1999

Inequalities Between Pythagoras Numbers and Algebraic Ranks in Witt Rings of Fields.

Sidney Taylor Hawkins
Louisiana State University and Agricultural & Mechanical College

Follow this and additional works at: https://digitalcommons.lsu.edu/gradschool_disstheses

Recommended Citation

Hawkins, Sidney Taylor, "Inequalities Between Pythagoras Numbers and Algebraic Ranks in Witt Rings of Fields." (1999). *LSU Historical Dissertations and Theses*. 6942.
https://digitalcommons.lsu.edu/gradschool_disstheses/6942

This Dissertation is brought to you for free and open access by the Graduate School at LSU Digital Commons. It has been accepted for inclusion in LSU Historical Dissertations and Theses by an authorized administrator of LSU Digital Commons. For more information, please contact gradetd@lsu.edu.

INFORMATION TO USERS

This manuscript has been reproduced 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.

Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

INEQUALITIES BETWEEN PYTHAGORAS
NUMBERS AND ALGEBRAIC
RANKS IN WITT RINGS OF FIELDS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by

Sidney Taylor Hawkins

B.S., Grambling State University, 1973

M.S., Louisiana Tech University, 1975

M.S., Tulane University, 1995

May 1999

UMI Number: 9936093

UMI Microform 9936093
Copyright 1999, by UMI Company. All rights reserved.

**This microform edition is protected against unauthorized
copying under Title 17, United States Code.**

UMI
300 North Zeeb Road
Ann Arbor, MI 48103

Acknowledgments

All the members of the Nathaniel Millner family have supported me throughout my graduate endeavors. This dissertation is dedicated to them, and especially to Nathaniel Millner, whose great encouragement has helped give birth to this dissertation even though he did not live to see its completion.

I thank Dr. Norman Francis, President of Xavier University, New Orleans, who encouraged me to return to graduate school to complete a doctoral degree in mathematics.

I thank Louisiana State University for supporting me with a Huel Perkins Fellowship during my graduate study.

I express my thanks to the entire faculty of the LSU Math Department, who have helped me at every stage of my studies.

I thank P.E. Conner, who helped formulate the problem discussed in this dissertation.

I thank the members of my doctoral committee, R. Fabec, P. Gilmer, J. Hurrelbrink, G. Olafsson, R. Perlis, R. Svoboda, and Gregory Stacy, whose confidence in me helped me believe in myself.

And I wish to express my special thanks to my advisor, R. Perlis, who has inspired me and helped me in ways too numerous to enumerate.

Table of Contents

Acknowledgments	ii
Abstract	iv
Chapter 1. Introduction.....	1
Chapter 2. Background on Quadratic Forms and Field Extensions.	3
2.1 Quadratic Forms	3
2.2 Witt Rings	5
2.3 Trace Forms	8
2.4 Hilbertian Fields	9
2.5 A Bit of Number Theory	10
2.6 Pfister Forms	12
Chapter 3. Pythagoras Numbers and Algebraic Ranks.....	13
3.1 The Conner Polynomial	13
3.2 The Main Result	16
Chapter 4. Degree Three Forms.....	20
4.1 A Long Computation	20
References	27
Vita	28

Abstract

This dissertation establishes new lower bounds for the algebraic ranks of certain Witt classes of quadratic forms. Let K denote a field of characteristic different from 2 and let q be a quadratic form over K . The form q is said to be *algebraic* when q is Witt equivalent to the trace form $q_{L|K}$ of some finite algebraic field extension $L|K$. When q is algebraic, the algebraic rank of q is defined to be the degree of the minimal extension $L|K$ whose trace form is Witt equivalent to q . It is an important, unsolved problem to find reasonable bounds on the algebraic rank of a given algebraic form.

This dissertation makes a beginning contribution to this problem of bounding the algebraic rank by investigating a simple, special case. Let σ denote a totally positive square-class in a field K (characteristic different from 2, as always). Assuming that the 1-dimensional quadratic form σX^2 is algebraic, what can be said about the algebraic rank? Even in this simple case, little was known prior to this dissertation. Let $py_K(\sigma)$ denote the pythagoras number of σ relative to K . This is the smallest natural number, j , such that σ can be written as a sum of j squares of elements in K . Let n be the algebraic rank of σX^2 . In general, n is unknown, and a reasonable lower bound is sought. The main result is:

$$py_K(\sigma) \leq 2^{n-d(n+1)}$$

where $d(n+1)$ is the sum of the coefficients of the 2-adic expansion of $n+1$. Thus, if σ is chosen with a large pythagoras number, then the algebraic rank n must be correspondingly large as well.

This dissertation also considers a slightly more general case.

Chapter 1

Introduction

This dissertation is concerned with a problem in the theory of quadratic forms over an arbitrary field K of characteristic different from 2. There is a special class of forms over K , called trace forms, which arise from finite separable field extensions of K (details are found in Chapter 1). Over arbitrary fields, the problem of deciding whether a given form is or is not a trace form remains unsolved. Olga Taussky-Todd (see [11]) gave a condition ('all signatures are non-negative') which is necessary for a form to be a trace form. Over certain fields, like the field of rational numbers, work of Conner-Perlis, [2], Kruskemper, [6], and Epkenhans [3] show that Taussky-Todd's condition, together with the mild condition that the rank of the form exceed 3, is also sufficient; however, over arbitrary fields no sufficient condition is known.

This dissertation concerns forms over K that are known from the outset to differ from a trace form by a hyperbolic form. That is, one starts with a form that is either itself a trace form or differs from some trace form by a sum of forms of the shape

$$x^2 - y^2.$$

In the language of Witt rings, this means that one starts with a form whose Witt class contains at least one trace form. The problem is to compute the algebraic rank of this Witt class, that is, to find the degree of the field extension of least degree over K whose trace form lies in the given class. Over the field of rational numbers, the work of Epkenhans essentially solves this problem: If q is a form, known to be Witt equivalent to some trace form, and whose anisotropic part (the part remaining after removing all hyperbolic subforms) has rank four or larger, then

the algebraic rank of q is exactly the rank of the anisotropic part. But essentially nothing was known about algebraic rank over general fields.

This dissertation makes a detailed study of a very special case of the problem of determining the algebraic rank. Namely, the 1-dimensional forms

$$\sigma x^2$$

are studied. By Taussky-Todd's condition, σ must be totally positive if this form is Witt equivalent to some trace form. Now take σ to be totally positive, and assume that σx^2 is Witt equivalent to a trace form of some extension of K . Under these circumstances, it is proved that the algebraic rank, n of σx^2 must satisfy the inequality

$$py_K(\sigma) \leq 2^{n-d(n+1)}$$

where $py_K(\sigma)$ is the pythagoras number of σ , this being the least number of squares of elements of K whose sum equals σ , and $d(n+1)$ is the number of 1's appearing in the binary expansion of $n+1$. Hence, if the pythagoras number of σ is large, then so is the algebraic rank.

These results generalize to forms that are multiples of σx^2 .

Chapter 2 provides the necessary background. Chapter 3 contains the main result. Chapter 4 contains a detailed study of arbitrary degree 3 forms. This was done partially to see whether the main inequality could be improved in this case—apparently it can't— and partially for intrinsic interest.

Chapter 2

Background on Quadratic Forms and Field Extensions

2.1 Quadratic Forms

This chapter contains the necessary background to make this dissertation self-contained. Details can be found in any standard text on quadratic forms, see, *e.g.*, [7], [8], [9]. Let K be a field. A *non-degenerate quadratic form over K* is any symmetric expression of the form

$$q = \sum_{i,j=1}^t a_{ij}x_i x_j \tag{1}$$

for which the coefficients a_{ij} satisfy the two conditions $a_{ij} = a_{ji}$ and $\det(a_{ij}) \neq 0$. If the characteristic of the field K is different from 2, then any expression of the form (1) can be made symmetric by replacing the coefficient a_{ij} by $\frac{a_{ij}+a_{ji}}{2}$. Throughout this dissertation we exclude fields of characteristic 2 and we always take our quadratic forms to be symmetric as well as non-degenerate.

Let q be given and let V be a vector space of dimension t over K . By fixing a basis $\theta_1, \theta_2, \dots, \theta_t$ each vector v of V can be written as a K -linear combination

$$v = \sum_{i=1}^t c_i \theta_i$$

with the coefficients c_i in K . The form q gives rise to a function from V to K whose value at v is obtained by replacing x_i in (1) by c_i ; this is an element of K which may be thought of as the *length* of the vector v . It is *not* assumed that K is an ordered field, so there is not necessarily a notion of ‘positive’ associated with K . In particular, it is *not* assumed that the ‘length’ of a non-zero vector v is positive; in fact this length can be 0 even when $v \neq 0$. Such non-zero vectors of 0 length are

called *isotropic* vectors. A form for which there are no isotropic vectors is called *anisotropic*.

Starting with one quadratic form q over K we obtain others by making an invertible linear transformation of the variables over K . Any two quadratic forms which arise from each other in this manner are called *isometric*. Two isometric quadratic forms may be thought of as expressing the same inner-product on V in terms of different bases; as such, isometric forms are considered to be 'equal'.

Under a suitable linear change of variables, any quadratic form over K (always of characteristic different from 2) is isometric to a *diagonal* quadratic form, that is, isometric to a form with $a_{ij} = 0$ whenever $i \neq j$. In practice, it can take some effort to actually diagonalize a given form, although algorithms exist that perform the diagonalization. In this dissertation, we take all forms to be diagonalized. The standard notation for the diagonalized form $\sum_{i=1}^t a_i x_i^2$ is

$$\sum_{i=1}^t a_i x_i^2 = \langle a_1, a_2, \dots, a_t \rangle.$$

Thus $\langle a_1 \rangle$ denotes the 1-dimensional form $a_1 x_1^2$, and the t -dimensional form $\langle a_1, a_2, \dots, a_t \rangle$ can also be written as

$$\langle a_1 \rangle + \langle a_2 \rangle + \dots + \langle a_t \rangle.$$

To interpret this latter sum as an expression in the form (1), distinct terms always get associated with different x_i 's. For example, $\langle a, a \rangle = \langle a \rangle + \langle a \rangle$ refers to the form $ax_1^2 + ax_2^2$. Care must be given to distinguish the 2-dimensional form $2\langle a \rangle$ (which is just $\langle a, a \rangle$) from the 1-dimensional form $\langle 2a \rangle$.

Replacing x_1 by cx_1 with $c \neq 0$ transforms ax_1^2 into $ac^2x_1^2$. Thus $\langle a \rangle$ and $\langle ac^2 \rangle$ are considered to be equal. Thus any coefficient in a diagonalized form can be replaced by itself times any non-zero square without changing the form. In particular, any

coefficient which is a non-zero square in K can be replaced by 1. A diagonalization of a form is not at all unique.

When the field K has an *ordering* then we can speak about a non-zero element of K element being positive or negative with respect to the given ordering. A field may have one, many, or no orderings. An ordering is determined by its *positive cone*, P . Let a quadratic form q over K be given. Each ordering of K gives rise to a *signature* of q , as follows. Write $q = \langle a_1, a_2, \dots, a_t \rangle$. Then

$$\text{sig}_P(q) = \#\{i | a_i > 0\} - \#\{i | a_i < 0\}.$$

Sylvester's classical 'Theorem of Inertia' shows that this signature does not depend on how q has been diagonalized. If K allows more than one ordering, then each ordering gives rise to a different signature. The form q over K is said to be *positive* when $\text{sig}_P(q) \geq 0$ for every ordering P of K . Whether a form q is positive or not depends on the field K as well as the form q . When K has no orderings at all, then every form q is considered to be positive by default.

The 1-dimensional form $\langle a \rangle$ is closely associated with the non-zero element a in K . The form $\langle a \rangle$ is positive precisely when the element a is *totally positive*, meaning that a is positive in every ordering of K . If K has no orderings at all, then every non-zero element (including -1) is considered to be totally positive.

2.2 Witt Rings

In 1937, Ernst Witt introduced a significant new notion into the study of quadratic forms over fields, see [12]. Up until 1937 one could add forms by concatenation, but there was no useful notion of subtracting forms. For example, $\langle a \rangle + \langle a \rangle$ refers to the form $ax_1^2 + ax_2^2$ and not to the form $2ax_1^2$. One can try to 'subtract' the form $\langle a \rangle$ from itself, formally producing

$$\langle a \rangle - \langle a \rangle = \langle a, -a \rangle.$$

But the resulting ‘difference’ is a 2-dimensional form. Witt suggested considering any form isometric to $\langle a, -a \rangle$ to be ‘trivial’. Any form which is a sum of these ‘trivial’ forms is called *hyperbolic* forms.

In Witt’s sense, one can at any time add or remove as many 2-dimensional forms $\langle a, -a \rangle$ as one wants. So two forms of different dimensions can be Witt equivalent. Given a form q , by removing as many hyperbolic planes $\langle a, -a \rangle$ as possible, which may involve several suitable re-diagonalizations, one obtains an anisotropic form which is Witt equivalent to the original form q . This anisotropic form is the form of smallest rank in the Witt class of q . Each Witt class contains exactly one anisotropic form, called the *anisotropic representative* of the Witt class.

Isometric forms are Witt equivalent, and a famous theorem of Witt states that two Witt equivalent forms are isometric if and only if they have the same dimension.

Witt equivalence allows forms to be subtracted: Given two diagonalized forms

$$\langle a_1, a_2, \dots, a_t \rangle \text{ and } \langle b_1, b_2, \dots, b_s \rangle$$

then their *formal difference* is

$$\langle a_1, a_2, \dots, a_t, -b_1, -b_2, \dots, -b_s \rangle.$$

As a form, this difference has dimension $t + s$, but when this form is regarded up to Witt equivalence rather than isometry, quite possibly some hyperbolic planes might split off. In particular, the difference of a form with itself

$$\langle a_1, a_2, \dots, a_t \rangle - \langle a_1, a_2, \dots, a_t \rangle$$

is a sum of t hyperbolic planes $\langle a_i, -a_i \rangle$ and hence is Witt equivalent to 0. Read up to Witt equivalence, the collection of all non-degenerate symmetric quadratic forms over a field K thus becomes an additive group, denoted $W(K)$. This additive

group also carries a multiplication making $W(K)$ into a commutative ring with identity, still denoted $W(K)$ and called the *Witt ring of K* . Multiplication is ‘tensor product’, which for diagonal forms is quite simple: for example, writing a simple dot in place of $\otimes$,

$$\langle a_1, a_2, a_3 \rangle \cdot \langle b_1, b_2 \rangle = \langle a_1 b_1, a_1 b_2, a_2 b_1, a_2 b_2, a_3 b_1, a_3 b_2 \rangle,$$

again read up to Witt equivalence.

The Witt ring of a field K depends only on the isomorphism class of K . Important classical field invariants can often be read in terms of the Witt ring $W(K)$. For example, the *level* of a field K is the minimal natural number n (if it exists) such that -1 can be written as a sum of n squares of elements in K . If -1 cannot be written as a sum of finitely-many squares in K then K has infinite level, in which case K is said to be *formally real*. A field is formally real if and only if the field admits an ordering, *i.e.*, can be ordered in at least one way. Pfister proved that the level of a non-formally real field is always a power of 2. Moreover, Pfister proved that the level of K is exactly one-half of the additive order of the multiplicative identity $\langle 1 \rangle \in W(K)$. Thus, the Witt ring of K detects the level of K .

There is a generalization of the notion of level. For a non-zero element $a \in K$, the *pythagoras number* of a relative to K , denoted $py_K(a)$, is the minimal natural number n (if it exists) such that a can be written as a sum of n squares of elements in K . If no such n exists, then the pythagoras number $py_K(a)$ is infinite. It is a fact that the element a has finite pythagoras number if and only if a is *totally positive*, meaning that a is positive in every ordering of K . If K has no ordering, then every non-zero element a of K is totally positive by default.

The pythagoras number of a , when finite, need not be a power of 2. However there is still a direct connection between $py_K(a)$ and the additive order of an

element in $W(K)$, which we will now explain. The pythagoras number is finite and lies between

$$2^{r-1} < py_K(a) \leq 2^r$$

for some integer $r \geq 0$ if and only if 2^r is the exact additive order of the element $\langle 1, -a \rangle$ in $W(K)$. This result is found as C.

2.3 Trace Forms

The standard reference for this section is [2].

The smallest fields are the rational numbers $\mathbb{Q}$, and the finite fields $\mathbb{F}_p$ where p is a prime number. To any of these one can adjoin a mixture of finitely-many (or even infinitely-many) transcendental and algebraic elements, creating more fields; all fields arise in this fashion. The standard examples are the algebraic number fields K (finite extensions of $\mathbb{Q}$), the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, and the finite fields $\mathbb{F}_q$ where q is a prime power. When one field L contains another, K , then L is said to be an *extension* of K , denoted by $L|K$. The bottom field K is called the *base field*. When L is an extension of K , then L is a K -vector space. The *degree* of the extension is the vector-space dimension of L considered as a K -vector space. If α denotes a root of a polynomial $f \in K[x]$ with coefficients in K , then the smallest extension of K containing α is denoted $K[\alpha]$, and is a finite extension of K . If the polynomial f has no repeated roots (in some algebraic closure of K) then the extension $K[\alpha] | K$ is called *separable*.

Let $L|K$ denote a finite separable field extension of degree n , where $L = K[\alpha]$. The form $q_{L|K} = q_{L|K}(x_1, x_2, \dots, x_n)$ in n variables defined by

$$q_{L|K}(x_1, x_2, \dots, x_n) = \sum_{i,j=1}^n (\text{trace}_{L|K} \alpha^{i+j}) x_i x_j$$

is the *trace form* of the extension. This is a non-degenerate quadratic form over K ; the non-degeneracy of this form being an alternative way of expressing the statement that $L|K$ is separable.

Any Witt class in $W(K)$ arising in this way, *i.e.*, any class of Witt equivalent forms which contains the trace form $q_{L|K}$ for some finite separable extension L of K , is called an *algebraic class*, or just *algebraic*. When the Witt class of a form q is algebraic, its *algebraic rank*, denoted $Alg\langle q \rangle$, is the smallest natural number n , for which there is a finite separable extension $L|K$ of degree n whose trace form $q_{L|K}$ is Witt equivalent to q . If the Witt class of a form q does not contain the trace form of any finite separable extension $L|K$, then the algebraic rank of q is infinity. The *geometric rank* of the Witt class of q is defined to be the rank (number of variables) of the smallest-ranked quadratic form that is Witt equivalent to q . Stated another way, the geometric rank of the Witt class of q , denoted $Geo\langle q \rangle$ is the rank of the unique anisotropic representative of q . Clearly, for any form q

$$Geo\langle q \rangle \leq Alg\langle q \rangle.$$

By a theorem of Olga Taussky-Todd, the algebraic rank of a form q over K is infinite if K admits at least one ordering for which the corresponding signature of q is negative. So a necessary condition for a form q to have finite algebraic rank is that q is positive, meaning that q has non-negative signature with respect to every ordering (if there are any!) of K .

2.4 Hilbertian Fields

The standard reference for this section is chapter 11 of [4]; see also [10].

There is an important special class of fields, called the *hilbertian fields*, for which it is known that this necessary condition is also sufficient to insure that a form have finite algebraic rank. By definition, a field K is *hilbertian* provided that for

every $n \geq 1$ and for every polynomial $p(x_1, x_2, \dots, x_{n+1})$ in $n + 1$ variables over K which is irreducible in $K[x_1, x_2, \dots, x_{n+1}]$ there is at least one choice of elements $a_1, a_2, \dots, a_n$ in K for which $p(a_1, a_2, \dots, a_n, x_{n+1})$ is irreducible in $K[x_{n+1}]$. Hilbert's Irreducibility Theorem states that the field $\mathbb{Q}$ of rational numbers is hilbertian. The class of hilbertian fields is very large but does not include all fields. For example, $\mathbb{R}$ and $\mathbb{C}$ are not hilbertian, nor is any finite field. However, if F is any field whatsoever, then by adjoining a transcendental element x to F we obtain $F(x)$ which is hilbertian. In addition to $F(x)$ for any field F , the following fields are also known to be hilbertian: Any number field, any infinite field finitely-generated over its prime subfield, and any finitely-generated extension of a hilbertian field.

In the special case when K is an algebraic number field, then Epkenhans has proved the following very strong result (see [3]): Let q be a positive anisotropic quadratic form of rank t over a number field K . If $t \geq 4$ then $\text{Alg}\langle q \rangle = \text{Geo}\langle q \rangle = t$, and if $t = 1, 2, 3$ then $\text{Alg}\langle q \rangle \leq 5$.

Scharlau and Kruskemper work, [10], shows that Epkenhans' result does not hold over arbitrary hilbertian fields. Chapter 3 contains a simple example, independent of [10], of an anisotropic positive quadratic form q of rank 9 over a hilbertian field K that is not isometric to a trace form of a degree 9 extension of K .

2.5 A Bit of Number Theory

The next result concerns a bit of number theory that will be needed in Chapter 3. The result is not at all new, but we give a full proof since we did not find a convenient reference.

Theorem 2.1. $\text{ord}_2[n!] = n - d(n)$

where $d(n)$ is the sum of the coefficients in the binary expansion of n .

Proof. We begin with some observations: For $k \geq 0$ the binary expansion of k

$$k = \sum_{j=0}^{\infty} c_j(k) 2^j$$

where the coefficients $c_j(k)$ are either 0 or 1 and are 0 for all large indices j . When $k = 0$ then $c_j(k) = 0$ for all j . For $k > 0$, then the binary expansion of k begins with either 0 or 1; in either case, we may think of this expansion as beginning with a string of 1's of length $s \geq 0$. These initial s non-zero coefficients are labeled $c_0(k), c_1(k), \dots, c_{s-1}(k)$ so the number s is also the index of the first zero coefficient:

$$s = \min\{j \mid c_j(k) = 0\}.$$

Adding 1 to k produces $k + 1$, whose binary expansion begins with a string of 0's of length s followed by the coefficient $c_s(k + 1) = 1$. Thus $k + 1$ begins with $1 \cdot 2^s$ and continues with higher powers of 2. Hence

$$\text{ord}_2(k + 1) = s \tag{2}$$

where, as above, s is the index of the first 0 coefficient in the expansion of k .

With this background, the proof of the theorem goes by induction on n . When $n = 1$, then $\text{ord}_2[1!] = 0$, the sum of the coefficients in the binary expansion 1 is $d(1) = 1$, and thus we have $\text{ord}_2[1!] = 1 - d(1)$ as we want. Now suppose that $\text{ord}_2[k!] = k - d(k)$ where $d(k)$ denotes the sum of the coefficients in the binary expansion of k . We must show that

$$\text{ord}_2[(k + 1)!] \stackrel{?}{=} (k + 1) - d(k + 1).$$

From the observations at the start of this proof, the binary expansion of k starts off with a string of 1's of length s followed by a 0, so the binary expansion of $k + 1$ begins with a string of 0's of length s followed by a 1, after which the expansions of k and $k + 1$ proceed the same way.

Hence the coefficient sum for $k + 1$ is

$$d(k + 1) = d(k) - s + 1.$$

Therefore

$$\text{ord}_2[(k + 1)!] = \text{ord}_2[k!] + \text{ord}_2[k + 1] = k - d(k) + s$$

which can be rewritten as

$$k - (d(k) - s) = k - [d(k) - s + 1] + 1 = (k + 1) - d(k + 1)$$

completing the proof. $\square$

2.6 Pfister Forms

A k -fold *Pfister form* over a field K is a quadratic form of the shape

$$\prod_{j=1}^k \langle 1, a_j \rangle,$$

with the coefficients a_j being non-zero elements of K . This chapter closes with a standard observation on Pfister forms.

Let $\wp$ denote the 1-dimensional Pfister form $\wp = \langle 1, x \rangle$. Then $\wp^2 = \langle 1, x, x, x^2 \rangle = \langle 1, 1, x, x \rangle = 2\wp$.

Lemma 2.2.

$$\wp^{r+1} = 2^r \wp$$

for any integer $r \geq 0$.

Proof. By induction on r . The statement is true when $r = 0$. Now suppose that the statement holds when r equals some integer $k \geq 0$. Then $\wp^{k+2} = \wp^{k+1} \cdot \wp = 2^k \wp \cdot \wp = 2^k \cdot (\wp)^2 = 2^k (2\wp) = 2^{k+1} \wp$. $\square$

Chapter 3

Pythagoras Numbers and Algebraic Ranks

3.1 The Conner Polynomial

Fix a natural number $n \geq 1$. Let

$$P_n(x) = \prod_{k=0}^n (x - k).$$

Thus, $P_n(x)$ is a polynomial of degree $n+1$ with constant term 0 and having roots $0, 1, 2, \dots, n$. This polynomial, called the *Conner polynomial*, was introduced in [5]. This polynomial can be interpreted as having coefficients in any commutative ring R , by identifying the natural number k with the ring element $k \cdot 1$ in R , where 1 is the multiplicative identity of the ring. In particular, it makes sense to evaluate $P_n(x)$ by replacing x by any ring element r . The ring R that is of interest here is the Witt ring $R = W(K)$ of a field K . In [1], it is proved that $P_n(x)$ vanishes on all Witt classes in $W(K)$ that are represented by a trace form $q_{L|K}$ of a finite separable field extension $L|K$ of degree n .

In this chapter the polynomial $P_n(x)$ will be evaluated on a 1-dimensional Witt class $\langle \sigma \rangle$ and on the m -dimensional Witt classes $m\langle \sigma \rangle$ for $m \leq n$.

Start by decomposing $P_n(x)$.

Write

$$P_n(x) = \sum_{j=1}^{n+1} s_j x^j,$$

recalling that the constant term $s_0 = 0$. Then

$$P_n(x) = P_n^+(x) + P_n^-(x)$$

where

$$P_n^+(x) = \sum_{j \text{ even}} s_j x^j$$

and

$$P_n^-(x) = \sum_{j \text{ odd}} s_j x^j.$$

Then $P_n^+(x)$ is an even function and $P_n^-(x)$ is an odd function.

Noting that m is a root of $P_n(x)$, since $m \leq n$, we see that

$$0 = P_n(m) = P_n^+(m) + P_n^-(m).$$

This gives

Lemma 3.1. $P_n^+(m) = -P_n^-(m)$ when $m \leq n$. $\square$

Now consider $P_n(x)$ evaluated at $-x$. Since the component polynomials $P_n^+(x)$ and $P_n^-(x)$ are even and odd, respectively, it follows that

$$P_n(-x) = P_n^+(-x) + P_n^-(-x) = P_n^+(x) - P_n^-(x). \text{ With Lemma 3.1, this yields}$$

Lemma 3.2. $P_n(-x) = 2P_n^+(x)$. $\square$

Since $-m$ is not a root of $P_n(x)$ when m lies outside the range $0, 1, \dots, n$, it follows that

Lemma 3.3. $P_n^+(m) \neq 0 \in \mathbb{Z}$ for $m \geq 1$. $\square$

Now take $m \geq 1$. Then $P_n(-m)$ is given by

$$\prod_{k=0}^n (-m - k) = (-1)^{n+1} (m)(m+1) \cdots (m+n) = (-1)^{n+1} \frac{(n+m)!}{(m-1)!}$$

which can be rewritten as $(-1)^{n+1} \frac{(n+m)! \cdot m}{m!}$. Combining this with $2P_n^+(m) = P_n(-m)$ from Lemma 3.2 gives

Lemma 3.4. $P_n^+(m) = (-1)^{n+1} \cdot \frac{m}{2} \cdot \frac{(n+m)!}{m!}$. $\square$

Now fix a square-class $\sigma \in K^*/K^{*2}$ and consider the Witt class $m\langle\sigma\rangle$, this being the Witt class of the quadratic form $\sigma x_1^2 + \sigma x_2^2 + \cdots + \sigma x_n^2$. We suppose that σ is *totally positive*, meaning that σ is positive in every ordering of K . If K has no

orderings, then every square-class σ is totally positive, by definition. Each signature of K gives rise to a signature of the Witt class $m\langle\sigma\rangle$, and these signatures are all positive since σ was chosen to be totally positive. We now additionally assume that the ground field K is hilbertian. Then, by [10] it follows that $m\langle\sigma\rangle$ is algebraic. Let $E|K$ be a minimal algebraic extension of degree $n \geq m$ for which the Witt class of the trace form $\langle E \rangle = m\langle\sigma\rangle$. We want to find lower bounds for n .

By [1], the polynomial $P_n(x)$ vanishes on the Witt class $\langle E \rangle$, whence

$$P_n(\langle E \rangle) = 0.$$

Hence $P_n(m\langle\sigma\rangle) = 0$. But $P_n(m\langle\sigma\rangle) = P_n^+(m\langle\sigma\rangle) + P_n^-(m\langle\sigma\rangle)$. Recalling that $P_n^+(x)$ is even, and that when an exponent j is even then $(m\langle\sigma\rangle)^j = m^j\langle 1 \rangle$ since an even power of the 1-dimensional class $\langle\sigma\rangle$ gives the multiplicative identity $\langle 1 \rangle$. Thus,

$$P_n^+(m\langle\sigma\rangle) = P_n^+(m).$$

Similarly, $P_n^-(x)$ is odd, and raising $m\langle\sigma\rangle$ to an odd power j gives $m^j\langle\sigma\rangle$. Hence,

$$P_n^-(m\langle\sigma\rangle) = P_n^-(m) \cdot \langle\sigma\rangle.$$

Recalling that $P_n^-(m) = -P_n^+(m)$ from Lemma 3.1 gives

$$P_n(m\langle\sigma\rangle) = P_n^+(m) \cdot (\langle 1 \rangle - \langle\sigma\rangle).$$

Combining this with Lemma 3.4 gives a formula for $P_n(m\langle\sigma\rangle)$. But this polynomial vanishes at $m\langle\sigma\rangle$, so

Lemma 3.5. *When $m\langle\sigma\rangle$ has algebraic rank $n \geq m$, then*

$$(-1)^{n+1} \cdot \frac{m}{2} \cdot \frac{(n+m)!}{m!} \cdot (\langle 1 \rangle - \langle\sigma\rangle) = 0 . \quad \square$$

In the next section, these lemmas will be used to obtain the main result.

3.2 The Main Result

Lemma 3.5 of the previous section leads to the first formulation of the main result.

The integer $(-1)^{n+1} \cdot \frac{m}{2} \cdot \frac{(n+m)!}{m!}$ can be written as an odd integer times a power of 2 : we write

$$(-1)^{n+1} \cdot \frac{m}{2} \cdot \frac{(n+m)!}{m!} = c \cdot 2^{R(n,m)}$$

where c is an odd integer.

Theorem 3.6. *When $m\langle\sigma\rangle$ has algebraic rank $n \geq m$, then*

$$py_K(\sigma) \leq 2^{R(n,m)}$$

where $R(n, m)$ is defined above.

Proof. By Lemma 3.5, $\langle 1, -\sigma \rangle$ has finite additive order dividing $c \cdot 2^{R(n,m)}$. By Theorem 6.4,(i), of [9], any Witt class with finite additive order has 2-power order. Let 2^j denote the exact additive order of $\langle 1, \sigma \rangle$. So 2^j divides $c \cdot 2^{R(n,m)}$, and since c is odd, this means that 2^j divides $R(n, m)$. Hence

$$2^j \leq 2^{R(n,m)} .$$

By Proposition 1.3 of Chapter 11 of [7], the additive order of $\langle 1, -\sigma \rangle$ is the smallest 2-power greater than or equal to the pythagoras number $py_K(\sigma)$. So

$$py_K(\sigma) \leq 2^j \leq 2^{R(n,m)}$$

proving Theorem 3.6 . $\square$

It is desirable to simplify the expression for $R(n, m)$, this being the exact exponent of 2 in the factorization of $(-1)^{n+1} \cdot \frac{m}{2} \cdot \frac{(n+m)!}{m!}$. Restated,

$$R(n, m) = ord_2[(-1)^{n+1} \cdot \frac{m}{2} \cdot \frac{(n+m)!}{m!}] .$$

Thus, $R(n, m) = \text{ord}_2(m) - 1 + \text{ord}_2[(n + m)!] - \text{ord}_2[m!]$. By Theorem 2.1, $\text{ord}_2[(n + m)!] = n + m - d(n + m)$ and $\text{ord}_2[m!] = m - d(m)$. Putting this together shows that $R(n, m)$ is given by

$$\text{ord}_2(m) - 1 + n + m - d(n + m) - [m - d(m)] = \text{ord}_2(m) - 1 + n - d(n + m) + d(m).$$

Thus the theorem above can be restated as the following main theorem:

Theorem 3.7. *When $m\langle\sigma\rangle$ has finite algebraic rank $n \geq m$, then*

$$py_K(\sigma) \leq 2^{R(n, m)}$$

where $R(n, m) = \text{ord}_2(m) - 1 + n - d(n + m) + d(m)$. $\square$

Two special cases of this theorem are singled out for their independent interest: The case when $\langle m\sigma \rangle$ has algebraic rank $n = m$, and the case when $m = 1$.

Corollary 3.8. *When $\langle\sigma\rangle$ has finite algebraic rank $n = m$, then*

$$py_K(\sigma) \leq 2^{m + \text{ord}_2(m) - 1}.$$

Proof. Since $n = m$ then $R(n, m) = \text{ord}_2(m) - 1 + n - d(n + m) + d(m)$ becomes $R(m, m) = \text{ord}_2(m) - 1 + m$ because $d(n + m) = d(2m) = d(m)$. $\square$

In the second interesting special case, when $m = 1$, it is not necessary to assume $n \geq m$ when $m = 1$ since automatically $n \geq 1$.

Corollary 3.9. *When $\langle\sigma\rangle$ has finite algebraic rank n , then*

$$py_K(\sigma) \leq 2^{n - d(n+1)}$$

where $d(n + 1)$ denotes the sum of the coefficients in the binary expansion of $n + 1$.

Proof. Simply observe that $R(n, 1) = \text{ord}_2(1) - 1 + n - d(n + 1) + d(1)$, which equals $n - d(n + 1)$. $\square$

In [10], Scharlau and Krüskemper have given deep examples showing that there are forms having all signatures non-negative over a hilbertian field that do not have finite algebraic rank. In particular, the very strong result of Epkenhans stating that over a number field any form of rank not less than 4 having all signatures non-negative is isometric to a trace form does not generalize to arbitrary hilbertian fields. We wish to observe in passing that this non-generalization of Epkenhans' theorem easily follows from Corollary 3.9 .

Let $K = \mathbb{Q}(X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8, X_9)$ denote the function field in nine variables over $\mathbb{Q}$. Then K is hilbertian. Put

$$\sigma = X_1^2 + X_2^2 + X_3^2 + X_4^2 + X_5^2 + X_6^2 + X_7^2 + X_8^2 + X_9^2.$$

Then σ is a totally positive element of K . Corollary 2.4 of chapter 9 of [7] shows that $py_K(\sigma) = 9$. Then the form $q = \sigma x_1^2 + x_2^2 - x_3^2 + x_4^2 - x_5^2$ is a quadratic form of rank 5 over K and every signature of q is positive. The Witt class of q is just the Witt class $\langle \sigma \rangle$. If Epkenhans' result holds over K , then this form q is isometric to the trace form of a degree 5 extension of K . Hence $\langle \sigma \rangle$ has algebraic rank no greater than 5. But the corollary above shows that $9 = py_K(\sigma) \leq 2^{5-d(6)}$. But $5 - d(6) = 5 - 2 = 3$ and it is false that $9 \leq 2^3$. Thus Epkenhans' result does not generalize, at least without some change.

To end this section, it is worth observing that, for m fixed, the exponent $R(n, m)$ increases without bound as n increases. This follows simply from the definition:

$$R(n, m) = \text{ord}_2[(-1)^{n+1} \cdot \frac{m}{2} \cdot \frac{(n+m)!}{m!}]$$

since, for m fixed, the 2-order of $(n+m)!$ clearly increases without bound as n goes to infinity.

Lemma 3.10. *For m fixed*

$$\lim_{n \rightarrow \infty} R(n, m) = \infty. \quad \square$$

Chapter 4

Degree Three Forms

4.1 A Long Computation

This chapter is devoted to establishing the direct but somewhat involved computation of $P_n(\langle a, b, c \rangle)$ of an arbitrary rank-3 quadratic form. This is done to see whether the special case of rank 3 will lead to improved results. It turns out that it does not.

Theorem 4.1. *For $n \geq 3$ and odd, then*

$$P_n(\langle a, b, c \rangle) = \frac{(n+1)!}{8} \cdot T_n(\langle a, b, c \rangle)$$

where

$$T_n\langle a, b, c \rangle = 4\langle 1 \rangle - 2\langle a, b, c, -abc \rangle + \frac{(n+1)(n+4)}{2} \cdot \langle 1, -a \rangle \langle 1, -b \rangle \langle 1, -c \rangle$$

in the Witt ring $W(K)$.

Proof. Begin by writing

$$\langle a, b, c \rangle = \langle a \rangle \langle 1, ab \rangle + \langle c \rangle.$$

The piece $\langle 1, ab \rangle$ is a 1-fold Pfister form which we shall denote simply by $\wp$. So $\langle a, b, c \rangle = \langle a \rangle \wp + \langle c \rangle$. The reason we write $\langle a, b, c \rangle$ in terms of $\wp$ is that, by Lemma 2.2, $\wp^r = 2^{r-1}\wp$, and this feature will help us compute P_n .

So

$$P_n(\langle a, b, c \rangle) = P_n(\langle a \rangle \wp + \langle c \rangle) \tag{3}$$

which is the same as

$$P_n^+(\langle a \rangle \wp + \langle c \rangle) + P_n^-(\langle a \rangle \wp + \langle c \rangle). \tag{4}$$

We will compute P_n^+ and P_n^- separately.

$$P_n^+(\langle a \rangle \wp + \langle c \rangle) = \sum_{j=1}^{\frac{n+1}{2}} s_{2j} (\langle a \rangle \wp + \langle c \rangle)^{2j}.$$

Expanding the inside with the binomial theorem, replacing the even-power terms $(\langle a \rangle \wp)^{2r}$ with $2^{2r-1} \wp$ and the odd-power terms $(\langle a \rangle \wp)^{2s-1}$ with $2^{2s-2} \wp \langle a \rangle$ via Lemma 1.2 of chapter 1 gives

$$P_n^+(\langle a \rangle \wp + \langle c \rangle) = \sum_{j=1}^{\frac{n+1}{2}} s_{2j} \left(\sum_{r=0}^{2j} \binom{2j}{r} (\langle a \rangle \wp)^r \langle c \rangle^{2j-r} \right).$$

Break the inner sum into three pieces, letting $r = 0$, then $r > 0$ even, and finally r odd. Putting this together gives

$$P_n^+(\langle a \rangle \wp + \langle c \rangle) = P_n^+(1) \langle 1 \rangle + \wp \cdot A_+ + A_- \wp \langle ac \rangle \quad (5)$$

where

$$A_+ = \sum_{j=1}^{\frac{n+1}{2}} s_{2j} \sum_{r=1}^j \binom{2j}{2r} 2^{2r-1} \quad (6)$$

and

$$A_- = \sum_{j=1}^{\frac{n+1}{2}} s_{2j} \sum_{s=1}^j \binom{2j}{2s-1} 2^{2s-2} \quad (7)$$

Similarly,

$$P_n^-(\langle a \rangle \wp + \langle c \rangle) = P_n^-(1) \langle c \rangle + B_+ \wp \langle c \rangle + B_- \wp \langle a \rangle \quad (8)$$

where

$$B_+ = \sum_{i=2}^{\frac{n+1}{2}} s_{2i-1} \sum_{r=1}^{i-1} \binom{2i-1}{2r} 2^{2r-1} \quad (9)$$

and

$$B_- = \sum_{i=1}^{\frac{n+1}{2}} s_{2i-1} \sum_{s=1}^i \binom{2i-1}{2s-1} 2^{2s-2}. \quad (10)$$

The expressions A_+ , A_- , B_+ and B_- are integers. The next step is to rewrite each of them as something recognizable. While not obvious, it will turn out that $A_+ = A_-$ (the B 's, however, are not equal).

The expression for A_+ comes from the basic relation $\wp^r = 2^{r-1}\wp$. Thus we should get a similar expression by computing $P_n^+(x+1)$ and then replacing x^r by $2^{r-1}x$. This suggests putting $x = 2$ and computing $P_n^+(3) = P_n^+(2+1)$. Following the steps outlined above gives

$$P_n^+(3) = P_n^+(1) + 2A_+ + 2A_-.$$

Changing a sign converts $3 = 2 + 1$ into $1 = 2 - 1$ and we compute

$$P_n^+(1) = P_n^+(2-1) = P_n^+(1) + 2A_+ - 2A_-.$$

Therefore

$$A_+ = A_-,$$

from which it further follows that

$$P_n^+(3) = P_n^+(1) + 4A_+.$$

Therefore

$$A_+ = A_- = \frac{P_n^+(3) - P_n^+(1)}{4}. \quad (11)$$

Combining this with the explicit values of $P_n^+(3)$ and $P_n^+(1)$ from Lemma 2.3 gives

$$A_+ = A_- = \frac{(n+1)!}{8} \cdot \frac{(n+1)(n+4)}{2}. \quad (12)$$

Now compute P_n^- at the inputs $3 = 2 + 1$ and $1 = 2 - 1$. This gives

$$P_n^-(3) = P_n^-(1) + 2B_+ + 2B_-$$

and

$$P_n^-(1) = -P_n^-(1) - 2B_+ + 2B_-.$$

Adding gives

$$P_n^-(3) + P_n^-(1) = 4B_-$$

so

$$B_- = \frac{P_n^-(3) + P_n^-(1)}{4}.$$

Subtracting gives

$$P_n^-(3) - P_n^-(1) = 2P_n^-(1) + 4B_+$$

so

$$P_n^-(3) - 3P_n^-(1) = 4B_+$$

hence

$$B_+ = \frac{P_n^-(3) - 3P_n^-(1)}{4}.$$

Recall from Lemma I:2 that for $1 \leq m \leq n$ that $P_n^-(m) = -P_n^+(m)$. Since we have $1 \leq 3 \leq n$ we have

$$B_- = -\frac{P_n^+(3) + P_n^+(1)}{4} \tag{13}$$

and

$$B_+ = -\frac{P_n^+(3) - 3P_n^+(1)}{4}. \tag{14}$$

Using (11) the B's can be written in terms of the A's as follows: B_- is given by

$$-\frac{P_n^+(3) + P_n^+(1)}{4} = -\frac{P_n^+(3) - P_n^+(1) + 2P_n^+(1)}{4} = -A_+ - \frac{P_n^+(1)}{2}$$

while B_+ is given by

$$-\frac{P_n^+(3) - 3P_n^+(1)}{4} = -\frac{P_n^+(3) - P_n^+(1) - 2P_n^+(1)}{4} = -A_+ + \frac{P_n^+(1)}{2}.$$

This finishes the computation of A_+ , A_- , B_+ , and B_- . Now return to the original problem of computing $P_n(\langle a, b, c \rangle)$. With (5)

$$P_n^+(\langle a, b, c \rangle) = P_n^+(1)\langle 1 \rangle + [\wp \cdot A_+] \cdot \langle 1, ac \rangle$$

and with (8) we find

$$P_n^-(\langle a, b, c \rangle) = P_n^-(1)\langle c \rangle + (B_+\wp\langle c \rangle + B_-\wp\langle a \rangle).$$

This latter expression can be written in terms of A_+ , which equals A_- , and P_n^+ as follows:

$$P_n^-(\langle a, b, c \rangle) = -P_n^+(1)\langle c \rangle + \frac{P_n^+(1)}{2}\wp\langle c \rangle - \frac{P_n^+(1)}{2}\wp\langle a \rangle - A_+\wp\langle a, c \rangle.$$

Now, $\wp = \langle 1, ab \rangle$, so $\wp\langle a \rangle = \langle a, b \rangle$ and $\wp\langle c \rangle = \langle c, abc \rangle$. Combining this via (3) shows that $P_n(\langle a, b, c \rangle)$ equals

$$P_n^+(1)\langle 1 \rangle + A_+\langle 1, ab, ac, bc \rangle - P_n^+(1)\langle c \rangle + \frac{P_n^+(1)}{2}\langle c, abc \rangle - \frac{P_n^+(1)}{2}\langle a, b \rangle - A_+\langle a, b, c, abc \rangle.$$

Factoring out A_+ shows that $P_n(\langle a, b, c \rangle)$ equals

$$P_n^+(1)(\langle 1, -c \rangle + \frac{P_n^+(1)}{2}\langle c, abc \rangle - \frac{P_n^+(1)}{2}\langle a, b \rangle + A_+\langle 1, -a \rangle\langle 1, -b \rangle\langle 1, -c \rangle).$$

Note that $A_+ = \frac{(n+1)!}{8} \cdot \frac{(n+1)(n+4)}{2}$ has a factor of $\frac{(n+1)!}{8}$ while $P_n^+(1) = \frac{(n+1)!}{2}$. We wish to show that $\frac{(n+1)!}{8}$ is a factor of the entire sum, so we replace $P_n^+(1)$ by its equivalent form $P_n^+(1) = \frac{4P_n^+(1)}{4}$ and we replace $\frac{P_n^+(1)}{2}$ by $\frac{P_n^+(1)}{2} = \frac{2P_n^+(1)}{4}$. Doing this shows $P_n(\langle a, b, c \rangle)$ equals

$$\frac{4P_n^+(1)}{4}\langle 1 \rangle - \frac{2P_n^+(1)}{4}\langle a, b, c, -abc \rangle + A_+\langle 1, -a \rangle\langle 1, -b \rangle\langle 1, -c \rangle.$$

Now replace $P_n^+(1)$ by $\frac{(n+1)!}{2}$ and A_+ by $\frac{(n+1)!}{8} \cdot \frac{(n+1)(n+4)}{2}$ and factor out $\frac{(n+1)!}{8}$ to obtain final form:

$$P_n(\langle a, b, c \rangle) = \frac{(n+1)!}{8} \cdot T_n\langle a, b, c \rangle$$

where

$$T_n\langle a, b, c \rangle = 4\langle 1 \rangle - 2\langle a, b, c, -abc \rangle + \frac{(n+1)(n+4)}{2} \cdot \langle 1, -a \rangle\langle 1, -b \rangle\langle 1, -c \rangle. \quad \square$$

The discriminant of $\langle a, b, c \rangle$ is the square-class $d = (-1)^3 abc = -abc$. The geometric rank of $\langle a, b, c \rangle$ is 1 if the form is isotropic, and 3 otherwise.

Lemma 4.2. *The form $\langle a, b, c \rangle$ has geometric rank 3 if and only if $-ab$ is not a square in K^* and $-ac$ is not a norm from $K(\sqrt{-ab})|K$.*

Proof. Suppose $\langle a, b, c \rangle$ is isotropic. Then $\langle a, b, c \rangle$ represents 0 so $\langle 1, ab, ac \rangle$ represents 0, so $\langle 1, ab \rangle$ represents $-ac$. Thus, $-ac$ is a norm from $K(\sqrt{-ab})|K$. This proves: If $-ac$ is not a norm from $K(\sqrt{-ab})|K$, then $\langle a, b, c \rangle$ is anisotropic, so it has geometric rank 3. This proves sufficiency. For necessity, we will prove that if either $-ab = 1$ or if $-ac$ is a norm from $K(\sqrt{-ab})|K$ then $\langle a, b, c \rangle$ is isotropic. If $-ac$ is a norm, then $-ac$ is represented by $\langle 1, ab \rangle$ so $\langle a, ab, ac \rangle$ represents 0 so $\langle a, b, c \rangle$ is isotropic. Finally, suppose $-ab = 1$ in K^*/K^{*2} . Then $-a = b$. Since $\langle 1, -1, ac \rangle$ is certainly isotropic, then $\langle a, -a, c \rangle$ is isotropic, and this form is $\langle a, b, c \rangle$. $\square$

The next lemma is (III.3.6) of [2].

Lemma 4.3. *If the algebraic rank of $\langle a, b, c \rangle$ is 3, then either $d = -1 \in K^*/K^{*2}$ and $\langle a, b, c \rangle = 3\langle 1 \rangle$ in $W(K)$, or $d \neq -1 \in K^*/K^{*2}$ and $\langle a, b, c \rangle = \langle 1 \rangle - 2(\langle 1 \rangle - \langle d \rangle)$. $\square$*

Now suppose that $\langle a, b, c \rangle$ has algebraic rank $n \geq 3$. Note that necessarily n is odd. Then the form is a zero of the polynomial

$$P_n(x) = \prod_{k=0}^n (x - k).$$

Our next chore is to actually compute this product when $x = \langle a, b, c \rangle$.

Since $P_n(\langle a, b, c \rangle) = 0$, then we immediately obtain:

Corollary 4.4. *If $\langle a, b, c \rangle$ has algebraic rank $n \geq 3$, then in $W(K)$ the Witt class $T_n(\langle a, b, c \rangle)$ has finite additive order dividing the maximum 2-power in $\frac{(n+1)!}{8}$. $\square$*

As an application of this corollary, we now prove

Corollary 4.5. *Let the square-class $a \in K^*/K^{*2}$ be totally positive, and let 2^u be least power of 2 for which the pythagoras number of a satisfies $py_K(a) \leq 2^u$. If $\langle a, a, a \rangle$ has finite algebraic rank then 2^u divides $\frac{(n+3)!}{4}$.*

Proof. Consider the form $\langle a, a, a \rangle$. The discriminant is $d = -a^3 = -a$. The form $\langle a, a, a \rangle$ is algebraic of algebraic rank $n \geq 3$. Then by Lemma 2.2 on Pfister forms we have

$$(\langle 1, -a \rangle)^3 = 2^2 \langle 1, -a \rangle.$$

Thus

$$T_n(3\langle a \rangle) = 4\langle 1 \rangle - 2\langle a, a, a, -a \rangle + \frac{(n+1)(n+4)}{2}(\langle 1, -a \rangle)^3.$$

But $\langle a, -a \rangle$ is 0 in $W(K)$, so $T_n\langle a, a, a \rangle$ is equal to

$$4\langle 1 \rangle - 4\langle a \rangle + \frac{(n+1)(n+4)}{2}4\langle 1, -a \rangle = 4\langle 1, -a \rangle + (n+1)(n+4) \cdot 2\langle 1, -a \rangle.$$

Factoring out $\langle 1, -a \rangle$ and simple algebra then gives

$$T_n(3\langle a \rangle) = 2(n+2)(n+3)\langle 1, -a \rangle.$$

Finally, $P_n(\langle a, a, a \rangle) = \frac{(n+1)!}{8} \cdot T_n(\langle a, a, a \rangle)$ is given by

$$\frac{(n+1)!}{8} 2(n+2)(n+3)\langle 1, -a \rangle = \frac{(n+3)!}{4} \langle 1, -a \rangle = 0.$$

Thus the additive order of $\langle 1, -a \rangle$, which by Proposition 1.3 of Chapter 11 of [7] is precisely the 2^u in the statement of the lemma, divides $\frac{(n+3)!}{4}$. $\square$

References

- [1] P. Beaulieu, T. Palfrey, The Galois number, *Mathematische Annalen*, 309, (1997), 81-96.
- [2] P. E. Conner and R. Perlis, *A survey of trace forms of algebraic number fields*, Pure Mathematics, 2, World Scientific Publishing, 1984.
- [3] M. Epkenhans, On trace forms of algebraic number fields, *Archiv der Mathematik*, 60, No. 6, (1993), 527-529.
- [4] M. Fried, M. Jarden, *Field Arithmetic*, *Ergebnisse der Math.* series 3, vol 11, Springer-Verlag, 1986.
- [5] J. Hurrelbrink, Annihilating polynomials for group rings and Witt rings, *Canadian Math. Bull.*, 32, (1989), 412-416.
- [6] M. Krüskemper, Algebraic number field extensions with prescribed trace form, *Journal of Number Theory*, 40, (1992), 120-124.
- [7] T. Y. Lam, *The algebraic theory of quadratic forms*, W. A. Benjamin, 1973.
- [8] A. Pfister, *Quadratic forms with applications to algebraic geometry and topology*, Cambridge University Press, London Mathematical Society Lecture Note Series 217, 1995.
- [9] W. Scharlau, *Quadratic and hermitian forms*, *Grundlehren der mathematischen Wissenschaften*, 270, Springer-Verlag, 1985.
- [10] W. Scharlau, M. Krüskemper, On positive quadratic forms, *Bull. Soc. Math. Belg*, 20 (1988) 2, ser. A, 255-280.
- [11] O. Taussky-Todd, The discriminant matrices of an algebraic number field, *J. London Math. Soc.* 43 (1968), 152-154.
- [12] E. Witt, Theorie der quadratischen Formen in beliebigen Körpern, *J. reine angew. Math.*, 176, (1937), 31-44.

Vita

Sidney Taylor Hawkins was born in 1938, one year after the Witt ring was introduced to the world. His parents were Joseph D. Hawkins, Sr., of Monroe, Louisiana, and Mrs. Odalie Elizabeth Taylor Hawkins, of St. Louis, Missouri. He was raised on a farm near Monroe. He earned a bachelor of science degree in mathematics from Grambling State University in 1973. In 1975 he earned a master of science degree in mathematics from Louisiana Tech. From 1975 until 1988 he taught math at Grambling and Dillard University. He taught in the Math Department of Xavier University, New Orleans, from 1988 until 1995. Beginning in 1991 he concurrently took classes at Tulane University where he earned a second master's degree in 1995. From 1995 until 1999, he pursued doctoral studies in mathematics at Louisiana State University. He anticipates receiving the degree of Doctor of Philosophy in mathematics in May, 1999.

DOCTORAL EXAMINATION AND DISSERTATION REPORT

Candidate: Sidney Taylor Hawkins

Major Field: Mathematics

Title of Dissertation: Inequalities between Pythagoras Numbers and Algebraic Ranks in Witt Rings of Fields

Approved:

Robert Perlis

Major Professor and Chairman

William W. Sawyer

Dean of the Graduate School

EXAMINING COMMITTEE:

P. J. ...

B. D. ...

Dr. G. ...

J. Humelbrink

John Gregory Houg

Date of Examination:

March 26, 1999

IMAGE EVALUATION TEST TARGET (QA-3)

APPLIED IMAGE, Inc
1653 East Main Street
Rochester, NY 14609 USA
Phone: 716/482-0300
Fax: 716/288-5989

© 1993, Applied Image, Inc., All Rights Reserved