \sqrt{\bar{\alpha}})^2 = 11 + 2\sqrt{29}$, then $\sqrt{\beta} + \sqrt{\bar{\beta}} = 2\sqrt{\alpha}$, so $(\sqrt{\beta} + \sqrt{\bar{\beta}})^2 = 4\alpha$, i. e., $22 + 2\sqrt{5} = \{\sqrt{11 + 2\sqrt{29}} + \sqrt{11 - 2\sqrt{29}}\}^2$. So taking the square root of both sides of this equation yields

$$A - \sqrt{11 + 2\sqrt{29}} = \sqrt{5} + \sqrt{11 - 2\sqrt{29}} = \sqrt{16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}}},$$

from which it follows that $A = B$.

Now the lattice diagram for the dual field to that of $\mathbb{Q}(A)$ is:

The last thing left to show is that the second of the two quartics

Shanks has given, $x^4 - x^3 - 5x^2 - x + 1$, is equivalent to the minimal poly-

nomial of the dual fields, i. e., $f^*(x) = x^4 - 22x^2 + 5$. Ferrari's method

will be used. The resolvent cubic of $f(x) = x^4 - x^3 - 5x^2 - x + 1$ is:

$$y^3 + 5y^2 - 3y - 22 = (y - 2)(y - \frac{-7 + \sqrt{5}}{2})(y - \frac{-7 - \sqrt{5}}{2}).$$

When any root y of this resolvent cubic is chosen, it can be substituted into the equivalent formulation of $f(x)$ as

$$f(x) = (x^2 - x/2 + y/2)^2 - (\lambda x + \mu)^2, \text{ in order to find } \lambda \text{ and } \mu \text{ so that } f(x)$$

may be treated as the product of two quadratics.

Choosing $y = 2$ makes $\mu = 0$, and $|\lambda| = \frac{\sqrt{29}}{2}$, so that the largest root of $f(x)$ is $\frac{C+1}{4}$ where $C = \sqrt{29} + \sqrt{14 + 2\sqrt{29}}$.

Choosing $y = \frac{-7 - \sqrt{5}}{2}$ makes $|\lambda| = \frac{\sqrt{7 - 2\sqrt{5}}}{2}$, and

$|\mu| = \frac{1}{2} \sqrt{\frac{19 + 7\sqrt{5}}{2}} = \frac{3 + \sqrt{5}}{4} \sqrt{7 - 2\sqrt{5}}$, so that C can also be expressed as:

$$\sqrt{7 - 2\sqrt{5}} + \sqrt{36 + 2\sqrt{5} + 2\sqrt{7 - 2\sqrt{5}} + 8\sqrt{\frac{19 + 7\sqrt{5}}{2}}} =$$

$\sqrt{29} + \sqrt{7 + 2\sqrt{5}} + \sqrt{7 - 2\sqrt{5}}$. From the first expression of C ,

$Q(C) = Q(\sqrt{14 + 2\sqrt{29}})$. Now because $14 + 2\sqrt{29} = (5 + \sqrt{29})(11 - 2\sqrt{29})$,

$Q(C)$ is conjugate to $Q(\sqrt{11 + 2\sqrt{29}})$.

CHAPTER 2

A Solution to $abc = a + b + c = 1$ in

a Cyclic Cubic Rational Extension

In this chapter a solution to the equations $abc = a + b + c = 1$ in a cyclic cubic extension of the rational numbers will be shown to exist. The question of the existence of such a solution is due to Hugh Edgar. This proof of the existence of a solution comes from some notes of Andrew Bremner and Patrick Morton. The following are the main results of this chapter:

(1) the only integer d that makes the roots of $x^3 - x^2 + dx - 1$ provide a solution to $abc = a + b + c = 1$ in a cyclic cubic rational extension is $d = -4$;

(2) $(-4, 13)$ and $(-4, -13)$ are the only integral points on the curve $Y^2 = -4X^3 + X^2 + 18X - 31$;

(3) $(16, 52)$ and $(16, -52)$ are the only integral points on the curve $Y^2 = X^3 + X^2 - 72X - 496$.

Assume that a, b , and c are the distinct roots of a cubic polynomial

$f(x) = (x - a)(x - b)(x - c) = x^3 - x^2 + dx - 1$, where $d \in \mathbb{Z}$. Assuming this polynomial to be irreducible over $\mathbb{Q}[x]$, it will be necessary to determine the Galois group of the splitting field of $f(x)$. By corollary 4.7 on p. 271 of Hungerford [6], this Galois group is either A_3 , or S_3 , and, the discriminant of $f(x)$ is the square of an element of $\mathbb{Q}$ if and only if the Galois group is A_3 .

To find the discriminant of $f(x)$, let

$g(x) = f(x + \frac{1}{3}) = x^3 + \frac{3d-1}{3}x + \frac{9d-2}{27}$. By proposition 4.8 on p. 271 of Hungerford [6], the discriminant of $f(x)$ is

$\Delta^2 = -4(d - \frac{1}{3})^3 - 27(\frac{9d-2}{27})^2 = -4d^3 + d^2 + 18d - 31$. By substituting y for Δ and letting $Y = 4y$ and $X = -4d$, the expression for the discriminant becomes $Y^2 = X^3 + X^2 - 72X - 496$.

If there exist X and Y , both rational integers, such that X and Y satisfy the latter equation of the discriminant of $f(x)$, then the Galois group is A_3 for the $f(x)$ that comes from these X and Y . What is needed is to find out if there are such X and Y .

By the rational root theorem, the polynomial

$h(X) = X^3 + X^2 - 72X - 496$ is irreducible over $\mathbb{Q}$; hence, if

$h(\theta) = 0$, then $\partial_Q \theta = 3$. Also, $h(X)$ has only one real root because the relative maximum is less than zero; hence, by the Dirichlet unit theorem, the rank of the unit group of the splitting field of $h(X)$ is 1.

Assuming θ to be a root of $h(X)$, let $\alpha = \frac{\theta^2 - 35\theta - 60}{208}$ in order to obtain a power-integral basis for $\mathbb{Q}(\theta)$. The equation $\alpha^3 - \alpha + 2 = 0$ is satisfied by α because

$$\alpha^3 - \alpha + 2 = \frac{(\theta^3 + \theta^2 - 72\theta - 496)(\theta^3 - 106\theta^2 + 3673\theta - 41084)}{208^3}.$$

In fact $\theta = \alpha^2 - 6\alpha - 1$, which implies $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$. The norm of the ideal generated by $X - \theta$ is $N((X - \theta)) = Y^2$. According to Delone and Faddeev [4] the ring of algebraic integers of $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ is a unique factorization domain. So finding a prime factorization of Y^2 will aid the search for rational X and Y that satisfy the latter equation for the discriminant of $f(x)$.

By factoring out an $X - \theta$ from $h(X)$, the following factorization of Y^2 can be obtained: $Y^2 = (X - \theta)[X^2 + (\theta + 1)X + (\theta^2 + \theta - 72)]$. To check if $X - \theta$ and $X^2 + (\theta + 1)X + (\theta^2 + \theta - 72)$ have any common divisors, $\gcd(X - \theta, X^2 + (\theta + 1)X + (\theta^2 + \theta - 72))$ must be examined. But

$\gcd(X - \theta, 3\theta^2 + 2\theta - 72)$ can be examined instead because

$$X^2 + (\theta + 1)X + (\theta^2 + \theta - 72) = (X - \theta)[X + (2\theta + 1)] + 3\theta^2 + 2\theta - 72 \text{ and}$$

$$3\theta^2 + 2\theta - 72 = [X^2 + (\theta + 1)X + (\theta^2 + \theta - 72)] - (X - \theta)^2 - (X - \theta)(3\theta + 1).$$

The latter greatest common divisor will be examined in terms of α .

Letting $\wp_2 = (\alpha + 1)$, $\wp'_2 = (\alpha)$, $\wp_{13} = (1 - 2\alpha + 2\alpha^2)$, and

$\wp'_{13} = (-3 + 4\alpha + 4\alpha^2)$ be ideals in the ring of integers of $\mathbb{Q}(\alpha)$, an expression for the ideal generated by $3\theta^2 + 2\theta - 72$ in terms of ideals in the ring of integers of $\mathbb{Q}(\alpha)$ can be obtained. This expression is

$$(3\theta^2 + 2\theta - 72) = \wp_2^{11} \cdot \wp_{13}^2 \text{—in fact } (2) = \wp_2^2 \cdot \wp'_2 \text{ and } (13) = \wp_{13}^2 \cdot \wp'_{13}, \text{ which}$$

shows that $\wp_2, \wp'_2, \wp_{13}$, and $\wp'_{13}$ are prime. Now all that remains is to find the ideal generated by $\gcd(X - \theta, 3\theta^2 + 2\theta - 72)$ in terms of these prime ideals in the ring of integers of $\mathbb{Q}(\alpha)$.

To find the ideal that is equal to $(X - \theta, 3\theta^2 + 2\theta - 72)$, the ideal

$(X - \theta)$ can be factored as a product of prime ideals: $(X - \theta) = \delta \vartheta^2$, and

the ideal $(3\theta^2 + 2\theta - 72)$ can be factored as $(3\theta^2 + 2\theta - 72) = \delta \zeta^2$, where δ

is a squarefree common divisor of $(X - \theta)$ and $(3\theta^2 + 2\theta - 72)$. But

$Y^2 = \text{Norm}(X - \theta) = \text{Norm}(\delta) \cdot \text{Norm}(\vartheta^2)$, so $\text{Norm}(\delta) = 1$, which implies

that, without loss of generality, $\delta = (1)$. Thus, $X - \theta = \pm\epsilon^i(a + b\alpha + c\alpha^2)^2$,

where ϵ is the fundamental unit (by Delone and Faddeev [4],

$\epsilon = 1 - \alpha - \alpha^2$), $i = 0$ or 1 , and $a, b, c \in \mathbb{Z}$. Taking note that

$\alpha \approx -1.5213797068$, $\epsilon \approx 0.20678349454 \geq 0$. If θ is the real root of

$h(X) = X^3 + X^2 - 72X - 496$, then θ is greater than 0 because

$h(0) = -496$, and

$$\lim_{x \rightarrow +\infty} h(x) = +\infty.$$

If $X \leq \theta$, then $Y^2 \leq 0$, which is a contradiction. Therefore $X \geq \theta$, and

$(X - \theta) = \epsilon^i(a + b\alpha + c\alpha^2)^2$. There are now only two cases ($i = 0$ and $i = 1$)

which must be examined to determine which yields an expression for the

ideal $(X - \theta)$.

Case 1 ($i = 0$):

Solving for a, b , and c ,

$$X - \theta = (a + b\alpha + c\alpha^2)^2 = a^2 + 2ab\alpha + (2ac + b^2)\alpha^2 + 2bc\alpha^3 + c^2\alpha^4.$$

Now, $\alpha^3 = \alpha - 2 \Rightarrow \alpha^4 = \alpha^2 - 2\alpha$, so, by substitution,

$$\begin{aligned} X - \theta &= a^2 + 2ab\alpha + (2ac + b^2)\alpha^2 + 2bc(\alpha - 2) + c^2(\alpha^2 - 2\alpha) \\ &= (a^2 - 4bc) + (2ab + 2bc - 2c^2)\alpha + (2ac + b^2 + c^2)\alpha^2. \end{aligned}$$

Recalling that $\theta = \alpha^2 - 6\alpha - 1$,

$X - \theta = X - (\alpha^2 - 6\alpha - 1) = (X + 1) + 6\alpha - \alpha^2$, which yields the following three identities:

1. $X + 1 = a^2 - 4bc$,
2. $6 = 2ab + 2bc - 2c^2 \Rightarrow 3 = ab + bc - c^2$, and
3. $-1 = 2ac + b^2 + c^2$.

Taking $\frac{1}{2}(2.) + 3(3.)$ yields $0 = ab + bc + 2c^2 + 6ac + 3b^2$, or

$0 = (b + 6c)(a + 3b - 17c) + 104c^2$. Hence,

$(b + 6c)(a + 3b - 17c) = -104c^2$. If $b \equiv 1 \pmod{2}$, then, taking

$\frac{1}{2}(2.) \pmod{2}$ gives $1 \equiv a + c - c^2 \pmod{2}$, which implies that

$a \equiv 1 \pmod{2}$. Continuing with this procedure, $(3.) \pmod{2}$

becomes $1 \equiv 1 + c^2 \pmod{2}$, which implies that $c \equiv 0 \pmod{2}$.

Now, looking at $(3.) \pmod{4}$, $-1 \equiv 2ac + b^2 + c^2 \pmod{4}$ implies

that $b^2 \equiv -1 \pmod{4}$, which is impossible. Thus $b \not\equiv 1 \pmod{2}$.

Trying $b \equiv 0 \pmod{2}$ and looking at $(3.) \pmod{2}$, leads to

$c \equiv 1 \pmod{2}$. Taking $(3.) \pmod{4}$, $-1 \equiv 0 + 2ac + c^2 \pmod{4}$,

or $-2 \equiv 2ac \pmod{4}$, which implies that $-1 \equiv ac \pmod{2}$.

Thus, $a \equiv 1 \pmod{2}$.

Having so far established that $a, c \equiv 1 \pmod{2}$, and $b \equiv 0 \pmod{2}$, the next thing to do is to try to find specific integer values of a, b , and c . This will be accomplished by working with the equation $(b + 6c)(a + 3b - 17c) = -104c^2$. Taking a look at $\gcd(b + 6c, a + 3b - 17c, c)$, in particular, $\gcd(b + 6c, c)$, the fact that $b + 6c - 6c = b$ implies that $\gcd(b + 6c, c) \mid b$. Letting $G = \gcd(b + 6c, c)$ and returning to equation (3.), $G \mid -1 = 2ac + b^2 + c^2$, so $G = 1$. This means that $\gcd(b + 6c, a + 3b - 17c, c) = 1$.

Let $b + 6c = 2um^2$, $a + 3b - 17c = \frac{-52}{u}n^2$, and $c = mn$ for $m, n, u \in \mathbb{Z}$, with $\gcd(m, n) = 1$, and $u \mid 52$. By substitution, $\gcd(b + 6c, c) = \gcd(2um^2, mn) = 1$, so $m \mid 1$, which implies that $m = \pm 1$. It may be assumed, however, that $m = 1$ because the object of concern is $-104c^2 = -104(mn)^2$, which has an m^2 factor, so m 's sign does not matter. Taking note that $c = mn$, $b = 2um^2 - 6mn$, and $a = 35mn - 6um^2 - \frac{52}{u}n^2$,

the equation $-1 = b^2 + 2ac + c^2$ becomes

$$-1 = 4u^2 - 36un + 107n^2 - \frac{104}{u}n^3, \text{ or}$$

$$0 = (4u^2 + 1) - 36un + 107n^2 - \frac{104}{u}n^3.$$

Recalling that $u|52$, there are 12 possible values of u that need to be checked to find out if any yield an integral value for n that, together with the corresponding u value, satisfies the above equation.

$$u = 1 \Rightarrow -1 = 4 - 36n + 107n^2 - 104n^3 \Rightarrow$$

$$104n^3 - 107n^2 + 36n - 5 = 0 \Rightarrow n|5, \text{ but none of } n = \pm 1, \text{ or } \pm 5$$

works $\Rightarrow \Leftarrow$

$$u = -1 \Rightarrow -1 = 4 + 36n + 107n^2 + 104n^3 \Rightarrow n|5, \text{ but none of}$$

$n = \pm 1, \text{ or } \pm 5$ works $\Rightarrow \Leftarrow$

$$u = 2 \Rightarrow -1 = 16 - 72n + 107n^2 - 52n^3 \Rightarrow n|17 \Rightarrow$$

$n = \pm 1$ or, ± 17 . Out of these only $n = 1$ works. This case,

where $u = 2$ and $n = 1$, will be examined below.

$$u = -2 \Rightarrow -1 = 16 + 72n + 107n^2 + 52n^3 \Rightarrow n|17. \text{ Out of}$$

the four possible values of n , only $n = -1$ works. This case,

where $u = -2$ and $n = -1$ will be examined below.

$u = 4 \Rightarrow -1 = 64 - 144n + 107n^2 - 26n^3 \Rightarrow n|65$, but none
of $n = \pm 1, \pm 5, \pm 13$, or ± 65 works $\Rightarrow \Leftarrow$

$u = -4 \Rightarrow -1 = 64 + 144n + 107n^2 + 26n^3 \Rightarrow n|65$, but none
of $n = \pm 1, \pm 5, \pm 13$, or ± 65 works $\Rightarrow \Leftarrow$

$u = 13 \Rightarrow -1 = 676 - 468n + 107n^2 - 8n^3 \Rightarrow n|677$, but
none of $n = \pm 1$, or ± 677 works $\Rightarrow \Leftarrow$

$u = -13 \Rightarrow -1 = 676 + 468n + 107n^2 + 8n^3 \Rightarrow n|677$, but
none of $n = \pm 1$, or ± 677 works $\Rightarrow \Leftarrow$

$u = 26 \Rightarrow -1 = 2704 - 936n + 107n^2 - 4n^3 \Rightarrow n|2705$, but
none of $n = \pm 1, \pm 5, \pm 541$, or ± 2705 works $\Rightarrow \Leftarrow$

$u = -26 \Rightarrow -1 = 2704 + 936n + 107n^2 + 4n^3 \Rightarrow n|2705$, but
none of $n = \pm 1, \pm 5, \pm 541$, or ± 2705 works $\Rightarrow \Leftarrow$

$u = 52 \Rightarrow -1 = 10816 - 1872n + 107n^2 - 2n^3 \Rightarrow n|10817$,
but none of $n = \pm 1, \pm 29, \pm 373$, or ± 10817 works $\Rightarrow \Leftarrow$

$u = -52 \Rightarrow -1 = 10816 + 1872n + 107n^2 + 2n^3 \Rightarrow n|10817$,
but none of $n = \pm 1, \pm 29, \pm 373$, or ± 10817 works $\Rightarrow \Leftarrow$

Out of all 12 possible u values only two worked. These

two values will now be used to compute values for a, b , and c .

Recalling that $m = 1$, when $u = 2, n = 1$, and these values of

u, m , and n make $a = -3, b = -2$, and $c = 1$. Likewise, when

$u = -2, n = -1$, and a, b , and c become $3, 2$, and -1 ,

respectively. Thus $(a, b, c) = \pm(3, 2, -1)$, and, going back to

equation (1.), $X + 1 = a^2 - 4bc = 9 + 8$. Hence $X = 16$.

Substituting this value for X into the latter equation for

the discriminant of $f(x)$, $Y^2 = X^3 + X^2 - 72X - 496$, yields

$Y = \pm 52$. Now, returning to the former equation for the

discriminant of $f(x)$, $\Delta^2 = -4d^3 + d^2 + 18d - 31$, there are

two integral values for Δ and d that satisfy this equation.

These values are $\Delta = \pm 13, d = -4$.

Case 2 ($i = 1$):

Now $X - \theta = \epsilon(a + b\alpha + c\alpha^2)^2$, where $\epsilon = 1 - \alpha - \alpha^2$,

$\theta = \alpha^2 - 6\alpha - 1$, and

$$(a + b\alpha + c\alpha^2)^2 = (a^2 - 4bc) + 2(ab + bc - c^2)\alpha + (2ac + b^2 + c^2)\alpha^2.$$

By substituting for ϵ, θ , and $(a + b\alpha + c\alpha^2)^2$, and using the fact

that $\alpha^3 - \alpha + 2 = 0$, the following three identities are

obtained:

1. $X + 1 = a^2 + 2b^2 - 2c^2 + 4ac + 4ab$,
2. $6 = c^2 - a^2 + 4bc + b^2 + 2ac$, and
3. $-1 = 2c^2 - 2ab + 2bc - a^2$.

Working modulo 2, equation (2.) becomes

$$0 \equiv a + b + c \pmod{2}, \text{ equation (3.) becomes } 1 \equiv a \pmod{2},$$

and these two equations imply that $b \equiv c + 1 \pmod{2}$.

Working modulo 4, equation (2.) becomes

$$2 \equiv c^2 - a^2 + b^2 + 2ac \pmod{4}, \text{ and, using the previously}$$

obtained information about a and b , this congruence

$$\text{becomes } 2 \equiv 2c^2 \pmod{4}. \text{ Looking at equation (3.) modulo 4,}$$

$$-1 \equiv 2 - 2ab + 2bc - 1 \pmod{4}. \text{ Using the facts that}$$

$$-2ab \equiv -2(c + 1) \pmod{4}, \text{ and } 2b \equiv 2(c + 1) \pmod{4},$$

$$\text{equation (3.) becomes } -2 \equiv -2(c + 1) + 2(c + 1)c \pmod{4}, \text{ or}$$

$$0 \equiv 2c^2 \pmod{4}, \text{ which contradicts the fact that}$$

$$2 \equiv 2c^2 \pmod{4}. \text{ Hence } i \neq 1.$$

The examination of the two cases of values for i has shown that the only integral solutions to the equation of the discriminant of $f(x)$,

$\Delta^2 = -4d^3 + d^2 + 18d - 31$, are $d = -4, \Delta = \pm 13$. This means that the cubic $f(x) = x^3 - x^2 - 4x - 1$ has A_3 as its Galois group, and the roots of this cubic provide a solution to the equations $abc = a + b + c = 1$.

CHAPTER 3

Unit Solutions to $\alpha + \beta + \gamma = \alpha\beta\gamma$ in Rings of Integers of Low-Degree Rational Extensions

In this chapter the existence of solutions to the equation $u_1 + u_2 + u_3 = u_1u_2u_3$, where u_1, u_2 , and u_3 are units in some rings of integers of low-degree (i. e., of degree less than or equal to 4) extensions of the rational numbers, will be demonstrated. The problem of finding solutions to the equation $xyz = x + y + z = 1$ was originally tackled by Cassels [3], who, using the theory of elliptic curves, showed that no solutions exist when x, y , and z are rational. A year later, in 1961, Sierpinski ([12] and [13]) presented an elementary argument that the equation $xyz = x + y + z = 1$ has no rational solutions. Then, in 1987, Mollin, Small, Varadarajan, and Walsh [9] proved that there are only three quadratic extensions of the rational numbers that have unit solutions to the equation $xyz = x + y + z$ in their rings of integers. These extensions are $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{5})$. A proof of Mollin, Small, Varadarajan, and Walsh's theorem will appear below. The information contained in this chapter

comes from three unpublished papers co-authored by Liang-Cheng Zhang, Jonathan Gordon, and Hugh Edgar ([16], [17], and [5]). Throughout this chapter, K is assumed to be a real number field with unit group U_K having rank 1. The following theorem is the main result of the first paper [16]:

THEOREM: Let K be a real number field with unit group U_K having rank 1. If the fundamental unit, η , is greater than 3, then the equation $u_1 + u_2 + u_3 = u_1 u_2 u_3$ has no solutions in U_K .

Proof:

Let $u_i = \pm \eta^{l_i}$, with $l_i \in \mathbb{Z}$, for $i = 1, 2$, and 3 , be a solution to $u_1 + u_2 + u_3 = u_1 u_2 u_3 = u$, and assume also that $u > 0$. Then at least one $u_i > 0$, so assume $u_1 \geq u_2 \geq u_3$ with $u_1 > 0$.

Consequently, one of the following statements holds:

$$1. \ u_1 \geq u_2 \geq u_3 > 0 \Rightarrow \eta^{l_1} + \eta^{l_2} + \eta^{l_3} = \eta^{l_1} \eta^{l_2} \eta^{l_3} = \eta^{l_1+l_2+l_3}; \text{ or}$$

$$2. \ u_1 \geq 0, u_2, u_3 < 0 \Rightarrow u_2 = -\eta^{l_2}, u_3 = -\eta^{l_3} \Rightarrow$$

$$\eta^{l_1} - \eta^{l_2} - \eta^{l_3} = \eta^{l_1} \eta^{l_2} \eta^{l_3} = \eta^{l_1+l_2+l_3}.$$

Each of the two statements will be considered separately.

(1.) This statement, together with the assumption that

$\eta > 3$, implies that $l_1 \geq l_2 \geq l_3$. Now either $l_2 + l_3 \geq 1$, or

$l_2 + l_3 \leq 0$. If $l_2 + l_3 \geq 1$, then

$$\eta^{l_1+l_2+l_3} = \eta^{l_1} \eta^{l_2+l_3} \geq \eta^{l_1} \eta^1 > 3\eta^{l_1} \geq \eta^{l_1} + \eta^{l_2} + \eta^{l_3} \Rightarrow \Leftarrow$$

If $l_2 + l_3 \leq 0$, then $\eta^{l_2+l_3} \leq 1 \Rightarrow$

$$\eta^{l_1+l_2+l_3} = \eta^{l_1} \eta^{l_2+l_3} \leq \eta^{l_1} < \eta^{l_1} + \eta^{l_2} + \eta^{l_3} \Rightarrow \Leftarrow$$

So (1.) is impossible.

(2.) If $l_2 + l_3 \geq 0$, then $\eta^{l_2+l_3} \geq 1 \Rightarrow$

$$\eta^{l_1+l_2+l_3} = \eta^{l_1} \eta^{l_2+l_3} \geq \eta^{l_1} > \eta^{l_1} - \eta^{l_2} - \eta^{l_3} \Rightarrow \Leftarrow$$

If $l_2 + l_3 < 0$, then $\eta^{l_2+l_3} \leq \frac{1}{\eta} \Rightarrow$

$$\eta^{l_1+l_2+l_3} = \eta^{l_1} \eta^{l_2+l_3} \leq \frac{1}{\eta} \eta^{l_1} < \frac{1}{3} \eta^{l_1}. \text{ Notice that } l_3 < l_1 \text{ because}$$

$$l_1 \leq l_3 \Rightarrow \eta^{l_1} - \eta^{l_3} \leq 0 \Rightarrow \eta^{l_1} - \eta^{l_2} - \eta^{l_3} \leq -\eta^{l_2} < 0, \text{ which is}$$

impossible since $u > 0$. So $l_3 \leq l_1 - 1$.

A similar argument shows that $l_2 < l_1$ and hence $l_2 \leq l_1 - 1$.

So both $l_3 - l_1$ and $l_2 - l_1$ are less than or equal to -1 .

Now, $\eta^{l_2} = \eta^{l_1} \eta^{l_2-l_1} \leq \eta^{l_1} \frac{1}{\eta} < \frac{1}{3} \eta^{l_1}$, and

$\eta^{l_3} = \eta^{l_1} \eta^{l_3-l_1} \leq \eta^{l_1} \frac{1}{\eta} < \frac{1}{3} \eta^{l_1}$. Then

$$\eta^{l_2+l_3} < \frac{2}{3}\eta^{l_1} \Rightarrow \eta^{l_1} - (\eta^{l_2} + \eta^{l_3}) > \eta^{l_1} - \frac{2}{3}\eta^{l_1} = \frac{1}{3}\eta^{l_1}.$$

$$\text{So } \eta^{l_1+l_2+l_3} < \frac{1}{3}\eta^{l_1} < \eta^{l_1} - \eta^{l_2} - \eta^{l_3} \Rightarrow \Leftarrow$$

Thus (2.) is impossible.

Because both (1.) and (2.) are impossible, the equation

$u_1 + u_2 + u_3 = u_1 u_2 u_3$ has no solutions based on the

hypotheses of this theorem.

Q. E. D.

Corollary: Let $K = \mathbb{Q}(\sqrt[3]{m})$ be a pure cubic field, and U_K be the group of units in the ring of algebraic integers of K . Then $\exists$ no solution to $u_1 + u_2 + u_3 = u_1 u_2 u_3$ in U_K .

Proof:

Setting $m = ab^2$, with a and b positive squarefree integers such that $(a, b) = 1$, then, by definition, $K = \mathbb{Q}(\sqrt[3]{ab^2})$ is a pure cubic field. There is no loss in generality in assuming that $a > b$ because $\mathbb{Q}(\sqrt[3]{ab^2}) = \mathbb{Q}(\sqrt[3]{a^2b})$.

If η is a unit, then so are $-\eta$ and $\frac{1}{\eta}$; hence, the

fundamental unit η can be assumed to be greater than 1.

The following lemma will show that, under the

hypotheses of this corollary, $\eta > 1$ implies that $\eta > 3$.

Lemma: Given the hypotheses of the corollary above, $\eta > 1 \Rightarrow \eta > 3$.

Proof (of the lemma):

Taking a look at the discriminant of K , d_K , there are two possibilities:

1. $d_K = -27a^2b^2$ if $ab^2 \not\equiv \pm 1 \pmod{9}$, or
2. $d_K = -3a^2b^2$ if $ab^2 \equiv \pm 1 \pmod{9}$.

By Artin's lower bound on the discriminant d_K ,

on p. 170 of Artin [1], $4\eta^3 + 24 > |d_K|$. In the case of the first

possibility for d_K , if $ab \geq 3$, then $|d_K| > 132 \Rightarrow \eta > 3$. For

$ab^2 = 2$, or $\mathbb{Q}(\sqrt[3]{2})$, the fundamental unit is

$\eta = 1 + \sqrt[3]{2} + \sqrt[3]{4} > 3$. Hence, $\eta > 3$ if $d_K = -27a^2b^2$. In the

case of the second possibility for d_K ,

$ab \geq 7 \Rightarrow |d_K| > 132 \Rightarrow \eta > 3$.

Q. E. D. (Lemma)

Returning to the proof of the corollary, the lemma

shows that $\eta > 3$. Therefore, the equation

$u_1 + u_2 + u_3 = u_1 u_2 u_3$ has no solutions in U_K .

Q. E. D. (Corollary)

Now the case of K being a quadratic extension of the rational numbers will be dealt with. The following lemma will be used to prove the second corollary to the theorem above:

Lemma: Let $K = \mathbb{Q}(\sqrt{d})$ with d a squarefree element of $\mathbb{Z}$, $d > 1$ and $d \neq 2, \text{ or } 5$. If $\eta > 1$ is the fundamental unit of K , then $\eta > 3$.

Proof:

Let $\eta = a + b\sqrt{d} > 1$ and $\eta' = a - b\sqrt{d}$ for $a, b \in \frac{1}{2}\mathbb{Z}$. It follows that $\eta\eta' = N(\eta) = \pm 1$, and $|\eta'| = \frac{1}{\eta} < 1$. By definition of η and η' , $a = \frac{1}{2}(\eta + \eta') > 0$, and $b = \frac{1}{2\sqrt{d}}(\eta - \eta') > 0$. By examining $d \pmod{4}$, two cases will be considered:

1. $d \not\equiv 1 \pmod{4}$, and
2. $d \equiv 1 \pmod{4}$.

In the first case, except when $d = 3$, $a + b\sqrt{d} \geq 1 + \sqrt{6} > 3$.

When $d = 3$, $\eta = 2 + \sqrt{3} > 3$ is the fundamental unit greater than 1. In the second case, $d \geq 13$ and $a, b \geq \frac{1}{2}$. Also,

$$\eta + \frac{1}{\eta} \geq \eta - \eta' = 2b\sqrt{d} \geq \sqrt{d}, \text{ which implies } \eta^2 + 1 \geq \sqrt{d}\eta,$$

or $\eta^2 - \sqrt{d}\eta + 1 \geq 0$. The unit, η , cannot be smaller than

the largest root of this quadratic, so

$$\eta \geq \frac{\sqrt{d} + \sqrt{d-4}}{2} \geq \frac{\sqrt{13} + 3}{2} > 3.$$

Q. E. D.

Corollary (Mollin, et. al. [9]): Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer, and let U_K denote the group of units in the ring of integers of K . There exist solutions in U_K to $u_1 + u_2 + u_3 = u_1u_2u_3$ if and only if $d = -1, 2$, or 5 .

Proof:

For $d > 1$, and $d \neq 2$, or 5 , the preceding lemma, taken together with the theorem, shows that there are no solutions to $u_1 + u_2 + u_3 = u_1u_2u_3$ in U_K .

For $d = -1$, $u_1 = 1$, $u_2 = i$, and $u_3 = -i$ is a solution.

For $d = 2$, $u_1 = 1 + \sqrt{2}$, $u_2 = 1 - \sqrt{2}$, and $u_3 = -1$ is a solution.

For $d = 5$, $u_1 = \frac{1+\sqrt{5}}{2}$, $u_2 = 2 + \sqrt{5}$, and $u_3 = 1$ is a solution.

For $d < -3$ there is no solution to $u_1 + u_2 + u_3 = u_1u_2u_3$ since

$U_K = \{\pm 1\}$. Finally, for $d = -3$, $U_K = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$,

where $\zeta = \frac{1+i\sqrt{3}}{2}$. Note that if $|u_1 + u_2 + u_3| = 1, |u_n| = 1$ for

$n = 1, 2$, or 3 , and $u_n \in U_K$, then $\exists 1 \leq i < j \leq 3 \ni u_i + u_j = 0$.

This fact can be observed on unit circles as follows:

Nondegenerate case:

Degenerate case:

Hence, $1 = |\zeta^{l_1+l_2+l_3}| = |\zeta^{l_1} + \zeta^{l_2} + \zeta^{l_3}|$ and $|\zeta^{l_i}| = 1$ for

$i = 1, 2$, or 3 . Without loss of generality, assume

$\zeta^{l_2} = -\zeta^{l_1}$. Then $\zeta^{l_3} = \zeta^{l_1} + \zeta^{l_2} + \zeta^{l_3} =$

$$\zeta^{l_1+l_2+l_3} = -\zeta^{2l_1+l_3} \Rightarrow (\zeta^{l_1})^2 = -1 \iff \zeta^{l_1} = \pm i \Rightarrow$$

Q. E. D.

Now the question of the existence of solutions to

$u_1 + u_2 + u_3 = u_1 u_2 u_3$, where the u_i are units in the rings of integers of mixed cubic extensions of $\mathbb{Q}$, will be answered. A mixed extension K of $\mathbb{Q}$ is one for which $r_1 r_2 > 0$. The following theorem shows that solutions exist for only two real mixed extensions of $\mathbb{Q}$.

THEOREM: Let K be a mixed cubic extension of $\mathbb{Q}$. Then there exist no real solutions to $u_1 + u_2 + u_3 = u_1 u_2 u_3$ in U_K except for the following 2 fields:

$K_1 = \mathbb{Q}(\eta_1)$, where $\text{Irr}(\eta_1, \mathbb{Q}, x) = x^3 - x^2 - x - 1$, and

$K_2 = \mathbb{Q}(\eta_2)$, where $\text{Irr}(\eta_2, \mathbb{Q}, x) = x^3 - x - 1$ and both

$\eta_1, \eta_2 \in \mathbb{R}$.

Proof:

The fact that K is a mixed extension of $\mathbb{Q}$, and $[K:\mathbb{Q}] = 3$

implies that $0 < r_1 < 3$, so $r_1 = 1$, or 2 . If $r_1 = 2$, then

$r_1 + 2r_2 = 3 \Rightarrow r_2 = \frac{1}{2}$, which is impossible. So $r_1 = 1$ and

$r_2 = 1$. By the Dirichlet unit theorem,

$r = r_1 + r_2 - 1 = 1 = \text{the rank of } U_K$. So let η be the

fundamental unit such that $\eta > 1$.

The following argument shows that $K = Q(\eta)$:

$$\eta \in K/Q \text{ \& } [K:Q] = 3 \Rightarrow Q(\eta) \subseteq K. \partial_Q(\eta) = 1 \Rightarrow \eta = \pm 1,$$

which contradicts $\eta > 1$, so

$$\partial_Q(\eta) = 3 \Rightarrow [Q(\eta):Q] = 3 = [K:Q], \text{ hence } Q(\eta) = K.$$

Now, let $f(x) = \text{Irr}(\eta, Q, x)$. By proposition 1 on p. 60 of

Samuel [10], η is a unit $\iff N(\eta) = \pm 1$. Actually $N(\eta) = \eta\eta'\eta'' = 1$

because $\eta > 1$ and η 's conjugates η' and η'' are complex

conjugates of each other. So, if $f(x) = x^3 + ax^2 + bx - 1$,

with $a, b \in \mathbb{Z}$, and if U_K contains a solution to

$u_1 + u_2 + u_3 = u_1 u_2 u_3$, then w. l. o. g., either

$$1. \eta^{l_1+l_2+l_3} = \eta^{l_1} + \eta^{l_2} + \eta^{l_3}, \text{ or}$$

$$2. \eta^{l_1+l_2+l_3} = \eta^{l_1} - \eta^{l_2} - \eta^{l_3},$$

for some $l_i \in \mathbb{Z}$, with $\eta^{l_i} > 0$ and $l_1 \geq l_2 \geq l_3$.

In case (1.),

$$\eta^{l_1+l_2+l_3} - \eta^{l_1} - \eta^{l_2} - \eta^{l_3} = 0 \iff \eta^{l_1+l_2} - \eta^{l_1-l_3} - \eta^{l_2-l_3} - 1 = 0.$$

So η satisfies the polynomial $h_1(x) = x^{l_1+l_2} - x^{l_1-l_3} - x^{l_2-l_3} - 1$,

and $h_1(1) = 1 - 1 - 1 - 1 = -2$. Looking at $l_1 + l_2$ modulo 2,

$l_1 + l_2 \equiv 0 \text{ or } 1 \pmod{2}$. If $l_1 + l_2 \equiv 0 \pmod{2}$, then

$l_1 \equiv l_2 \pmod{2}$, which is equivalent to

$l_1 - l_3 \equiv l_2 - l_3 \pmod{2}$. So $h_1(-1) = 1 + 1 + 1 - 1 = 2$ for

$l_1 - l_3 \equiv 1 \pmod{2}$, or $h_1(-1) = 1 - 1 - 1 - 1 = -2$ for

$l_1 - l_3 \equiv 0 \pmod{2}$. If $l_1 + l_2 \equiv 1 \pmod{2}$, then

$l_1 - l_3 \not\equiv l_2 - l_3 \pmod{2}$ and $h_1(-1) = -1 - 1 = -2$.

In case (2.),

$$\eta^{l_1+l_2+l_3} - \eta^{l_1} + \eta^{l_2} + \eta^{l_3} = 0 \iff \eta^{l_1+l_2} - \eta^{l_1-l_3} + \eta^{l_2-l_3} + 1 = 0.$$

So η satisfies the polynomial $h_2(x) = x^{l_1+l_2} - x^{l_1-l_3} + x^{l_2-l_3} + 1$,

and $h_2(1) = 1 - 1 + 1 + 1 = 2$. Following the same procedure

as in case (1.) above, if $l_1 + l_2 \equiv 0 \pmod{2}$, then

$h_2(-1) = 1 + 1 - 1 + 1 = 2$ when $l_1 - l_3 \equiv 1 \pmod{2}$, and

$h_2(-1) = 1 - 1 + 1 + 1 = 2$ when $l_1 - l_3 \equiv 0 \pmod{2}$. If

$l_1 + l_2 \equiv 1 \pmod{2}$, then $l_1 - l_3 \not\equiv l_2 - l_3 \pmod{2}$ and

$h_2(-1) = -1 + 1 + 1 + 1 = 2$ when $l_1 - l_3 \equiv 1 \pmod{2}$,

and $h_2(-1) = -1 - 1 - 1 + 1 = -2$ when $l_1 - l_3 \equiv 0 \pmod{2}$.

Hence $h_1(x)$ and $h_2(x) = \pm 2$ for $x = \pm 1$. Letting

$h(x) = h_1(x)$ or $h_2(x)$, $h(\pm 1) = \pm 2$. Now $f(\eta) = 0$, $h(\eta) = 0$,

and $f(x) = \text{Irr}(\eta, \mathbb{Q}, x)$, so $f(x) | h(x) \Rightarrow f(\pm 1) | h(\pm 1)$.

Consequently, $f(\pm 1) = \pm 1$ or ± 2 .

Because the only real root of f is $\eta > 1$, and f is positive for sufficiently large (positive) x , $f(x) < 0$ for $x < \eta$. Now, $\pm 1 < \eta \Rightarrow f(\pm 1) = -1$ or -2 . So, looking at f ,
 $f(1) = 1 + a + b - 1 = a + b = -1$ or -2 , and
 $f(-1) = -1 + a - b - 1 = a - b - 2 = -1$ or -2 . Noting that
 $a + b \equiv a - b - 2 \pmod{2}$, there are just two systems of
linear equations that yield the values for a , and b :

$$\begin{array}{ccc}
a + b = -1 & \text{or} & a + b = -2 \\
a - b = 1 & & a - b = 0 \\
\Downarrow & & \Downarrow \\
a = 0, b = -1 & \text{or} & a = -1, b = -1.
\end{array}$$

Therefore, if η is a solution of $u_1 u_2 u_3 = u_1 + u_2 + u_3$, the minimal polynomial of η must be either $x^3 - x^2 - x - 1$, or $x^3 - x - 1$. So defining K_1, η_1, K_2 , and η_2 as:

$$\text{Irr}(\eta_1, \mathbb{Q}, x) = x^3 - x^2 - x - 1 \text{ for } K_1 = \mathbb{Q}(\eta_1), \text{ and}$$

$$\text{Irr}(\eta_2, \mathbb{Q}, x) = x^3 - x - 1 \text{ for } K_2 = \mathbb{Q}(\eta_2),$$

solutions to $u_1 u_2 u_3 = u_1 + u_2 + u_3$ can be found in K_1 and K_2 .

In K_1 , $\eta_1^3 - \eta_1^2 - \eta_1 - 1 = 0 \iff \eta_1^3 = \eta_1^2 + \eta_1 + 1 = (\eta_1^2)(\eta_1)(1)$,

and a solution to $u_1 u_2 u_3 = u_1 + u_2 + u_3$ is:

$$u_1 = \eta_1^2,$$

$$u_2 = \eta_1, \text{ and}$$

$$u_3 = 1.$$

In K_2 , because $\eta_2^3 - \eta_2 - 1 = 0$,

$$(\eta_2^3 + \eta_2)(\eta_2^3 - \eta_2 - 1) = \eta_2^6 - \eta_2^3 - \eta_2^2 - \eta_2 = 0$$

$$\iff \eta_2^6 = \eta_2^3 + \eta_2^2 + \eta_2. \text{ So a solution, in } K_2, \text{ to}$$

$u_1 u_2 u_3 = u_1 + u_2 + u_3$ is:

$$u_1 = \eta_2^3,$$

$$u_2 = \eta_2^2, \text{ and}$$

$$u_3 = \eta_2.$$

Q. E. D.

The case of an imaginary cubic field will be disposed of in the following corollary.

Corollary: Let K' be an imaginary cubic field. Then there is a solution to $u_1 u_2 u_3 = u_1 + u_2 + u_3$ in $U_K \iff K'$ is one of two possibilities:

1. $K'_1 = \mathbb{Q}(\eta'_1)$ where $\text{Irr}(\eta'_1, \mathbb{Q}, x) = x^3 - x^2 - x - 1$, or

2. $K'_2 = \mathbb{Q}(\eta'_2)$ where $\text{Irr}(\eta'_2, \mathbb{Q}, x) = x^3 - x - 1$,

for $\eta'_1, \eta'_2 \in \mathbb{C} \setminus \mathbb{R}$.

Proof:

By assumption, K' is an imaginary cubic field, so $r = 1$.

Let η' be a fundamental unit with the property that

$|\eta'| < 1$. Now $\partial_{\mathbb{Q}}(\eta') = 3$, otherwise, $\eta' \in \{1, -1\}$, which

contradicts the fact that $|\eta'| < 1$. Hence, $K = \mathbb{Q}(\eta')$. Let

$f(x) = \text{Irr}(\eta', \mathbb{Q}, x)$, η be the real conjugate of η' , and $K = \mathbb{Q}(\eta)$.

Because K and K' are conjugate extensions of $\mathbb{Q}$, and η and

η' are conjugate over $\mathbb{Q}$, $\exists$ an isomorphism

$\sigma: K' \rightarrow K \ni \sigma(\eta') = \eta$. Thus, $\eta'^{l_1+l_2+l_3} = \eta'^{l_1} + \eta'^{l_2} + \eta'^{l_3}$, or

$\eta'^{l_1+l_2+l_3} = \eta'^{l_1} - \eta'^{l_2} - \eta'^{l_3}$ if and only if the same is true for

$\eta \in K$. The rest follows from the theorem.

Q. E. D.

The final case of whether the equation $u_1 u_2 u_3 = u_1 + u_2 + u_3$ has any solutions in the unit group of a ring of integers of a number field of rank 1, is that for a totally imaginary quartic extension of $\mathbb{Q}$. Rather than

presenting all the details of the work required to handle this case (these details are in the yet-to-be-published paper by Edgar, Gordon, and Zhang [5]), instead a proposition, required to prove the theorem which tackles this last case, will be proved. The proof of this proposition involves concepts and techniques which have not yet been used in this thesis. Also, this proof is based on the following lemma, stated without proof below, which is a strengthened version of the first theorem of this chapter.

Lemma: Let K be a number field with a unit group that has rank 1. Let W_K be the roots of unity of K , η be a fundamental unit such that $|\eta| > 1$, and let $\zeta_n = e^{2\pi i/n}$. If $W_K \subseteq \langle \zeta_6 \rangle$ and $|\eta| > 3$, then there is no solution to $u_1 u_2 u_3 = u_1 + u_2 + u_3$ in K .

Proposition: Given that K is a totally imaginary quartic field such that $W_K = \langle \zeta_6 \rangle$, if K is a complex-multiplication field (or CM-field), and η is a fundamental unit with $|\eta| > 1$, then there exists a solution to $u_1 u_2 u_3 = u_1 + u_2 + u_3$ in U_K if and only if one of the following two conditions is true about K :

1. $K \supset \mathbb{Q}(\sqrt{2})$ or $K \supset \mathbb{Q}(\sqrt{5})$, or
2. $K = \mathbb{Q}(\eta)$, where $\text{Irr}(\eta, \mathbb{Q}, x) = x^4 + 5x^2 + 1$.

Proof:

According to p. 39 of Washington [15], because K is a quartic CM-field with $W_K = \langle \zeta_6 \rangle$, $K = \mathbb{Q}(\sqrt{-3}, \sqrt{m})$, where $m > 0$ is a squarefree integer. By the lemma, if $\exists$ a solution to $u_1 u_2 u_3 = u_1 + u_2 + u_3$ in U_K , then $|\eta| \leq 3$.

Letting $K^+ = K \cap \mathbb{R} = \mathbb{Q}(\sqrt{m})$, then, according to

Washington [15], $Q = (U_K : W_K U_{K^+}) = 1$ or 2 . If $Q = 1$, then

$U_K \cong W_K \times U_{K^+} \Rightarrow \eta^+ = \zeta_6^n \eta$ for some $n \in \mathbb{Z}_6$, where η^+ is a fundamental unit in K^+ . Hence, $|\eta^+| = |\zeta_6^n| |\eta| = 1 \cdot |\eta|$.

So if $\exists$ a solution to $u_1 u_2 u_3 = u_1 + u_2 + u_3$ in U_K , then

$|\eta^+| \leq 3$. If $Q = 2$, then $|\eta^+| \leq 9$ because η^+ may be the

square of the fundamental unit of K that is not in K^+ .

Let $m > 100$. If $m \equiv 1 \pmod{4}$, then

$$\eta^+ + \frac{1}{\eta^+} \geq \sqrt{m} \Rightarrow (\eta^+)^2 - \sqrt{m} \eta^+ + 1 \geq 0 \Rightarrow$$

$$\eta^+ \geq \frac{\sqrt{m} + \sqrt{m-4}}{2} > \frac{10 + 4\sqrt{6}}{2} > 9.$$

If $m \not\equiv 1 \pmod{4}$, then $\eta^+ \geq 1 + \sqrt{100} > 9$. Hence, if $\exists$ a

solution to $u_1 u_2 u_3 = u_1 + u_2 + u_3$ in U_K , then $m < 100$.

According to Table 1, on p. 422 of Borevich and

Shafarevich [2], $|\eta^+| < 9$ for the quadratic fields $Q(\sqrt{m})$,

where $m = 2, 3, 5, 10, 13, 15, 17, 21, 26, 29, 53$, or 77 .

Solutions have already been shown to exist for $K^+ = Q(\sqrt{2})$

and $K^+ = Q(\sqrt{5})$. If $K^+ = Q(\sqrt{3})$,

$K = Q(\sqrt{3}, \sqrt{-3}) \Rightarrow i \in K \Rightarrow W_K \neq \langle \zeta_6 \rangle$, so there are no

solutions when $m = 3$.

From p. 39 of Washington [15], $Q = 2 \iff \sigma: U_K \rightarrow W_K \ni$

$\sigma(\epsilon) = \epsilon/\bar{\epsilon}$ is surjective. So if $Q = 2$, then

$\exists \epsilon \in U_K \ni \epsilon/\bar{\epsilon} = -1 \Rightarrow \epsilon$ is purely imaginary. If

$m = 10, 13, 17, 26, 29, 53$, or 77 , then $Q(\sqrt{m}, \sqrt{-3}) = K$ has

no purely imaginary units. This can be observed by noting

that for $m = 13, 17, 29, 53$, or 77 , if α is an element of O_K ,

then, by p. 52 of Marcus [8], $\alpha = \frac{a + b\sqrt{m} + c\sqrt{-3} + d\sqrt{-3m}}{4}$,

for $a, b, c, d \in \mathbb{Z}$. If $\alpha \in C \setminus \mathbb{R}$, then $\alpha = \frac{c\sqrt{-3} + d\sqrt{-3m}}{4}$, and

$N_Q^K(\alpha) = \frac{9}{256}[c^4 - 2c^2d^2m + d^4m^2]$. If α is a unit, then

$N_Q^K(\alpha) = \pm 1$. But this is impossible because the equation

$$c^4 - 2c^2d^2m + d^4m^2 = \pm \frac{256}{9}$$

would have to be true for $c, d, m \in \mathbb{Z}$. Thus there exist no purely imaginary units

in the ring of integers of $K = \mathbb{Q}(\sqrt{m}, \sqrt{-3})$ where

$m = 13, 17, 29, 53$, or 77 , hence there are no solutions to

$$u_1u_2u_3 = u_1 + u_2 + u_3 \text{ in } U_K, \text{ and } Q = 1.$$

Now, for $m = 10$ or 26 , if α is an element of the ring of integers of $K = \mathbb{Q}(\sqrt{m}, \sqrt{-3})$, then, by p. 52 of Marcus [8],

$$\alpha = \frac{a + b\sqrt{m} + c\sqrt{-3} + d\sqrt{-3m}}{2}, \text{ for } a, b, c, d \in \mathbb{Z}. \text{ Again, if}$$

$$\alpha \text{ is purely imaginary, then } a, b = 0 \Rightarrow \alpha = \frac{c\sqrt{-3} + d\sqrt{-3m}}{2}$$

for $c, d \in \mathbb{Z}$, and $N_Q^K(\alpha) = \frac{9}{16}[c^4 - 2c^2d^2m + d^4m^2]$. If α is a

unit, then $N_Q^K(\alpha) = \pm 1$, but, because $c, d, m \in \mathbb{Z}$,

$$N_Q^K(\alpha) = \pm 1 \Rightarrow 9 \mid 16, \text{ which is impossible. Hence there are}$$

no purely imaginary units in the ring of integers of

$K = \mathbb{Q}(\sqrt{m}, \sqrt{-3})$, where $m = 10$ or 26 .

For $m = 15$, if $\alpha \in O_K$, then, by p. 52 of Marcus [8], α has

$$\text{the form } \alpha = \frac{a + b\sqrt{15} + c\sqrt{-3} + d\sqrt{-5}}{2}, \text{ for } a, b, c, d \in \mathbb{Z}.$$

Thus, if α is purely imaginary, $a, b = 0 \Rightarrow \alpha = \frac{c\sqrt{-3} + d\sqrt{-5}}{2}$

and $N_Q^K(\alpha) = \frac{1}{16}[9c^4 - 30c^2d^2 + 25d^4]$. If α is a unit,

$N_Q^K(\alpha) = \pm 1 \Rightarrow 3c^2 - 5d^2 = \pm 4$. Now, viewing this

equation modulo 5, $c^2 \equiv 0$ or $\pm 1 \pmod{5}$, hence,

$3c^2 - 5d^2 \equiv 0$ or $\pm 3 \pmod{5} \not\equiv \pm 4$. So, O_K , for

$K = \mathbb{Q}(\sqrt{15}, \sqrt{-3})$, contains no purely imaginary units.

So far, $K = \mathbb{Q}(\sqrt{m}, \sqrt{-3})$, has been shown to contain no purely imaginary units for

$m = 10, 13, 15, 17, 26, 29, 53$, or 77 . Thus $Q \neq 2$

for these m . This means that $Q = 1$ for these m , or the

fundamental units of $\mathbb{Q}(\sqrt{m})$ are the fundamental units of

K . But, according to Washington [15], p. 39, for each m ,

$|\eta| > 3$. Thus $u_1u_2u_3 = u_1 + u_2 + u_3$ has no solutions in U_K

for these values of m .

The only remaining value of m that needs to be checked

is $m = 21$. Looking at $K = \mathbb{Q}(\sqrt{21}, \sqrt{-3})$, let $\alpha \in O_K$. From

pp. 51-2 of Marcus [8], any such α can be expressed as

$\alpha = \frac{a + b\sqrt{21} + c\sqrt{-3} + d\sqrt{-7}}{4}$, for $a, b, c, d \in \mathbb{Z}$. Because α is

desired to be purely imaginary, $\alpha = \frac{c\sqrt{-3} + d\sqrt{-7}}{2}$. Now

$N_Q^K(\alpha) = \frac{9c^4 - 42c^2d^2 + 49d^4}{256}$. If α is a unit, $N_Q^K(\alpha) = \pm 1$,

so $\frac{9c^4 - 42c^2d^2 + 49d^4}{256} = \pm 1 \Rightarrow 9c^4 - 42c^2d^2 + 49d^4 = \pm 256$,

or $(-3c^2 + 7d^2)^2 = 256 \Rightarrow -3c^2 + 7d^2 = \pm 16 \Rightarrow$

$-3c^2 \equiv \pm 2 \pmod{7}$. Looking at $-3c^2 \equiv 2 \pmod{7}$, this

implies that $c^2 \equiv 4 \pmod{7} \Rightarrow c \equiv \pm 2 \pmod{7}$. In fact,

$c = \pm 2, d = \pm 2$ yield units. Taking a look at

$$f(x) = (x - \frac{\sqrt{-3} + \sqrt{-7}}{2})(x - \frac{\sqrt{-3} - \sqrt{-7}}{2})(x + \frac{\sqrt{-3} + \sqrt{-7}}{2})(x + \frac{\sqrt{-3} - \sqrt{-7}}{2}),$$

$$f(x) = x^4 + 5x^2 + 1 = (x^2 - \sqrt{-3}x + 1)(x^2 + \sqrt{-3}x + 1).$$

Choosing $\eta = \frac{\sqrt{-3} + \sqrt{-7}}{2}$,

$$\text{Irr}(\eta, \mathbb{Q}(\sqrt{-3}), x) = x^2 - \sqrt{-3}x + 1 = x^2 - (\zeta_6 + \zeta_6^2)x + 1.$$

Hence, $\eta^2 - \zeta_6\eta - \zeta_6^2\eta + 1 = 0 \Rightarrow \eta^2 = \zeta_6\eta + \zeta_6^2\eta - 1$, and by

letting $u_1 = \zeta_6\eta, u_2 = \zeta_6^2\eta$, and $u_3 = -1$, a solution to

$u_1u_2u_3 = u_1 + u_2 + u_3$ has been found.

Q. E. D.

BIBLIOGRAPHY

1. Artin, Emil. *Theory of Algebraic Numbers*. Trans. and published by George Striker. Göttingen, Germany, 1959.
2. Borevich, Z. I. and I. R. Shafarevich. *Number Theory*. New York: Academic Press, 1966 (p. 422).
3. Cassels, J. W. S. "On a Diophantine Equation." *Acta Arithmetica*, 6, 1960: pp. 47-52.
4. Delone, B. N. and D. K. Faddeev. *The Theory of Irrationalities of the Third Degree*. Providence, R. I.: American Mathematical Society, 1964 (p. 141).
5. Edgar, Hugh, L. C. Zhang, and J. R. Gordon. "On Unit Solutions of the Equation $xyz = x + y + z$ in Totally Imaginary Quartic Fields." (to be published).
6. Hungerford, Thomas W. *Algebra*. New York: Springer-Verlag, 1974.
7. Lazarus, Andrew J. Letter to the editor. *The American Mathematical Monthly*, 96(January 1989): p. 17.
8. Marcus, D. A. *Number Fields*. New York: Springer-Verlag, 1974 (pp. 51-2).
9. Mollin, R. A., S. Small, K. Varadarajan, and P. G. Walsh. "On Unit Solutions of the Equation $xyz = x + y + z$ in the Ring of Integers of a Quadratic Field." *Acta Arithmetica*, 48, 1987: pp. 341-5.
10. Samuel, Pierre. *Algebraic Theory of Numbers*. Trans. Allan J.

Silberger. Boston: Houghton Mifflin Company, 1969.

11. Shanks, Daniel. "Incredible Identities." *Fibonacci Quarterly*, 12(October 1974): pp. 271, 280.
12. Sierpinski, W. "On Some Unsolved Problems of Arithmetics." *Scripta Mathematica*, 25, 1960: pp. 125-36.
13. Sierpinski, W. "Remarques sur le Travail de M. J. W. S. Cassels's 'On a Diophantine Equation'." *Acta Aritihmetica*, 6, 1961: pp. 469-71.
14. Van der Ploeg, C. E. "Duality in Nonnormal Quartic Fields." *The American Mathematical Monthly*, 94(March 1987): pp. 279-84.
15. Washington, L. C. *Introduction to Cyclotomic Fields*. New York: Springer-Verlag, 1982 (p. 39).
16. Zhang, L. C., and J. R. Gordon. "On Unit Solutions of the Equation $xyz = x + y + z$ in a Number Field with Unit Group of Rank 1." (to be published).
17. Zhang, L. C., and J. R. Gordon. "On Unit Solutions of the Equation $xyz = x + y + z$ in Not Totally Real Cubic Fields." (to be published).