INFORMATION TO USERS

This was produced from a copy of a document sent to us for microfilming. While the most advanced technological means to photograph and reproduce this document have been used, the quality is heavily dependent upon the quality of the material submitted.

The following explanation of techniques is provided to help you understand markings or notations which may appear on this reproduction.

1. The sign or "target" for pages apparently lacking from the document photographed is "Missing Page(s)". If it was possible to obtain the missing page(s) or section, they are spliced into the film along with adjacent pages. This may have necessitated cutting through an image and duplicating adjacent pages to assure you of complete continuity.

2. When an image on the film is obliterated with a round black mark it is an indication that the film inspector noticed either blurred copy because of movement during exposure, or duplicate copy. Unless we meant to delete copyrighted materials that should not have been filmed, you will find a good image of the page in the adjacent frame.

3. When a map, drawing or chart, etc., is part of the material being photographed the photographer has followed a definite method in "sectioning" the material. It is customary to begin filming at the upper left hand corner of a large sheet and to continue from left to right in equal sections with small overlaps. If necessary, sectioning is continued again—beginning below the first row and continuing on until complete.

4. For any illustrations that cannot be reproduced satisfactorily by xerography, photographic prints can be purchased at additional cost and tipped into your xerographic copy. Requests can be made to our Dissertations Customer Services Department.

5. Some pages in any document may have indistinct print. In all cases we have filmed the best available copy.

University
Microfilms
International

300 N. ZEEB ROAD, ANN ARBOR, MI 48106
18 BEDFORD ROW, LONDON WC1R 4EJ, ENGLAND

8106176

LEEP, DAVID BENJAMIN

COMMON VALUE PROPERTIES OF QUADRATIC FORMS

The University of Michigan PH.D. 1980

University
Microfilms
International 300 N. Zeeb Road, Ann Arbor, MI 48106

COMMON VALUE PROPERTIES OF QUADRATIC FORMS

by
David Benjamin Leep

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
1980

Doctoral Committee:

Professor D.J. Lewis, Chairman
Assistant Professor Krishnaswami Alladi
Professor Melvin Hochster
Professor James S. Milne
Professor Chia-Shun Yih

RULES REGARDING THE USE OF

MICROFILMED DISSERTATIONS

Microfilmed or bound copies of doctoral dissertations submitted to The University of Michigan and made available through University Microfilms International or The University of Michigan are open for inspection, but they are to be used only with due regard for the rights of the author. Extensive copying of the dissertation or publication of material in excess of standard copyright limits, whether or not the dissertation has been copyrighted, must have been approved by the author as well as by the Dean of the Graduate School. Proper credit must be given to the author if any material from the dissertation is used in subsequent written or published work.

ACKNOWLEDGEMENTS

I would like to thank Professor D.J. Lewis for his support and encouragement throughout my stay at The University of Michigan. I am very grateful for the many suggestions and improvements he made during the writing of this dissertation. Professor D.B. Shapiro also played an important role in the development of this work. Our many conversations helped clarify the ideas contained in this work. Peggy Lubahn has done an excellent job of typing this dissertation. Her patience and diligence are greatly appreciated.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS. ii

INTRODUCTION. 1

CHAPTER

I. PIECEWISE EQUIVALENCE RELATIONS. 12

II. COMMON VALUE PROPERTIES OF QUADRATIC FORMS OVER NUMBER FIELDS. 30

III. GALOIS THEORY AND COMMON VALUE PROPERTIES OVER NUMBER FIELDS. 69

IV. FIELDS WITH FINITE HASSE NUMBER. 99

BIBLIOGRAPHY. 127

INTRODUCTION

The study of quadratic forms over fields leads to many extremely difficult questions that can be answered completely only if additional structure is imposed on the field.

Let F be a field of characteristic not 2, $\dot{F} = F - \{0\}$, and let F^2 be the nonzero squares of F. A famous theorem due to Witt [Wi, Satz 7] states that if α and β are two isometric quadratic forms defined over F, then there exists a sequence $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_m = \beta$ such that for each $i = 0, 1, \ldots, m-1$, if $\alpha_i = \langle c_1, \ldots, c_n \rangle$ and $\alpha_{i+1} = \langle d_1, \ldots, d_n \rangle$ then for some j, k, $\langle c_j, c_k \rangle \cong \langle d_j, d_k \rangle$ and $c_i = d_i$ for all $i \neq j,k$ (where $\cong$ means 'isometric to').

Throughout this introduction we assume the reader is familiar with terminology and notation used in this subject. They are listed at the end of the introduction for the reader's convenience.

We consider a problem in Chapter I suggested by D. Shapiro that generalizes Witt's procedure. Let G be a multiplicative subgroup of $\dot{F}$ that contains F^2. If $\alpha = \langle a_1, \ldots, a_n \rangle$ and $\beta = \langle b_1, \ldots, b_n \rangle$, we say

α and β are strictly G-equivalent, $\alpha \tilde{G} \beta$, if $a_i b_i \in G$ for $i = 1, 2, \ldots, n$. We say α is G-equivalent to β, $\alpha \overset{\approx}{G} \beta$, if there exists a sequence $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_m = \beta$ such that for $i = 0, 1, \ldots, m-1$, either $\alpha_i \cong \alpha_{i+1}$ or $\alpha_i \tilde{G} \alpha_{i+1}$.

Let $\mathcal{I}_G$ be the ideal in the Witt ring $W(F)$ generated by all forms $\langle 1, -g \rangle$, $g \in G$. It follows that $\alpha \overset{\approx}{G} \beta$ implies $\alpha \equiv \beta \pmod{\mathcal{I}_G}$ and $\dim \alpha = \dim \beta$. We say G has piecewise equivalance or simply G has PE if $\alpha \equiv \beta \pmod{\mathcal{I}_G}$ and $\dim \alpha = \dim \beta$ imply $\alpha \overset{\approx}{G} \beta$. It is usually very difficult to decide whether G has PE. We concentrate in Chapter I on binary PE, i.e., when $\dim \alpha = \dim \beta = 2$.

Let $K = F(\sqrt{G})$ where $F(\sqrt{G})$ is the minimal field containing all square roots of elements in G. It is always true that $\mathcal{I}_G \subseteq \ker(W(F) \to W(K))$ where $W(F) \to W(K)$ is the induced map of the Witt rings of F and K. A subgroup G has the kernel property if $\mathcal{I}_G = \ker(W(F) \to W(K))$. We say G has the kernel property for 4-dimensional forms if 4-dimensional forms in $\ker(W(F) \to W(K))$ lie in $\mathcal{I}_G$. A field is 1-amenable if every subgroup G of $\dot{F}$ has the kernel property. It is important to know if a field is 1-amenable, since it was shown in [ELW_1] that if F is 1-amenable then Pfister's conjecture on the Clifford invariant holds for F. It has been shown in [ELW_1] and [ELW_2] that all global fields, p-adic fields and fields

with Hasse number ≤ 2 are 1-amenable. The rational function field $\mathbb{Q}(x)$ is not 1-amenable. For general fields, very little is known.

We let $D_F(\alpha) = D(\alpha)$ be the nonzero values of F represented by α over F and we let $\tilde{D}^G(\alpha) = \{a \in \dot{F} | \alpha \underset{G}{\tilde{\simeq}} \langle a \rangle \perp \alpha' \text{ for some } \alpha' \text{ defined over } F\}$. We show in (1.14) that a subgroup G has binary PE if and only if every 2-fold Pfister form $\langle\langle -a, -b \rangle\rangle \in \mathcal{I}_G$ has $b \in \tilde{D}^G(\langle 1, -a \rangle)$. In (1.15) we show $\tilde{D}^G(\langle 1, a \rangle)$ is the group generated by the groups $\{D(\langle 1, ag \rangle)\}$ where $g \in G$. It is always true that $\prod_{g \in G} D_F(\langle 1, -ag \rangle) \subseteq \dot{F} \cap D_K(\langle 1, -a \rangle)$ where $K = F(\sqrt{G})$. In (1.16) we see that these latter two groups are equal if and only if G has binary PE and the kernel property for 4-dimensional forms.

There is a common value property closely related to binary PE. An extension K/F satisfies CV(m,n) if for all forms α, β defined over F of dimensions m, n, respectively, whenever α and β represent over K a common value, then they represent over K a common value in $\dot{F}$. That is, $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$ implies $D_K(\alpha) \cap D_K(\beta) \cap \dot{F} \neq \emptyset$. In (1.24) we show that every subgroup G of $\dot{F}$ has binary PE and the kernel property for 4-dimensional forms if and only if every finite multiquadratic extension K/F satisfies CV(2,2) where $K = F(\sqrt{G})$.

In Chapters II and III, we specialize to number fields and characterize those extensions K/F that satisfy CV(m,n)

as well as other common value properties defined there. We mention a few of those results below.

Let K/F be a finite extension of number fields and let $E(K/F)$ be the set of primes p of F for which $[K_p:F_p]$ is even for each prime P of K dividing p. We say $E(K/F)$ is a global square set if $d \in F_p^2$ for each $p \in E(K/F)$ implies $d \in F^2$. We show in (2.14) that K/F satisfies $CV(2,2)$ if and only if $E(K/F)$ is a global square set. We show in (2.26) that K/F always satisfies $CV(m,n)$ when $(m, n) \neq (2, 2)$.

An extension K/F is excellent if for all forms α defined over F which are isotropic over K, there exists a form β defined over F such that $\alpha \cong_K H \perp \beta$, where H is the form $\langle 1, -1\rangle$. If K/F satisfies $CV(2,2)$ then it is easy to show K/F is excellent for 4-dimensional forms [(2.8)]. We show in (2.14) that the converse holds if K/F is a finite extension of number fields. This is a surprising result that is known not to hold for general fields, even for quadratic extensions. Later in (2.27) we show that if a finite extension of number fields is excellent for 4-dimensional forms, then it is excellent for all forms. Excellent extensions were introduced in [ELW_1] as an aid to studying many open problems in quadratic form theory. See [ELW_1] for a discussion of these problems.

We also study the strong common value property SCV. An extension K/F satisfies $SCV(m,n)$ if for all ordered

pairs (α, β) of forms defined over F of dimensions m, n respectively, whenever $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$, then $D_F(\alpha) \cap D_K(\beta) \neq \emptyset$. Note that SCV is not a symmetric property whereas CV is symmetric. In (2.5) we give a local characterization of this property over number fields when $(m, n) = (2, 2)$. If $n \geq 3$, we show in (2.25) that a finite extension of number fields always satisfies SCV(m,n). The property SCV(m,2) with $m \geq 3$ only holds for certain extensions of number fields. We give a local characterization of such extensions in (2.28).

In Chapter III, we relate the common value property CV(2,2) to Galois theory. Let L be a finite normal extension of a number field F that contains K and let $G = \mathrm{Gal}(L/F)$. We find sufficient conditions on G so that K/F satisfies CV(2,2). Let H be the subgroup of G that fixes K, J a Sylow 2-group of H, and J' a Sylow 2-group of G containing J. We say $E(K/F)$ is a strong global square set if $E(K/F) - T$ is a global square set for every finite set T of primes in F. Consider the following five statements.

1) For each subgroup N of index 2 in G, $J' \notin \bigcup_{g \in G} g^{-1}Jg \cup N$, or if no such N exists, $J' \notin \bigcup_{g \in G} g^{-1}Jg$.

2) $E(K/F)$ is a strong global square set.

3) $E(K/F)$ is a global square set.

4) $E(K/F)$ is an infinite set.

5) $J' \not\subseteq \bigcup_{g \in G} g^{-1}Jg$.

We show in (3.1) that 1) $\Longleftrightarrow$ 2) $\not\Longrightarrow$ 3) $\not\Longrightarrow$ 4) $\Longleftrightarrow$ 5). Examples are constructed showing these nonimplications. The connection with Galois theory is through the Frobenius automorphism $\sigma(L/F, P)$ where P is a prime in L that divides a finite prime p in F which is unramified in L . We show in (3.4) that if p is unramified in L , then $p \in E(K/F)$ if and only if $\sigma(L/F, P)$ is an even element of G [see definition (3.3)].

If K contains a normal extension K' of F such that $[K':F]$ is even, then we show in (3.24) that $E(K/F)$ is a strong global square set. If $[K:F] = 2^n$ for some $n \geq 1$ then we show in (3.25) that $E(K/F)$ is a strong global square set.

In Chapter IV, we study fields F that have finite Hasse number $\tilde{u}(F)$, where $\tilde{u}(F)$ is the smallest integer n such that every form α of degree $> n$ that is indefinite with respect to every ordering of F is isotropic over F . If a field F has finite Hasse number, then F satisfies the ED property (see [Wr_2]). This means every form α can be effectively diagonalized in the sense that there exists a diagonalization $\langle a_1, \ldots, a_n \rangle$ of α such

that $W_F(a_i) \subseteq W_F(a_{i+1})$, $1 \leq i \leq n-1$, where $W_F(a_i)$ is the set of orderings of F for which $a_i < 0$. An ED field satisfies the strong approximation property SAP. This means given any two disjoint closed sets A , B in the space $X(F)$ of orderings of F (defined in Chapter IV), there exists $a \in \dot{F}$ such that $a > 0$ in each ordering of A and $a < 0$ in each ordering of B (see $[Wr_2]$).

We determine sufficient conditions for extensions of the above-mentioned fields to be excellent. In (4.4) we show that if F is an ED field and K is an extension of F with $\tilde{u}(K) = n$, then K/F is excellent if and only if K/F is excellent for forms of dimension $\leq n+1$.

Let $\tilde{u}(F) \leq 2$. In (4.7) we show F is 1-amenable and every finite multiquadratic extension K of F is excellent. This result has already appeared in $[ELW_2]$ with a slightly different proof.

Using a result from $[ELW_2]$ we show in (4.9) that if $\tilde{u}(F) = n$, then a finite multiquadratic extension K/F is excellent if and only if K/F is excellent for forms of dimension $\leq n$.

If $\tilde{u}(F) = 4$, we show in (4.10) that F is 1-amenable if and only if F is 1-amenable for 4-dimensional forms. This in turn is equivalent to the condition that each finite multiquadratic extension K/F is excellent.

A field F is linked if the quaternion algebras defined over F form a subgroup of the Brauer group of F .

It is shown in [E] that a linked field F satisfies $\tilde{u}(F) \leq 8$ and the converse holds if $\tilde{u}(F) \leq 4$. In (4.15) we show a linked field F is 1-amenable if and only if F is 1-amenable for 2-fold and 3-fold Pfister forms.

In (4.11) we show that if F satisfies the strong approximation property (SAP) and $\tilde{u}(K) < \infty$, then K/F satisfies CV(m,n) whenever $m,n \geq \tilde{u}(K)$. If F satisfies ED and $\tilde{u}(K) < \infty$, then we show K/F satisfies SCV(m,n) whenever $n \geq \tilde{u}(K)$, $m \geq 1$.

Let $K = F(\sqrt{G})$ be a finite multiquadratic extension of F. Let $I(F)$ be the ideal of $W(F)$ generated by even dimensional forms. Suppose F satisfies SAP and $I^n(F)$ is torsion free for some $n \geq 2$. If $\alpha \in I^n(F)$ and α is hyperbolic over K, we show in (4.14) that $\alpha \in \mathcal{N}_G$.

If F is a p-adic field, we show in (4.16) that every finite extension K/F is excellent, F is 1-amenable, and K/F satisfies CV(m,n) for all (m, n).

Chapter I consists of a number of results from joint research with D. Shapiro on piecewise equivalence. That research will be published jointly in a separate paper. We include Chapter I in this thesis since it motivates the research reported in the later chapters.

Notations, basic conventions, and terminology. What follows is a list of basic terms that will be used in this work. More details can be found in [L].

$\alpha = \langle a_1, \ldots, a_n \rangle$ is the quadratic form $a_1x_1^2 + \cdots + a_nx_n^2$.

form = quadratic form .

$\alpha \cong_F \beta$ means α is isometric to β over the field F . If the field F is understood, we write $\alpha \cong \beta$.

dim α = dimension of α . If $\alpha = \langle a_1, \ldots, a_n \rangle$, then dim $\alpha = n$.

"anisotropic over F" means there are no nontrivial zeros over F .

"isotropic over F" means there exists a nontrivial zero over F .

$c\alpha = \langle ca_1, \ldots, ca_n \rangle$, $c \in \dot{F}$.

$-\beta = (-1)\beta$.

$\alpha \perp \beta$ = orthogonal sum of two forms. If $\beta = \langle b_1, \ldots, b_s \rangle$, then $\alpha \perp \beta = \langle a_1, \ldots, a_n, b_1, \ldots, b_s \rangle$.

$\alpha \otimes_F \beta$ = tensor product over F of two forms. $\alpha \otimes_F \beta =$

$\langle \ldots, a_i b_j, \ldots \rangle$. The dimension of $\alpha \otimes_F \beta$ is $\dim \alpha \cdot \dim \beta$.

$\det \alpha = a_1 \cdots a_n \, F^2 \in \dot{F}/\dot{F}^2$. We write $\det \alpha = a_1 \cdots a_n$ but it is understood that $\det \alpha$ is a square class of $\dot{F}$, not an element of $\dot{F}$.

$d(\alpha)$ = discriminant of $\alpha = (-1)^{\frac{n(n-1)}{2}} \det \alpha$ where $\dim \alpha = n$.

$H = \langle 1, -1 \rangle$ = the hyperbolic plane.

"α is hyperbolic" means $\alpha \cong H \perp \cdots \perp H$.

$D_F(\alpha) = \{a \in \dot{F} \mid \alpha$ represents a over $F\}$. $D(\alpha) = D_F(\alpha)$ if the field F is understood. Note that $D_F(\alpha)$ consists of the nonzero values of F represented by α over F .

$W(F)$ = Witt ring of F . We say $\alpha = \beta$ in $W(F)$ if the anisotropic parts of α and β are isometric over F . If $\alpha = \beta$ in $W(F)$ and $\dim \alpha = \dim \beta$, then $\alpha \cong_F \beta$. If $\alpha = \beta$ in $W(F)$ and $\dim \alpha$, $\dim \beta$ are even, then $d(\alpha) = d(\beta)$.

If $F \subseteq K$, then $W(F) \to W(K)$ is the map that sends α to $\alpha \otimes_F K$, i.e., α is simply considered as a form over K by extension of scalars.

The n-fold Pfister form $\langle\langle a_1, \ldots, a_n \rangle\rangle$ =

$\langle 1, a_1 \rangle \otimes \cdots \otimes \langle 1, a_n \rangle$. For example, $\langle\langle a, b \rangle\rangle = \langle 1, a, b, ab \rangle$.

$I(F)$ = the ideal of $W(F)$ generated by all even dimensional forms. The ideal $I^n(F)$ is generated by all n-fold Pfister forms.

A p-adic field F is a complete field with respect to a discrete valuation having a finite residue class field $\overline{F}$.

Springer's Theorem [L, p. 198]. Let K/F be a finite extension such that $[K:F]$ is odd. If α is a quadratic form defined over F such that α is anisotropic over F , then α is anisotropic over K .

CHAPTER I

PIECEWISE EQUIVALENCE RELATIONS

Let F be a field of characteristic not 2. Let $\dot{F}$ denote the group of nonzero elements of F and let F^2 be the subgroup of squares in $\dot{F}$. All quadratic forms considered in this work are nonsingular. (The zero quadratic form $\langle 0 \rangle$ is considered nonsingular.) We shall assume that each form has been diagonalized.

Let α and β be two quadratic forms defined over F such that $\alpha \cong \beta$. A well-known theorem due to Witt (see [Wi, Satz 7] or [L, p. 21]) asserts that there exists a sequence of diagonal forms $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_m = \beta$ such that for each i, $0 \leq i \leq m-1$, if $\alpha_i = \langle c_1, \ldots, c_n \rangle$ and $\alpha_{i+1} = \langle d_1, \ldots, d_n \rangle$ then for some j and k, $\langle c_j, c_k \rangle \cong \langle d_j, d_k \rangle$ and $c_i = d_i$ for all $i \neq j,k$.

In this work, by a subgroup G we will always mean a subgroup of $\dot{F}$ which contains F^2. The purpose of this chapter is to consider a generalization of Witt's result where forms in the sequence above can be altered by elements of a subgroup G of $\dot{F}$. First we make some definitions.

(1.1) Definition. Let $\alpha = \langle a_1, \ldots, a_n \rangle$ and $\beta = \langle b_1, \ldots, b_n \rangle$ be forms defined over F and let G be a subgroup of $\dot{F}$. Then α and β are strictly G-equivalent, written $\alpha \stackrel{\sim}{G} \beta$, if $a_i b_i \in G$ for each i, $1 \leq i \leq n$.

Clearly $\stackrel{\sim}{G}$ is an equivalence relation. If $\alpha \stackrel{\sim}{G} \beta$, then it is easy to see that there exists a sequence $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_m = \beta$ such that for each i, $0 \leq i \leq m-1$, if $\alpha_i = \langle c_1, \ldots, c_n \rangle$ and $\alpha_{i+1} = \langle d_1, \ldots, d_n \rangle$ then for some j, $c_j d_j \in G$ and $c_i = d_i$ for all $i \neq j$.

(1.2) Definition. Two forms α and β defined over F are G-equivalent, written $\alpha \stackrel{\approx}{G} \beta$, if there exists a sequence $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_m = \beta$ such that for each i, $0 \leq i \leq m-1$, either $\alpha_i \cong \alpha_{i+1}$ or $\alpha_i \stackrel{\sim}{G} \alpha_{i+1}$.

Thus G-equivalence is the equivalence relation generated by isometry and strict G-equivalence. It follows from above that if $\alpha \stackrel{\approx}{G} \beta$, we could choose a sequence as in (1.2) where at most a binary subform is altered in each step.

(1.3) Notation. Let G be a subgroup of $\dot{F}$. We let $\mathfrak{o}_G$ be the ideal in the Witt ring $W(F)$ generated by all the forms $\langle 1, -g \rangle$, $g \in G$.

(1.4) Proposition. Let α, β be forms defined over F and let G be a subgroup of $\dot{F}$. If $\alpha \equiv \beta \pmod{\sigma_G}$ then $\dim \alpha \equiv \dim \beta \pmod 2$. If in addition $\dim \alpha$, $\dim \beta$ are even, then $d(\alpha)d(\beta) \in G$.

Proof: Since $\alpha \perp -\beta \in \sigma_G \subseteq I(F)$, it follows $\dim(\alpha \perp -\beta)$ is even, so $\dim \alpha \equiv \dim \beta \pmod 2$.

Since $d(\langle 1, -g\rangle) = g$ for each $g \in G$ and since $d(\gamma_1 \perp \gamma_2) = d(\gamma_1)d(\gamma_2)$ when $\gamma_1, \gamma_2 \in I(F)$, it follows that $d(\alpha \perp -\beta) \in G$. If $\dim \alpha$, $\dim \beta$ are even, then $d(\alpha \perp -\beta) = d(\alpha)d(-\beta) = d(\alpha)d(\beta) \in G$.

(1.5) Notation. Let G be a subgroup of $\dot{F}$. We let $F(\sqrt{G})$ be the field obtained from F by adjoining $\sqrt{g}$ for each $g \in G$. Then $F(\sqrt{G})$ is called a multiquadratic extention of F. If G is generated over F^2 by $\{g_1, \ldots, g_n\}$, then $F(\sqrt{G}) = F(\sqrt{g_1}, \ldots, \sqrt{g_n})$.

(1.6) Proposition. Let $K = F(\sqrt{G})$ be a finite multiquadratic extension of F. If $a \in \dot{F} \cap K^2$, then $a \in G$.

Proof: Let $[K:F] = 2^n$. We prove the proposition by induction on n. It follows that $K = F(\sqrt{g_1}, \ldots, \sqrt{g_n})$ for some $g_i \in G$. Let $E = F(\sqrt{g_1}, \ldots, \sqrt{g_{n-1}})$. Then $K = E(\sqrt{g_n})$ and $a \in \dot{E} \cap K^2$. A trivial calculation shows $a \in E^2 \cup g_n E^2$. Thus there exists $b \in E^2$ such that

either $a = b$ or $a = g_n b$. In either case $b \in \dot{F} \cap E^2$. By induction it follows that $b \in G_1 \subseteq G$ where G_1 is the group generated by $\{g_1, \ldots, g_{n-1}\}$ over F^2. It follows that $a \in G$.

We note that if $[G:F^2] = 2^n$, then it follows from (1.6) that $[F(\sqrt{G}):F] = 2^n$.

(1.7) Theorem. Let G be a subgroup of $\dot{F}$ and let $K = F(\sqrt{G})$. Let α, β be two forms defined over F. Consider the following statements.

i) $\alpha \tilde{\simeq}_G \beta$.

ii) $\alpha \tilde{\tilde{\simeq}}_G \beta$.

iii) $\alpha \equiv \beta \pmod{\mathfrak{q}_G}$ and $\dim \alpha = \dim \beta$.

iv) $\alpha \tilde{\cong}_K \beta$.

Then i) $\rightarrow$ ii) $\rightarrow$ iii) $\rightarrow$ iv).

Proof: i) $\rightarrow$ ii). This is trivial.

ii) $\rightarrow$ iii). Since $\alpha \tilde{\tilde{\simeq}}_G \beta$, there exists a sequence $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_m = \beta$ such that either $\alpha_i \cong \alpha_{i+1}$ or $\alpha_i \tilde{\simeq}_G \alpha_{i+1}$. In the first case it is clear that $\alpha_i \equiv \alpha_{i+1} \pmod{\mathfrak{q}_G}$. In the second case, suppose $\alpha_i = \langle a_1, \ldots, a_n \rangle$ and $\alpha_{i+1} = \langle a_1 g_1, \ldots, a_n g_n \rangle$ for some $g_j \in G$. Then $\alpha_i \perp -\alpha_{i+1} = a_1\langle 1, -g_1 \rangle \perp \ldots \perp a_n \langle 1, -g_n \rangle \in \mathfrak{q}_G$ and thus $\alpha_i \equiv \alpha_{i+1} \pmod{\mathfrak{q}_G}$. Since congruence mod $\mathfrak{q}_G$ is an

equivalence relation, it follows that $\alpha \equiv \beta \pmod{\mathfrak{n}_G}$. It is trivial that $\dim \alpha = \dim \beta$.

iii) $\rightarrow$ iv) . Since every element of G is a square in K , it follows that in the map of Witt rings $W(F) \rightarrow W(K)$ the ideal $\mathfrak{n}_G$ maps to 0 in $W(K)$. If $\alpha \equiv \beta \pmod{\mathfrak{n}_G}$ then $\alpha = \beta$ in $W(K)$. Since $\dim \alpha = \dim \beta$, we see that $\alpha \tilde{\cong}_K \beta$.

We are interested in whether or not the converses iv) $\rightarrow$ iii) and iii) $\rightarrow$ ii) hold.

(1.8) Definition. Let G be a subgroup of $\dot{F}$ and let $K = F(\sqrt{G})$. The subgroup G has the kernel property if $\ker(W(F) \rightarrow W(K)) = \mathfrak{n}_G$. If every subgroup G of $\dot{F}$ has the kernel property, then F is 1-amenable.

(1.9) Proposition. A subgroup G of $\dot{F}$ has the kernel property if and only if for forms α , β of the same dimension defined over F , $\alpha \tilde{\cong}_K \beta$ implies $\alpha \equiv \beta \pmod{\mathfrak{n}_G}$ where $K = (F\sqrt{G})$.

Proof: Assume G has the kernel property and $\alpha \tilde{\cong}_K \beta$. Then $\alpha \perp -\beta = 0$ in $W(K)$ and trivially $\alpha \perp -\beta \in \ker(W(F) \rightarrow W(K))$. Thus $\alpha \perp -\beta \in \mathfrak{n}_G$ and $\alpha \equiv \beta \pmod{\mathfrak{n}_G}$.

Assume for forms α , β defined over F that

$\alpha \tilde{\equiv}_K \beta$ implies $\alpha \equiv \beta \pmod{\mathcal{n}_G}$. Let $\delta \in \ker(W(F) \to W(K))$. Then $\dim \delta$ is even since $\delta = 0$ in $W(K)$. Let $\delta = \langle a_1, \ldots, a_n, -b_1, \ldots, -b_n \rangle$, $\alpha = \langle a_1, \ldots, a_n \rangle$, and $\beta = \langle b_1, \ldots, b_n \rangle$. Then $\alpha \perp -\beta = 0$ in $W(K)$. Thus $\alpha = \beta$ in $W(K)$ and $\dim \alpha = \dim \beta$ and this implies $\alpha \tilde{\equiv}_K \beta$. Our assumption implies $\alpha \equiv \beta \pmod{\mathcal{n}_G}$ and therefore $\delta = \alpha \perp -\beta \in \mathcal{n}_G$.

Determining whether or not a field is 1-amenable is usually difficult. Every global field, local field, and field F with Hasse number $\tilde{u}(F) \leq 2$ is 1-amenable (see [ELW$_1$, (3.2)] and [ELW$_2$, (6.4)]). We prove these results later in Chapter IV using different methods. It is known that the rational function field $\mathbb{Q}(x)$ is not 1-amenable [Ww]. It is useful to know if a field is 1-amenable since Pfister's conjecture on the Clifford invariant holds in F if F is 1-amenable [ELW$_1$, (3.4)].

(1.10) Definition. A subgroup G of $\dot{F}$ has piecewise equivalence or simply G has PE if for forms α, β defined over F of the same dimension, $\alpha \equiv \beta \pmod{\mathcal{n}_G}$ implies $\alpha \tilde{\equiv}_G \beta$. If this implication holds for binary forms α, β then G has binary PE.

(1.11) Definition. A subgroup G of $\dot{F}$ has weak PE if for all forms α, β defined over F such that

dim α = dim β and $\alpha \equiv \beta \pmod{\mathcal{Q}_G}$, there exists a sequence $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_m = \beta$ such that

1) dim α_i = dim α_{i+1} , $0 \leq i \leq m-1$; and

2) If $\alpha_i = \langle c_1, \ldots, c_n \rangle$ and $\alpha_{i+1} = \langle d_1, \ldots, d_n \rangle$, then for some j,k , $\langle c_j, c_k \rangle \equiv \langle d_j, d_k \rangle \pmod{\mathcal{Q}_G}$ and $c_i = d_i$ for all $i \neq j,k$.

(1.12) Proposition. A subgroup G of $\dot{F}$ has PE if and only if G has binary PE and weak PE.

Proof: Suppose G has binary PE and weak PE . Let α , β be forms defined over F such that $\alpha \equiv \beta \pmod{\mathcal{Q}_G}$ and dim α = dim β . Let $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_m = \beta$ be a sequence as in (1.11). Since G has binary PE it follows that in condition 2) of (1.11) we have $\langle c_j, c_k \rangle \overset{\approx}{G} \langle d_j, d_k \rangle$ and thus $\alpha_i \overset{\approx}{G} \alpha_{i+1}$ for each i , $0 \leq i \leq m-1$. Therefore $\alpha \overset{\approx}{G} \beta$ since $\overset{\approx}{G}$ is an equivalence relation and so G has PE.

The converse is trivial.

We now study the question of whether or not a group G has binary PE.. The study of PE and weak PE will appear in a future work.

(1.13) Notation. Let $\alpha = \langle a_1, \ldots, a_n \rangle$ be a form

defined over F and let G be a subgroup of $\dot{F}$. We set

$$D^G(\alpha) = \{a \in \dot{F} \mid a = a_1 g_1 + \ldots + a_n g_n \text{ , where } g_1, \ldots, g_n \in G \cup \{0\}\}$$

and $\tilde{D}^G(\alpha) = \{a \in \dot{F} \mid \alpha \tilde{G} \langle a \rangle \perp \alpha' \text{ for some } \alpha'\}$.

Recall from the introduction that a Pfister form $\langle\langle -a, -b \rangle\rangle$ is the form $\langle 1, -a \rangle \otimes \langle 1, -b \rangle = \langle 1, -a, -b, ab \rangle$.

(1.14) Proposition. Let G be a subgroup of $\dot{F}$. The following are equivalent.

1) G has binary PE.

2) If $\langle\langle -a, -b \rangle\rangle \in \mathcal{I}_G$, then $b \in \tilde{D}^G(\langle 1, -a \rangle)$.

Proof: 1) $\rightarrow$ 2). If $\langle\langle -a, b \rangle\rangle \in \mathcal{I}_G$, then $\langle 1, -a \rangle \equiv \langle b, -ab \rangle \pmod{\mathcal{I}_G}$. From 1) we conclude $\langle 1, -a \rangle \tilde{G} \langle b, -ab \rangle$ so $b \in \tilde{D}^G(\langle 1, -a \rangle)$.

2) $\rightarrow$ 1). Let α, β be binary forms such that $\alpha \equiv \beta \pmod{\mathcal{I}_G}$. Suppose $\alpha = c_1\langle 1, -a \rangle$, $c_1, a \in \dot{F}$. Then $d(\alpha) = a$ and thus $d(\beta) = ag$ for some $g \in G$ by (1.4). We can write $\beta = c_2\langle 1, -ag \rangle$ where $c_2 \in \dot{F}$. We must show $c_1\langle 1, -a \rangle \tilde{G} c_2\langle 1, -ag \rangle$. Since $\langle 1, -a \rangle \tilde{G} \langle 1, -ag \rangle$, it is sufficient to show $\langle 1, -a \rangle \tilde{G} c_1c_2\langle 1, -a \rangle$. From $\alpha \equiv \beta \pmod{\mathcal{I}_G}$ it follows that $\langle 1, -a \rangle \equiv c_1c_2\langle 1, -a \rangle \pmod{\mathcal{I}_G}$ and thus $\langle\langle -a, -c_1c_2 \rangle\rangle \in \mathcal{I}_G$. By 2) we have $c_1c_2 \in \tilde{D}^G(\langle 1, -a \rangle)$. Therefore $\langle 1, -a \rangle \tilde{G}$

$c_1c_2\langle 1, -d\rangle$ for some $d \in \dot{F}$. It follows from (1.7) that $\langle 1, -a\rangle \equiv c_1c_2\langle 1, -d\rangle \pmod{\mathcal{N}_G}$ and thus by (1.4) that $ad \in G$. Then for some $g_1 \in G$, we have $d = ag_1$ and then

$$\langle 1, -a\rangle \overset{\sim}{\underset{G}{\approx}} c_1c_2\langle 1, -ag_1\rangle \overset{\sim}{\underset{G}{\approx}} c_1c_2\langle 1, -a\rangle$$

as desired.

(1.15) Proposition. Let G be a subgroup of $\dot{F}$. For each $a \in \dot{F}$, $\tilde{D}^G(\langle 1, a\rangle)$ is the group generated by the subgroups $D(\langle 1, ag\rangle)$, $g \in G$.

Proof: It follows from (1.4) that $c \in \tilde{D}^G(\langle 1, a\rangle)$ if and only if $\langle 1, a\rangle \overset{\sim}{\underset{G}{\approx}} c\langle 1, a\rangle$. If $c_1, c_2 \in \tilde{D}^G(\langle 1, a\rangle)$, then $c_1c_2\langle 1, a\rangle \overset{\sim}{\underset{G}{\approx}} c_1\langle 1, a\rangle \overset{\sim}{\underset{G}{\approx}} \langle 1, a\rangle$ and thus $c_1c_2 \in \tilde{D}^G(\langle 1, a\rangle)$. Since $c^{-1} = c \cdot (\frac{1}{c})^2$ it follows that $\tilde{D}^G(\langle 1, a\rangle)$ is a group that contains F^2.

If $c \in \tilde{D}^G(\langle 1, a\rangle)$, there is a sequence $\langle 1, a\rangle = \alpha_0, \alpha_1, \ldots, \alpha_m = c\langle 1, a\rangle$ where either $\alpha_i \overset{\sim}{\underset{G}{\approx}} \alpha_{i+1}$ or $\alpha_i \cong \alpha_{i+1}$, $0 \leq i \leq m-1$. Suppose $\alpha_i = c_i\langle 1, ag_i\rangle$ where $g_i \in G$. If $\alpha_i \overset{\sim}{\underset{G}{\approx}} \alpha_{i+1}$, then $\alpha_{i+1} = c_i\langle h, ag_ih'\rangle \cong c_ih\langle 1, ag_ihh'\rangle$, for some $h, h' \in G$. If $\alpha_i \cong \alpha_{i+1}$, then $\alpha_{i+1} = c_id\langle 1, ag_i\rangle$ for some $d \in D(\langle 1, ag_i\rangle)$ since $\det \alpha_i = \det \alpha_{i+1}$. In either case we have $\alpha_{i+1} = c_{i+1}\langle 1, ag_{i+1}\rangle$ where $g_{i+1} \in G$ and $c_{i+1} \in c_iD^G(\langle 1, a\rangle)$. Since $c_0 = 1$ and $c_m = c$, we see that c is a product

of m elements of $D^G(\langle 1, a\rangle)$.

A typical element of $D^G(\langle 1, a\rangle)$ is $g + ah = a^{-1}(ag)(1 + ag^{-1}h) \in D(\langle 1, a\rangle) \cdot D(\langle 1, ag\rangle) \cdot D(\langle 1, agh\rangle)$. Therefore if $c \in \tilde{D}^G(\langle 1, a\rangle)$, then c is a product of elements from $D(\langle 1, ag\rangle)$, $g \in G$.

(1.16) Proposition. Let G be a subgroup of $\dot{F}$ and let $K = F(\sqrt{G})$. Then $\dot{F} \cap D_K(\langle 1, -a\rangle) = \prod_{g\in G} D_F(\langle 1, -ag\rangle)$ for each $a \in \dot{F}$ if and only if G has binary PE and G has the kernel property for 4-dimensional forms. (That is, if $\dim \alpha = 4$ and $\alpha \in \ker(W(F) \to W(K))$ then $\alpha \in \mathcal{I}_G$.)

Proof: Suppose G has binary PE and the kernel property for 4-dimensional forms. It is always true that $\prod_{g\in G} D_F(\langle 1, -ag\rangle) \subseteq \dot{F} \cap D_K(\langle 1, -a\rangle)$ since each $g \in G$ is a square in K and $\dot{F} \cap D_K(\langle 1, -a\rangle)$ is a group. Let $b \in \dot{F} \cap D_K(\langle 1, -a\rangle)$. Then $\langle 1, -a\rangle \cong_K \langle b, -ab\rangle$ and so $\langle 1, -a\rangle \equiv \langle b, -ab\rangle \pmod{\mathcal{I}_G}$ since G has the kernel property for 4-dimensional forms (see (1.9)). Since $\langle\langle -1, -b\rangle\rangle \in \mathcal{I}_G$ and G has binary PE , it follows from (1.14) that $b \in \tilde{D}^G(\langle 1, -a\rangle)$. Then $b \in \prod_{g\in G} D_F(\langle 1, -ag\rangle)$ by (1.15).

Suppose $\dot{F} \cap D_K(\langle 1, -a\rangle) = \prod_{g\in G} D_F(\langle 1, -ag\rangle)$ for each $a \in \dot{F}$. Let $\langle\langle -a, -b\rangle\rangle \in \mathcal{I}_G$. Then $\langle 1, -a\rangle \equiv \langle b, ab\rangle \pmod{\mathcal{I}_G}$ and so $\langle 1, -a\rangle \cong_K \langle b, -ab\rangle$ by (1.7). Then

$b \in \dot{F} \cap D_K(\langle 1, -a\rangle) = \prod_{g\in G} D_F(\langle 1, -ag\rangle) = \tilde{D}^G(\langle 1, -a\rangle)$ by (1.15). Therefore G has binary PE by (1.14). Now let γ be a 4-dimensional form defined over F that is hyperbolic in K. Then $d(\gamma) \in \dot{F} \cap K^2$ and therefore $d(\gamma) \in G$ by (1.6). By scaling we may assume γ represents 1 over F so that we may write $\gamma = \langle 1, -a, -b, abg\rangle$ for some $g \in G$. Since $\langle 1, -a, -b, abg\rangle \equiv \langle\langle -a, -b\rangle\rangle \pmod{\sigma_G}$ it is sufficient to show if $\langle\langle -a, -b\rangle\rangle$ is hyperbolic in K then $\langle\langle -a, -b\rangle\rangle \in \sigma_G$. But if $\langle\langle -a, -b\rangle\rangle$ is hyperbolic in K then $\langle 1, -a\rangle \cong_K \langle b, -ab\rangle$ and so $b \in \dot{F} \cap D_K(\langle 1, -a\rangle) = \prod_{g\in G} D_F(\langle 1, -ag\rangle) = \tilde{D}^G(\langle 1, -a\rangle)$. It follows that $\langle 1, -a\rangle \tilde{G} \langle b, -ab\rangle$ and so $\langle 1, -a\rangle \equiv \langle b, -ab\rangle \pmod{\sigma_G}$ by (1.7). Therefore $\langle\langle -a, -b\rangle\rangle \in \sigma_G$.

(1.17) Proposition. Let G be a subgroup of $\dot{F}$ such that $[G:F^2] = 2$. Then G has the kernel property.

Proof: Let $K = F(\sqrt{G})$. Then $K(\sqrt{g})$ for some $g \in G$. Let $\gamma \in \ker(W(F) \to W(K))$. There exists a form δ defined over F such that $\gamma \cong_F \langle 1, -g\rangle \otimes \delta$ (see [L, p. 200]). Therefore $\gamma \in \sigma_G$.

(1.18) Proposition. Let G be a subgroup of $\dot{F}$ such that $[G:F^2] = 2$. Then G has binary PE.

Proof: Let $K = F(\sqrt{G}) = F(\sqrt{g})$ for some $g \in G$. Let $\gamma = \langle\langle -a, -b \rangle\rangle \in \mathcal{I}_G$. Then $\gamma = 0$ in the Witt ring $W(K)$ so $\gamma \cong_K H \perp H$.

If γ is isotropic over F, then γ is hyperbolic over F, since $\det \gamma = 1$. Then $\langle 1, -a \rangle \cong_F \langle b, -ab \rangle$ and so $b \in D_F(\langle 1, -a \rangle) \subseteq \tilde{D}^G(\langle 1, -a \rangle)$. By (1.14) G has binary PE.

Suppose γ is anisotropic over F. Since γ is hyperbolic in $F(\sqrt{g})$, it follows that $\gamma \cong_F \langle 1, -g \rangle \otimes c\langle 1, -d \rangle$ for some $c,d \in \dot{F}$ [L, p. 200]. Since γ is a Pfister form and $\gamma \cong_F c\langle\langle -g, -d \rangle\rangle$, it follows from [L, p. 279] that we may take $c = 1$. Then $\langle -a, -b, ab \rangle \cong_F \langle -g, -d, gd \rangle$, so $\langle g, -a, -b, ab \rangle$ is isotropic over F. Thus there exists $r \in D_F(\langle g, -a \rangle) \cap D_F(\langle b, -ab \rangle)$ and so $r \in \tilde{D}^G(\langle 1, -a \rangle) \cap \tilde{D}^G(\langle b, -ab \rangle)$. By (1.4), we conclude $\langle 1, -a \rangle \tilde{\cong}_G r\langle 1, -a \rangle$ and $\langle b, -ab \rangle \tilde{\cong}_G r\langle 1, -a \rangle$. Therefore $\langle 1, -a \rangle \tilde{\cong}_G \langle b, -ab \rangle$ and so $b \in \tilde{D}^G(\langle 1, -a \rangle)$. Then G has binary PE by (1.14).

(1.19) Corollary. Let $K = F(\sqrt{g})$ be a quadratic extension of F and let $a \in \dot{F}$. Then $D_K(\langle 1, -a \rangle) \cap \dot{F} = D_F(\langle 1, -a \rangle) \cdot D_F(\langle 1, -ag \rangle)$.

Proof: Let G be the group generated by g over F^2. Then $K = F(\sqrt{G})$ and $[G:F^2] = 2$. By (1.17) and (1.18), G has the kernel property and G has binary PE.

It follows from (1.16) that $D_K(\langle 1, -a\rangle) \cap \dot{F} = D_F(\langle 1, -a\rangle) \cdot D_F(\langle 1, -ag\rangle)$.

For later use in Chapter II, we introduce the following notation.

(1.20) Notation. For each $a \in \dot{F}$, set $N_F(a) = D_F(\langle 1, -a\rangle)$. Thus if $a \notin F^2$, then $N_F(a)$ is the set of nonzero norms from $F(\sqrt{a})$. Corollary (1.19) now reads $N_K(a) \cap \dot{F} = N_F(a) \cdot N_F(ag)$.

(1.21) Theorem. Suppose G is a subgroup of $\dot{F}$ and that every subgroup $G_0 \subseteq G$ such that $[G_0:F^2] < \infty$ has binary PE and the kernel property. Then G has binary PE and the kernel property.

Proof: Suppose $\langle\langle -a, -b\rangle\rangle \in \mathcal{O}_G$. Clearly there is a subgroup $G_0 \subseteq G$ such that $\langle\langle -a, -b\rangle\rangle \in \mathcal{O}_{G_0}$ and $[G_0:F^2] < \infty$. By (1.14) $b \in \tilde{D}^{G_0}(\langle 1, -a\rangle) \subseteq \tilde{D}^{G}(\langle 1, -a\rangle)$ and so by (1.14) G has binary PE.

Let $K = F(\sqrt{G})$ and let δ be a form defined over F such that $\delta \in \ker(W(F) \to W(K))$. Then δ is hyperbolic in some finite multiquadratic extension $F(\sqrt{G_0})$ where $G_0 \subseteq G$ and $[G_0:F^2] < \infty$. Since G_0 has the kernel property, $\delta \in \mathcal{O}_{G_0} \subseteq \mathcal{O}_G$ as desired.

(1.22) Theorem. Let H and G be subgroups of $\dot{F}$ such that $[G:H] = 2$. Let $K = F(\sqrt{H})$ and let $g \in G-H$. Consider statement (*) and the five following statements:

(*) If α, β are binary forms defined over F such that $d(\alpha \perp -\beta) = g$ and $\alpha \perp -\beta$ is isotropic over K, then $D_K(\alpha) \cap D_K(\beta) \cap \dot{F} \neq \emptyset$.

1) H has the kernel property for 4-dimensional forms, H has binary PE, and (*) holds.

2) G has the kernel property for 4-dimensional forms and G has binary PE.

3) (*) holds.

4) H has the kernel property for 4-dimensional forms and (*) holds.

5) G has the kernel property for 4-dimensional forms.

Then 1) $\rightarrow$ 2) $\rightarrow$ 3) and 4) $\rightarrow$ 5).

Proof: 4) $\rightarrow$ 5). Let δ be a 4-dimensional form defined over F such that δ is hyperbolic over $K(\sqrt{g})$. Just as in paragraph 2 of the proof of (1.16), we may assume $\delta = \langle\langle -a, -b\rangle\rangle$, $a,b \in \dot{F}$. Since $\langle 1, -a, -b, ab\rangle$ is hyperbolic over $K(\sqrt{g})$, it follows that $\langle g, -a, -b, ab\rangle$ is isotropic over K, since a 4-dimensional form of determinant g that is isotropic over $K(\sqrt{g})$ is already iso-

tropic over K [L, p. 125]. Let $\alpha = \langle g, -a\rangle$ and $\beta = \langle b, -ab\rangle$. It follows from (*) that there exists $r \in D_K(\alpha) \cap D_K(\beta) \cap \dot{F}$. It follows that $\langle g, -a, -r\rangle$ and $\langle b, -ab, -r\rangle$ are isotropic over K , so $\langle g, -a, -r, gar\rangle$ and $\langle b, -ab, -r, ar\rangle$ are isotropic and have determinant 1 so they are hyperbolic over K . Since H has the kernel property for 4-dimensional forms, it follows that these two forms lie in $\mathcal{O}_H$. Since $\langle g, -a, -r, gar\rangle \equiv \langle 1, -a, -r, ar\rangle \pmod{\mathcal{O}_G}$ and $\langle g, -a, -r, gar\rangle \in \mathcal{O}_H \subseteq \mathcal{O}_G$, it follows that $\langle 1, -a, -r, ar\rangle \in \mathcal{O}_G$ and $\langle b, -ab, -r, ar\rangle \in \mathcal{O}_H \subseteq \mathcal{O}_G$. Thus the difference $\langle 1, -a, -b, ab\rangle \in \mathcal{O}_G$ as desired.

1) $\rightarrow$ 2) . It follows from 4) $\rightarrow$ 5) that G has the kernel property for 4-dimensional forms. It remains to show that G has binary PE.

Let $\langle\langle -a, -b\rangle\rangle \in \mathcal{O}_G$. Then $\langle\langle -a, -b\rangle\rangle$ is hyperbolic over $K(\sqrt{g})$. Let $\alpha = \langle 1, -a\rangle$ and $\beta = b\langle 1, -ag\rangle$. Then $\alpha \perp -\beta = \langle 1, -a, -b, abg\rangle$ is isotropic over K since it is isotropic over $K(\sqrt{g})$ and its determinant is g (see the remarks above). Since $d(\alpha \perp -\beta) = g$, it follows from (*) that there exists $r \in D_K(\langle 1, -a\rangle) \cap D_K(b\langle 1, -ag\rangle) \cap \dot{F}$. Thus there exists $s \in \dot{F}$ such that $r = \frac{b}{s}$ and $\frac{1}{s} \in D_K(\langle 1, -ag\rangle) \cap \dot{F}$. Then $s \in D_K(\langle 1, -ag\rangle) \cap \dot{F}$ (multiply by s^2). It follows from (1.15) and (1.16) that $r \in \tilde{D}^H(\langle 1, -a\rangle)$ and $s \in \tilde{D}^H(\langle 1, -ag\rangle) \cap \dot{F}$. Therefore $b = rs \in \tilde{D}^G(\langle 1, -a\rangle)$

since $\tilde{D}^G(\langle 1, -a\rangle)$ is a group. It follows from (1.14) that G has binary PE.

2) $\rightarrow$ 3) . Let α , β be as in (*). We may scale to assume that $\alpha = \langle 1, -a\rangle$ and $\beta = b\langle 1, -ag\rangle$. Then $\alpha \perp -\beta$ is hyperbolic over $K(\sqrt{g})$ since $d(\alpha \perp -\beta) = 1$ in $K(\sqrt{g})$. By the kernel property, $\langle 1, -a, -b, abg\rangle \in \mathcal{N}_G$ and thus $\langle\langle -a, -b\rangle\rangle \in \mathcal{N}_G$. It follows that $b \in \tilde{D}^G(\langle 1, -a\rangle)$ since G has binary PE. Since $\tilde{D}^G(\langle 1, -a\rangle)$ is generated by $\tilde{D}^H(\langle 1, -a\rangle)$ and $\tilde{D}^H(\langle 1, -ag\rangle)$ (see (1.15)), we see that $b = rs$ for some $r \in \tilde{D}^H(\langle 1, -a\rangle)$ and $s \in \tilde{D}^H(\langle 1, -ag\rangle)$. It follows that $r \in \dot{F} \cap D_K(\langle 1, -a\rangle)$ and $s \in \dot{F} \cap D_K(\langle 1, -ag\rangle)$. Since $s = br/r^2$, we see that $br \in \dot{F} \cap D_K(\langle 1, -ag\rangle)$ and thus $r \in \dot{F} \cap D_K(b\langle 1, -ag\rangle)$. Therefore $r \in \dot{F} \cap D_K(\alpha) \cap D_K(\beta)$ and (*) holds.

We generalize (*) in definition (1.23) below. The common value property defined in (1.23) is one of several we study in the remainder of this work. In Chapter II we obtain complete results if F is a number field.

(1.23) Definition. The extension K/F satisfies the common value property CV(2,2) when for every pair of binary forms α , β defined over F , if $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$, then $D_K(\alpha) \cap D_K(\beta) \cap \dot{F} \neq \emptyset$.

We say a field F is 1-amenable for 4-dimensional

forms if every subgroup G of $\dot{F}$ has the kernel property for 4-dimensional forms.

(1.24) Theorem. A field F is 1-amenable for 4-dimensional forms and every subgroup G of $\dot{F}$ has binary PE if and only if every finite multiquadratic extension K/F satisfies CV(2,2).

Proof: Suppose F is 1-amenable for 4-dimensional forms and every subgroup G of $\dot{F}$ has binary PE. Let K be a multiquadratic extension of F. Then $K = F(\sqrt{H})$ for some subgroup H of $\dot{F}$. Let α, β be defined over F and suppose $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$. Let $d(\alpha \perp -\beta) = g$. If $g \in H$, then $g \in K^2$ and so $\alpha \perp -\beta$ is hyperbolic over K. Since a ternary subform of a hyperbolic 4-dimensional form is isotropic, if $\alpha \cong_F \langle a_1, a_2 \rangle$ then $\langle a_1 \rangle \perp -\beta$ is isotropic over K, so $a_1 \in D_K(\alpha) \cap D_K(\beta) \cap \dot{F}$. If $g \notin H$, let G be generated by H and g. Then $[G:H] = 2$. Since G has the kernel property for 4-dimensional forms and G has binary PE, it follows from (1.22) 2) $\rightarrow$ 3) that (*) holds. Therefore, in either case $D_K(\alpha) \cap D_K(\beta) \cap \dot{F} \neq \emptyset$, so K/F satisfies CV(2,2).

Suppose every finite multiquadratic extension satisfies CV(2,2). Let G be a subgroup of $\dot{F}$. By (1.21) we may assume $[G:F^2] < \infty$. Thus $[F(\sqrt{G}):F] < \infty$. Let H be a subgroup of G such that $[G:H] = 2$. By induction

we can assume H has binary PE and the kernel property for 4-dimensional forms. (If $H = F^2$, it is trivial that H has these properties.) By theorem (1.22) 1) $\rightarrow$ 2) we see that the result follows.

We see from theorem (1.24) that it is desirable to know when a multiquadratic extension K/F satisfies CV(2,2). This will be studied in Chapters II and III when F is a number field and in Chapter IV for other special fields.

CHAPTER II

COMMON VALUE PROPERTIES OF QUADRATIC FORMS OVER NUMBER FIELDS

In this chapter we define several types of common value properties of quadratic forms and obtain complete characterizations of these over number fields. The results will be applied to show that every subgroup of a number field has binary PE.

(2.1) Definitions. Let K/F be a finite extension of fields and let (α, β) be an ordered pair of quadratic forms defined over F.

i) The triple $(\alpha, \beta, K/F)$ satisfies the strong common value property SCV if $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$ implies $D_F(\alpha) \cap D_K(\beta) \neq \emptyset$.

ii) The triple $(\alpha, \beta, K/F)$ satisfies SCV' if either $(\alpha, \beta, K/F)$ or $(\beta, \alpha, K/F)$ satisfies SCV.

iii) The triple $(\alpha, \beta, K/F)$ satisfies the common value property CV if $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$ implies $D_K(\alpha) \cap D_K(\beta) \cap \dot{F} \neq \emptyset$.

iv) The extension K/F is excellent if for each form α defined over F and isotropic over K, there exists a

form β defined over F such that $\alpha \cong_K H \perp \beta$.

Given an ordered pair (m, n) of positive integers, we say the extension K/F satisfies $SCV(m,n)$ if for all pairs of forms (α, β) defined over F with $\dim \alpha = m$, $\dim \beta = n$, the triple $(\alpha, \beta, K/F)$ satisfies SCV. Similarly we speak of K/F satisfying $SCV'(m,n)$ and $CV(m, n)$. It is clear that $SCV'(m,n)$ is equivalent to $SCV'(n,m)$ and $CV(m,n)$ is equivalent to $CV(n,m)$.

It is obvious for the triple $(\alpha, \beta, K/F)$ that $SCV \to SCV' \to CV$. It is also obvious that every extension K/F satisfies $SCV(1,n)$ for all $n \geq 1$ and $SCV'(m,1)$ for all $m \geq 1$.

(2.2) Proposition. Let α and $\beta = \langle b \rangle$ be quadratic forms defined over F of dimensions m and 1 respectively and suppose $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$. Then $(\alpha, \beta, K/F)$ satisfies SCV if and only if $\alpha \perp -c\beta$ is isotropic over F for some $c \in \dot{F} \cap K^2$.

Proof: Suppose $\alpha \perp -c\beta$ is isotropic over F where $c \in \dot{F} \cap K^2$. Then $cb \in D_F(\alpha)$. Since $c \in K^2$, we have $cb \in D_K(\beta)$ and so $cb \in D_F(\alpha) \cap D_K(\beta)$.

Now suppose $(\alpha, \beta, K/F)$ satisfies SCV. Then there exists $r \in D_F(\alpha) \cap D_K(\beta)$. Since $r \in D_K(\beta)$, we have

$r = b\gamma^2$ for some $\gamma \in \dot{K}$. Letting $c = \gamma^2$ and noting $r \in \dot{F}$, we see $c \in \dot{F}$, so $c \in \dot{F} \cap K^2$. It follows $\alpha \perp -c\beta$ is isotropic over F since $r = bc$.

To study these three common value properties further, we now assume $m,n \geq 2$ and specialize to number fields. All the results that follow concerning number fields undoubtedly hold for global fields (see [W]). In Chapter IV, we shall study these properties for other special fields.

First we review some terminology and important results from number theory. Let F be a number field. We let $\Omega(F)$ denote the set of prime spots of F. If $p \in \Omega(F)$, F_p is the completion of F with respect to the topology induced by the p-adic valuation. A prime p is finite if its corresponding valuation is nonarchimedean and is infinite if the corresponding valuation is archimedean. A finite prime p is <u>nondyadic</u> if its residue class field has characteristic different from 2 and is <u>dyadic</u> if the characteristic is 2. If $a \in \dot{F}$ and $p \in \Omega(F)$ where p is finite, then $\text{ord}_p(a)$ is the exact power of p appearing in the prime decomposition of the ideal (a). A quadratic form α is isometric to a <u>unit form</u> over F_p for some finite $p \in \Omega(F)$ if $\alpha \cong_{F_p} \langle a_1, \ldots, a_n \rangle$ and $\text{ord}_p(a_i)$ is even for each a_i.

Let K be a finite extension of a number field F. Set

$$E(K/F) = \{p \in \Omega(K/F) \mid [K_P:F_p] \text{ is even for every } P \in \Omega(K) \text{ where } P|p\} .$$

The following convention regarding infinite primes is used. Let p be an infinite prime in $\Omega(F)$ and let $P \in \Omega(K)$ lie over p. Then $[K_P:F_p] \leq 2$. If for some P, $[K_P:F_p] = 2$, we say p ramifies in K. If $[K_P:F_p] = 1$ for each P that lies over p, then we say p is unramified. Thus if $p \in E(K/F)$ and p is unramified in K, then p is a finite prime.

A modulus is a formal product $m = \prod_{p \in T} p^{e(p)}$ where T is a finite subset of $\Omega(F)$, $e(p) \geq 0$, and if $p \in T$ is a real archimedean prime, $e(p) = 0$ or 1, and if p is a complex prime, then $e(p) = 0$. If $a \in \dot{F}$, then $a \equiv 1 \bmod m$ means $a \equiv 1 \pmod{p^{e(p)}}$ if $p \in T$ is finite and $a > 0$ in the completion F_p if $p \in T$ is a real archimedean prime. We let

$$F_{m,1} = \{a \in \dot{F} \mid a \equiv 1 \bmod m\} ,$$

$i(F_{m,1})$ = the fractional ideals (a) where $a \in F_{m,1}$, and

I^m = the group of fractional ideals of F generated by primes not occurring as factors of m.

We shall use the following generalized Dirichlet theorem (see [J, p. 182]). If $B \in I^m$, then the coset $\mathfrak{i}(F_{m,1})B$ contains infinitely many prime ideals.

Let M be a finite normal extension of F, p a finite prime in $\Omega(F)$ that is unramified in M, and let $P \in \Omega(M)$ such that $P|p$. We let $\sigma(M/F, P)$ denote the Frobenius automorphism of P in $\mathrm{Gal}(M/F)$. If $\mathrm{Gal}(M/F)$ is abelian, $\sigma(M/F, P)$ is the same for each $P|p$. In this case we write $\sigma(M/F, p)$. Assume M is an abelian extension of F and let m be a modulus that contains the primes in $\Omega(F)$ that ramify in M. We let $\phi = \phi_m$: $I^m \to \mathrm{Gal}(M/F)$ be the Artin map where ϕ is a multiplicative homomorphism that maps a prime ideal $p \in I^m$ to the Frobenius automorphism $\sigma(M/F, p)$.

(2.3) Proposition. Let F be a number field, m, n positive integers, $M = F(\sqrt{a_1}, \ldots, \sqrt{a_n}, \sqrt{b_1}, \ldots, \sqrt{b_m})$ and assume $[M:F] = 2^{m+n}$. Then there are infinitely many primes $p \in \Omega(F)$ such that $a_i \in F_p^2$, $1 \leq i \leq n$, and $b_j \notin F_p^2$, $1 \leq j \leq m$.

Proof: We have

$$\mathrm{Gal}(M/F) \cong \prod_{i=1}^{n} \mathrm{Gal}(F(\sqrt{a_i})/F) \times \prod_{j=1}^{m} \mathrm{Gal}(F(\sqrt{b_j})/F) .$$

Let σ' be the unique automorphism of M/F whose fixed

field is exactly $F(\sqrt{a_1}, \ldots, \sqrt{a_n})$, i.e., $\sigma' = (1, 1, \ldots, 1; -1, \ldots, -1)$. Since $Gal(M/F)$ is abelian and σ' has order 2 , it follows that $\{\sigma'\}$ is the division of σ' ; that is, the elements in $Gal(M/F)$ that are conjugate to $(\sigma')^t$ where t is relatively prime to 2 . It follows from the Frobenius density theorem [J, p. 134] that there are infinitely many primes $p \in \Omega(F)$ whose Frobenius automorphism $\sigma(M/F, p) = \sigma'$. For each of these primes p , $a_i \in F_p^2$, $1 \leq i < n$ and $b_j \notin F_p^2$, $1 \leq j \leq m$.

(2.4) Lemma. Let F be a p-adic field and let $\alpha = \langle 1, -a\rangle$ and $\beta = c\langle 1, -b\rangle$ where $a,b,c \in \dot{F}$. If $a,b \notin F^2$ and $ab \in F^2$, then either $D(\alpha) = D(\beta)$ or $D(\alpha) \cap D(\beta) = \emptyset$. If $a,b,ab \notin F^2$, then the sets $D(\alpha) \cap D(\beta)$, $D(\alpha) - D(\beta)$, $D(\beta) - D(\alpha)$, and $\dot{F} - (D(\alpha) \cup D(\beta))$ are each nonempty.

Proof: Assume $a,b \notin F^2$ and $ab \in F^2$. Since $\det(\alpha \perp -\beta) = ab \in F^2$, $\alpha \perp -\beta$ is anisotropic or hyperbolic over F . In the first case, $D(\alpha) \cap D(\beta) = \emptyset$ and in the second case, $\alpha \cong \beta$ so $D(\alpha) = D(\beta)$.

Now assume $a,b,ab \notin F^2$. Since $\det(\alpha \perp -\beta) \notin F^2$, $\alpha \perp -\beta$ is isotropic [L, p. 158] so $D(\alpha) \cap D(\beta) \neq \emptyset$. Since $a,b \notin F^2$, α and β are both anisotropic and thus by the nondegeneracy of the Hilbert symbol [L, p. 158], we conclude that α and β each represent exactly one half

of the square classes of $\dot{F}$. Therefore $D(\alpha) \cup D(\beta) \neq \dot{F}$. To show $D(\alpha) - D(\beta)$ and $D(\beta) - D(\alpha)$ are each non-empty sets, it is sufficient to show $D(\alpha) \neq D(\beta)$. Suppose $D(\alpha) = D(\beta)$. Then since $1 \in D(\beta)$, a determinant argument shows $\beta = \langle 1, -b \rangle$. Using the Hilbert symbol, it follows for all $t \in \dot{F}$ that $(a, t)_F = (b, t)_F$ which is equivalent to $(ab, t)_F = 1$. The nondegeneracy of the Hilbert symbol shows $ab \in F^2$ which is a contradiction. Therefore $D(\alpha) \neq D(\beta)$.

(2.5) Theorem. Let K/F be a finite extension of number fields. Let $\alpha = \langle 1, -a \rangle$ and $\beta = c\langle 1, -b \rangle$ where $a,b,c \in \dot{F}$. Let

$$A = \{p \in E(K/F) \mid a,b,ab \notin F_p^2\} ,$$

$$B = \{p \in E(K/F) \mid a \in F_p^2 , b \notin F_p^2\} ,$$

$$C = \{p \in \Omega(F) \mid \alpha \perp -\beta \text{ is anisotropic over } F_p\} .$$

Assume $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$. Then $D_F(\alpha) \cap D_K(\beta) = \emptyset$, i.e., $(\alpha, \beta, K/F)$ does not satisfy SCV if and only if $A = B = \emptyset$ and $|C|$ is odd.

Proof: Let T_0 be the set of primes p in $\Omega(F)$ that contains all dyadic primes, all infinite primes, and those finite primes p for which either α or β is not isometric to a unit form over F_p . If $B \neq \emptyset$, let T_0

also contain one prime p from B. Clearly T_0 is a finite set.

Let $T = T_0 \cup A \cup C$. The set A is finite since it can contain only finitely many nondyadic primes p, namely those p that divide the ideals (a) or (b). The set C is finite because a 4-dimensional form is anisotropic over F_p for only finitely many primes p [L, p. 150]. Therefore T is a finite set.

Let $m = \prod_{p \in T} p^{e(p)}$ be a modulus with sufficiently large exponents such that $F_{m,1} \subseteq F_p^2$ for all $p \in T$.

We now show that for each $p \in \Omega(F)$, we can choose $r_p \in \dot{F}_p$ such that $r_p \in D_{F_p}(\alpha) \cap D_{K_P}(\beta)$ for every $P|p$, $P \in \Omega(K)$. Since $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$, $\alpha \perp -\beta$ is isotropic over K and hence over all K_P. It follows from Springer's theorem that if $[K_P:F_p]$ is odd then $\alpha \perp -\beta$ is isotropic over F_p. In particular if $p \notin E(K/F)$ then $[K_P:F_p]$ is odd for some $P|p$ and so we can choose $r_p \in D_{F_p}(\alpha) \cap D_{F_p}(\beta)$. If $p \in E(K/F)$, then $\dot{F}_p \subseteq D_{K_P}(\beta)$ for each $P|p$. This occurs since for every $r_p \in \dot{F}_p$, the ternary form $\beta \perp -\langle r_p \rangle$ is isotropic over K_P since $[K_P:F_p]$ is even (see [L, p. 157] or [S, p. 194]). Thus when $p \in E(K/F)$, we choose $r_p \in D_{F_p}(\alpha)$.

Using the approximation theorem [J, p. 109], choose $r \in \dot{F}$ such that $\langle r \rangle \cong_{F_p} \langle r_p \rangle$ for all $p \in T$. Let

$R = \{p_1, \ldots, p_n\}$ be the (possibly empty) set of primes p not in T such that $\mathrm{ord}_p(r)$ is odd. By the generalized Dirichlet theorem there is a prime ideal q in the coset $i(F_{m,1})(p_1 \cdots p_n)^{-1}$ such that $q \notin T \cup R$. Thus there exists $x \in F_{m,1}$ such that $q = (x)(p_1 \cdots p_n)^{-1}$ whence $(x) = (p_1 \cdots p_n)q$.

For each $p \in T$, we have $r \in D_{F_p}(\alpha)$ and $x \in F_{m,1} \subseteq F_p^2$ and thus $\alpha \perp -\langle rx \rangle$ is isotropic over F_p. For each $p \notin T \cup \{q\}$, $\mathrm{ord}_p(rx)$ is even and thus $\alpha \perp -\langle rx \rangle$ is a ternary unit form. Therefore $\alpha \perp -\langle rx \rangle$ is isotropic over F_p since p is a finite nondyadic prime [L, p. 147]. Since $\alpha \perp -\langle rx \rangle$ is a ternary form, we conclude by Hilbert reciprocity [OM, 71:18] that $\alpha \perp -\langle rx \rangle$ is also isotropic over F_q. Therefore by the Hasse-Minkowski theorem [L, p. 168], $\alpha \perp -\langle rx \rangle$ is isotropic over F and so $rx \in D_F(\alpha)$.

If $p \in T - E(K/F)$, then $\beta \perp -\langle rx \rangle$ is isotropic over F_p because $x \in F_p^2$, $\langle r \rangle \cong_{F_p} \langle r_p \rangle$, and $r_p \in D_{F_p}(\beta)$. If $p \notin T \cup \{q\}$, then $\beta \perp -\langle rx \rangle$ is isotropic over F_p for the reasons given in the paragraph above. Since $\mathrm{ord}_q(rx)$ is odd, β is a unit form over F_q, and q is nondyadic, it follows that $\beta \perp -\langle rx \rangle$ is anisotropic over F_q if and only if β is anisotropic over F_q; i.e. if and only if $b \notin F_q^2$.

Let $n(r)$ be the number of primes p in $T \cap E(K/F)$

such that $\beta \perp -\langle rx \rangle$ is anisotropic over F_p. Note that $n(r)$ is independent of x since $x \in F_{m,1} \subseteq F_p^2$ for $p \in T$. By Hilbert reciprocity, $\beta \perp -\langle rx \rangle$ is anisotropic over F_p for an even number of primes p. Therefore $\beta \perp -\langle rx \rangle$ is anisotropic over F_q if and only if $n(r)$ is odd.

If r can be chosen subject to the restrictions above so that $n(r)$ is even, then $rx \in D_F(\alpha) \cap D_K(\beta)$. This is because $n(r)$ even implies $b \in F_q^2$ and so $rx \in D_{F_q}(\beta)$. This would show $rx \in D_{F_p}(\beta)$ for all p not in $E(K/F)$. Then $rx \in D_{K_p}(\beta)$ for all $P \in \Omega(K)$ since $\dot{F}_p \subseteq D_{K_p}(\beta)$ when $p \in E(K/F)$ and $P|p$. It follows from the Hasse-Minkowski theorem that $rx \in D_K(\beta)$.

Suppose there exists $p \in A$. Then since $A \subseteq T$, by lemma (2.4) we can make $n(r)$ even by choosing r_p such that $r_p \in D_{F_p}(\alpha) \cap D_{F_p}(\beta)$ or $r_p \in D_{F_p}(\alpha) - D_{F_p}(\beta)$, whichever is appropriate. Suppose there exists $p \in B$. By the construction of T, we can assume $p \in T$. Since $a \in F_p^2$ and $b \notin F_p^2$, it follows that α is isotropic and β is anisotropic over F_p. Since $\dim \beta = 2$, β represents exactly one half of the square classes of $\dot{F}_p$ and $\dot{F}_p \subseteq D_{F_p}(\alpha)$. Therefore $n(r)$ can be made even just as above. Therefore, if A or B is nonempty, then $D_F(\alpha) \cap D_K(\beta) \neq \emptyset$.

Now assume $A = B = \emptyset$. Under this assumption, we now show that $|C| = n(r)$. It will then follow that $|C|$ even implies $n(r)$ even, so $D_F(\alpha) \cap D_K(\beta) \neq \emptyset$. Suppose $\beta \perp -\langle rx \rangle$ is anisotropic over F_p for some $p \in T \cap E(K/F)$. Then β is anisotropic over F_p and $b \notin F_p^2$. But $p \in E(K/F)$ and $B = \emptyset$ so $a \notin F_p^2$. Therefore $ab \in F_p^2$ since $A = \emptyset$. It follows from lemma (2.4) that $D_{F_p}(\alpha)$ and $D_{F_p}(\beta)$ are either equal or disjoint and consequently since $rx \in D_{F_p}(\alpha)$, we see that $rx \notin D_{F_p}(\beta)$ implies $\alpha \perp -\beta$ is anisotropic over F_p . Now suppose $p \in T \cap E(K/F)$, where $\alpha \perp -\beta$ is anisotropic over F_p . Then $D_{F_p}(\alpha)$ and $D_{F_p}(\beta)$ are disjoint and since $rx \in D_{F_p}(\alpha)$, we conclude $rx \notin D_{F_p}(\beta)$ and so $\beta \perp -\langle rx \rangle$ is anisotropic over F_p . Therefore $n(r)$ equals the number of primes p in $T \cap E(K/F)$ where $\alpha \perp -\beta$ is anisotropic over F_p . This number is $|C|$ because $C \subseteq T$ and $\alpha \perp -\beta$ is isotropic over F_p when $p \notin E(K/F)$. The last two paragraphs show $D_F(\alpha) \cap D_K(\beta) = \emptyset$ implies $A = B = \emptyset$ and $|C|$ is odd.

Now assume $r \in D_F(\alpha) \cap D_K(\beta)$. We must show $A \neq \emptyset$ or $B \neq \emptyset$ or $|C|$ is even. It is sufficient to assume $A = B = \emptyset$ and prove $|C|$ is even. Suppose $\alpha \perp -\beta$ is anisotropic over F_p . Since $r \in D_{F_p}(\alpha)$, it follows

$\beta \perp -\langle r \rangle$ is anisotropic over F_p. Now suppose $\beta \perp -\langle r \rangle$ is anisotropic over F_p. Since $\beta \perp -\langle r \rangle$ is isotropic over K_P for each $P \in \Omega(K)$ it follows $[K_P:F_p]$ is even for each $P|p$ and thus $p \in E(K/F)$. Since β is anisotropic over F_p we see $b \notin F_p^2$ and thus $a \notin F_p^2$ because $B = \emptyset$. Therefore $ab \in F_p^2$ since $A = \emptyset$. By lemma (2.4), $D_{F_p}(\alpha)$ and $D_{F_p}(\beta)$ are disjoint because $r \in D_{F_p}(\alpha)$ and $r \notin D_{F_p}(\beta)$. Thus $\alpha \perp -\beta$ is anisotropic over F_p. Therefore $\alpha \perp -\beta$ is anisotropic over F_p if and only if $\beta \perp -\langle r \rangle$ is anisotropic over F_p. The latter occurs for an even number of primes by Hilbert reciprocity and so we conclude $|C|$ is even.

(2.6) Corollary. With the same hypotheses of the previous theorem, let $B' = \{p \in E(K/F) \mid a \notin F_p^2, b \in F_p^2\}$. Then $D_F(\alpha) \cap D_K(\beta) = \emptyset$ and $D_K(\alpha) \cap D_F(\beta) = \emptyset$, i.e., $(\alpha, \beta, K/F)$ does not satisfy SCV' if and only if $A = B = B' = \emptyset$ and $|C|$ is odd.

Proof: The result is immediate if the previous theorem is applied to $c(\beta \perp -\alpha) \cong_F \langle 1, -b\rangle \perp -c\langle 1, -a\rangle$.

(2.7) Theorem. Let K/F be a finite extension of number fields, $\alpha = \langle 1, -a\rangle$, and $\beta = c\langle 1, -b\rangle$, $a,b,c \in \dot{F}$. Then $(\alpha, \beta, K/F)$ satisfies SCV' if and only if

$(\alpha, \beta, K/F)$ satisfies CV.

Proof: If $(\alpha, \beta, K/F)$ satisfies SCV', then clearly $(\alpha, \beta, K/F)$ satisfies CV. Suppose $(\alpha, \beta, K/F)$ satisfies CV. Then there exists $r \in D_K(\alpha) \cap D_K(\beta) \cap \dot{F}$. In order to show that $(\alpha, \beta, K/F)$ satisfies SCV', it is sufficient to assume $A = B = B' = \emptyset$ and prove that $|C|$ is even. The assumption $A = B = B' = \emptyset$ implies $ab \in F_p^2$ whenever $p \in E(K/F)$.

We have $\alpha \cong_K \langle r, -ar\rangle$ and $\beta \cong_K \langle r, -br\rangle$ and hence $\alpha \perp -\beta \cong_K \langle r, -r\rangle \perp -ar\langle 1, -ab\rangle \cong_K H \perp \delta$ where $\delta = -ar\langle 1, -ab\rangle$. If $p \notin E(K/F)$, $\alpha \perp -\beta \cong_{F_p} H \perp \delta$ by Springer's theorem, since $[K_P:F_p]$ is odd for some $P|p$. If $p \in E(K/F)$, then $ab \in F_p^2$ and $H \perp \delta$ is hyperbolic over F_p. On the other hand, $\alpha \perp -\beta$ is either anisotropic or hyperbolic over F_p.

Let $S_p(\gamma)$ be the Hasse symbol of an arbitrary form γ defined over F_p [OM, p. 167]. The product $\prod_{p\in\Omega(F)} S_p(\gamma)$ always equals 1 [OM, 72:1]. We have $S_p(\alpha \perp -\beta) = S_p(H \perp \delta)$ if $p \notin E(K/F)$ or if $\alpha \perp -\beta$ is hyperbolic over F_p and $p \in E(K/F)$. If $p \in E(K/F)$ and $\alpha \perp -\beta$ is anisotropic over F_p, then $S_p(\alpha \perp -\beta) = -S_p(H \perp \delta)$ because both forms have the same dimension and determinant, but they are not isometric over F_p [OM, 63:20]. Since $\prod_{p\in\Omega(F)} S_p(\alpha \perp -\beta) = \prod_{p\in\Omega(F)} S_p(H \perp \delta)$, it fol-

lows that $\alpha \perp -\beta$ is anisotropic over F_p for an even number of primes p and therefore $|C|$ is even.

(2.8) Proposition. Suppose K/F satisfies $CV(2,2)$. Then K/F is an excellent extension for 4-dimensional forms.

Proof: Let γ be a 4-dimensional form defined over F that is isotropic over K. Let $\gamma = \langle a_1, a_2, -b_1, -b_2 \rangle$, $\alpha = \langle a_1, a_2 \rangle$, and $\beta = \langle b_1, b_2 \rangle$ where $a_1, a_2, b_1, b_2 \in \dot{F}$. Since $\alpha \perp -\beta$ is isotropic over K and K/F satisfies $CV(2,2)$, it follows there exists $r \in D_K(\alpha) \cap D_K(\beta) \cap \dot{F}$. Then $\alpha \cong_K \langle r, ra_1a_2 \rangle$ and $\beta \cong_K \langle r, rb_1b_2 \rangle$. Thus $\alpha \perp -\beta \cong_K H \perp \langle ra_1a_2, -rb_1b_2 \rangle = H \perp \delta$ where δ is a form defined over F. Therefore K/F is excellent for 4-dimensional forms.

The following lemma is a slight improvement of one appearing in [Wr, lemma 3.2].

(2.9) Lemma. Let F be a number field, $d \in \dot{F} - F^2$ and q a noncomplex prime in $\Omega(F)$ such that $d \in F_q^2$. Then there exists a 4-dimensional form γ defined over F such that $\det \gamma = d$, γ is anisotropic over F_q, and γ is isotropic over F_p for each $p \in \Omega(F) - \{q\}$.

Proof: Using the global square theorem [OM, 65:15], fix a prime $q' \neq q$ such that q' is finite, nondyadic, and $d \notin F_{q'}^2$. For each prime $p \neq q,q'$ let $\gamma_p = \langle d, -1, -1, 1\rangle$. Let γ_q be a 4-dimensional anisotropic form over F_q [L, p. 158]. Since $\det \gamma_q \in F_q^2$ [L, p. 158] and $d \in F_q^2$ it follows that for each $p \neq q'$, $\det \gamma_p = d$. A form $\gamma_{q'}$ defined over $F_{q'}$ will be specified below.

Let $S_p(\gamma_p)$ be the Hasse symbol of γ_p over F_p. Let $e = \prod_{p \neq q'} S_p(\gamma_p)$. Then e equals either 1 or -1. Let $\gamma_{q'}$ be the 4-dimensional form defined over $F_{q'}$ that has determinant d and $S_{q'}(\gamma_{q'}) = e$ [OM, p. 171]. Then $\gamma_{q'}$ is isotropic over $F_{q'}$ since $d \notin F_{q'}^2$. Since $\prod_{p \in \Omega(F)} S_p(\gamma_p) = 1$, there exists a form γ defined over F such that $\dim \gamma = 4$, $\det \gamma = d$, and $\gamma \cong_{F_p} \gamma_p$ for each $p \in \Omega(F)$ [OM, 72:1]. Therefore γ is isotropic over F_p for $p \in \Omega(F) - \{q\}$ and γ is anisotropic over F_q.

(2.10) Theorem. Let F be a number field and suppose a finite extension K/F is excellent for 4-dimensional forms. Then either $E(K/F) = \emptyset$ or for each $d \in \dot{F} - F^2$ there exists $p = p(d) \in E(K/F)$ such that $d \notin F_p^2$.

Proof: Let $d \in \dot{F} - F^2$. We may assume $E(K/F) \neq \emptyset$ so let $q \in E(K/F)$. If $d \notin F_q^2$, then we are done. Assume that $d \in F_q^2$. Since $q \in E(K/F)$, q is not a complex prime. By lemma (2.9) there exists a 4-dimensional form γ defined over F such that $\det \gamma = d$ and γ is anisotropic over F_q while it is isotropic over F_p for each $p \in \Omega(F) - \{q\}$. Since $q \in E(K/F)$, γ is isotropic over K_p for each $P|q$ because a 4-dimensional anisotropic form defined over a p-adic field is hyperbolic in an extension of even degree (see [L, p. 157] or [S, p. 194]. Therefore γ is isotropic over K_p for each $P \in \Omega(K)$ and so γ is isotropic over K by the Hasse-Minkowski theorem.

Since K/F is excellent for 4-dimensional forms and γ is isotropic over K, there exists a form δ defined over F such that $\det \delta = -d$ and $\gamma \cong_K H \perp \delta$. If $p \notin E(K/F)$, then $\gamma \cong_{F_p} H \perp \delta$ by Springer's theorem and hence $S_p(\gamma) = S_p(H \perp \delta)$. If $p \in E(K/F) - \{q\}$ and $d \in F_p^2$, then $\gamma \cong_{F_p} H \perp \delta$ because both forms are hyperbolic over F_p since they are isotropic and their determinants lie in F_p^2. Therefore $S_p(\gamma) = S_p(H \perp \delta)$ in this case also. We also have $S_q(\gamma) = -S_q(H \perp \delta)$ because both forms have the same dimension and determinant over F_q but one is anisotropic and the other is isotropic over F_q. Since $\prod_{p \in \Omega(F)} S_p(\gamma) = \prod_{p \in \Omega(F)} S_p(H \perp \delta)$, it follows there is another prime p' such that $S_{p'}(\gamma) = -S_{p'}(H \perp \delta)$.

The only possibility is that $p' \in E(K/F)$ and $d \notin F_{p'}^2$.

(2.11) Theorem. Let K/F be a finite extension of number fields. Suppose either $E(K/F) = \emptyset$ or for each $d \in \dot{F} - F^2$ there exists $p = p(d) \in E(K/F)$ such that $d \notin F_p^2$. Then K/F satisfies SCV'(2,2).

Proof: Let α and β be binary forms defined over F such that $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$. We can scale to assume $\alpha = \langle 1, -a\rangle$ and $\beta = c\langle 1, -b\rangle$, $a,b,c \in \dot{F}$. Suppose first that $E(K/F) = \emptyset$. Then for each $p \in \Omega(F)$, there exists $P \in \Omega(K)$ such that $P|p$ and $[K_p:F_p]$ is odd. Since $\alpha \perp -\beta$ is isotropic over K and hence K_p, it follows by Springer's theorem that $\alpha \perp -\beta$ is isotropic over F_p for each $p \in \Omega(F)$. Therefore $\alpha \perp -\beta$ is isotropic over F by the Hasse-Minkowski theorem and $D_F(\alpha) \cap D_F(\beta) \neq \emptyset$.

Now suppose $E(K/F) \neq \emptyset$. Assume first that $ab \in F^2$. Since $\alpha \perp -\beta$ is isotropic over K and $\det(\alpha \perp -\beta) = ab \in F^2$, it follows $\alpha \perp -\beta$ is hyperbolic over K and thus any ternary subform of $\alpha \perp -\beta$ is isotropic over K [L, p. 27]. In particular $\langle 1\rangle \perp -\beta$ is isotropic over K so $1 \in D_F(\alpha) \cap D_K(\beta)$. Now assume $ab \notin F^2$. By hypothesis, there exists $p \in E(K/F)$ such that $ab \notin F_p^2$. It follows that at least one of $\{a,b\}$ is not in F_p^2. Therefore by corollary (2.6), one of the sets A,B,B' de-

fined in (2.5) and (2.6) is nonempty so either $D_F(\alpha) \cap D_K(\beta) \neq \emptyset$ or $D_K(\alpha) \cap D_F(\beta) \neq \emptyset$. Thus $(\alpha, \beta, K/F)$ satisfies SCV' in each case and so K/F satisfies SCV'(2,2).

The first paragraph of the proof of theorem (2.11) shows the following:

(2.12) Corollary. Let K/F be a finite extension of number fields. If $E(K/F) = \emptyset$, then every anisotropic form defined over F is anisotropic over K.

The converse of corollary (2.12) is also true. The corollary and its converse appear in [Wr, p. 647].

(2.13) Definition. Let F be a number field. A nonempty set $S \subseteq \Omega(F)$ is a global square set if $d \in \dot{F} \cap F_p^2$ for each $p \in S$ implies $d \in F^2$.

This statement is simply the contrapositive of the condition on $E(K/F)$ in (2.11). Collecting the results in (2.7), (2.8), (2.10), and (2.11) gives the following theorem.

(2.14) Theorem. Let K/F be a finite extension of number fields. The following statements are equivalent.

1) K/F satisfies SCV'(2,2).

2) K/F satisfies CV(2,2).

3) K/F is excellent for 4-dimensional forms.

4) If $E(K/F) \neq \emptyset$, then $E(K/F)$ is a global square set.

(2.15) Corollary. Let $K \subseteq K' \subseteq K$ be a tower of number fields. If K'/F satisfies CV(2,2) and $E(K'/F) \neq \emptyset$, then K/F satisfies CV(2,2).

Proof: Since $E(K'/F)$ is a global square set by theorem (2.14) and $E(K'/F) \subseteq E(K/F)$, it is clear from definition (2.13) that $E(K/F)$ is a global square set. Then K/F satisfies CV(2,2) by theorem (2.13).

Later we shall remove the dimension restriction in 3) above. By (2.14) and (2.6), if $d \in \dot{F} - F^2$ and $d \in F_p^2$ for each $p \in E(K/F)$, then statement 4) in (2.14) fails and thus $(\alpha, \beta, K/F)$ doesn't satisfy SCV' for some pair of binary forms α, β where $\det(\alpha \perp -\beta) = d$. The following proposition and corollary show we can also specify $\det \alpha$ and $\det \beta$ as long as neither is a square in F and $\det \alpha \cdot \det \beta = d$.

(2.16) Proposition. Let $a,b,ab \in \dot{F} - F^2$. Then there exists $c \in \dot{F}$ such that $\alpha = \langle 1, -a \rangle$, $\beta = c\langle 1, -b \rangle$

and $\alpha \perp -\beta$ is anisotropic over F_p for exactly one prime $p \in \Omega(F)$.

Proof: By (2.3) there exist infinitely many primes $p \in \Omega(F)$ such that $a,b \notin F_p^2$. Of these primes p only finitely many are such that $ab \notin F_p^2$ since this could occur only for dyadic primes and primes that divide the ideals (a) or (b). Therefore there exists $q \in \Omega(F)$ such that $a,b \notin F_q^2$ and $ab \in F_q^2$. Also by (2.3), there exists $\ell \in \Omega(F)$ such that $a \in F_\ell^2$ and $b \notin F_\ell^2$. Thus $ab \notin F_\ell^2$.

For each $p \in \Omega(F) - \{\ell\}$ we define a form β_p over F_p as follows. Let $\beta_p = \langle 1, -b\rangle$ if $p \neq q,\ell$. Let $\beta_q = c_q\langle 1, -b\rangle$ where $c_q \in \dot{F}_q$ and $c_q \notin D_{F_q}(\langle 1, -b\rangle)$. This is possible since $b \notin F_q^2$ and so $\langle 1, -b\rangle$ represents exactly one half of the square classes of F_q by the non-degeneracy of the Hilbert symbol. The product $\prod_{p\neq\ell} S_p(\beta_p) = e$ where e equals 1 or -1 . Since $b \notin F_\ell^2$, there exists $c_\ell \in F_\ell$ such that if $\beta_\ell = c_\ell\langle 1, -b\rangle$, then $S_\ell(\beta_\ell) = e$ [OM, 63:23]. Since $\prod_p S_p(\beta_p) = 1$ and $\det \beta_p = -b$ for all $p \in \Omega(F)$, it follows that there exists a form β defined over F such that $\det \beta = -b$ and $\beta \cong_{F_p} \beta_p$ for each $p \in \Omega(F)$ [OM, 72:1]. Therefore $\beta \cong c\langle 1, -b\rangle$ for some $c \in \dot{F}$.

If $p \neq q,\ell$, then $\alpha \perp -\beta$ is isotropic over F_p

since $\alpha \perp -\beta \cong_{F_p} \langle 1, -a\rangle \perp -\langle 1, -b\rangle \cong_{F_p} H \perp \langle -a, b\rangle$.

Also, $\alpha \perp -\beta$ is isotropic over F_ℓ since $\det(\alpha \perp -\beta) = ab \notin F_\ell^2$. Finally we note $\alpha \perp -\beta$ is anisotropic over F_q . This is because $ab \in F_q^2$ and so $\langle 1, -a\rangle \cong_{F_q} \langle 1, -b\rangle$. If $\alpha \perp -\beta$ were isotropic over F_q , then $\alpha \perp -\beta$ would be hyperbolic over F_q and thus any 3-dimensional subform would be isotopic over F_q . But $\langle 1, -a\rangle \perp -\langle c_q\rangle$ is not isotropic over F_q because $c_q \notin D_{F_q}(\langle 1, -b\rangle) = D_{F_q}(\langle 1, -a\rangle)$. Therefore $\alpha \perp -\beta$ is anisotropic over F_p only when $p = q$.

(2.17) Corollary. Suppose $E(K/F) \neq \emptyset$, $d \in \dot{F} - F^2$, and $d \in F_p^2$ for each $p \in E(K/F)$. Let $a,b \in \dot{F} - F^2$ such that $ab = d$. Then there exists $c \in \dot{F}$ such that $\alpha = \langle 1, -a\rangle$, $\beta = c\langle 1, -b\rangle$, and $\alpha \perp -\beta$ is anisotropic over F_p for an odd number of primes p . In particular, using the notation of corollary (2.6), $A = B = B' = \emptyset$ and $|C|$ is odd.

Proof: By the previous proposition there exists $c \in \dot{F}$ such that $|C|$ is odd. It is clear that $A = B = B' = \emptyset$ because when $p \in E(K/F)$, $ab = d \in F_p^2$.

Next we consider in more detail the case of a quadratic extension K/F . Quadratic extensions yield the easiest

examples that show SCV(2,2) and CV(2,2) are not equivalent properties. We recall from Chapter I (1.20) that $N_F(x)$ is defined to be $D_F(\langle 1, -x\rangle)$ and that if $K = F(\sqrt{a})$ is a quadratic extension of F and $x \in \dot{F}$, then $D_{F(\sqrt{a})}(\langle 1, -x\rangle) \cap \dot{F} = N_F(x) \cdot N_F(ax)$.

(2.18) Proposition. Let K/F be a quadratic extension of number fields. Let $\alpha = \langle 1, -a\rangle$, $\beta = c\langle 1, -b\rangle$ where $a,b,c \in \dot{F}$ and suppose $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$. Then $(\alpha, \beta, K/F)$ satisfies CV and if $K \neq F(\sqrt{a})$ then $(\alpha, \beta, K/F)$ satisfies SCV.

Proof: Let $K = F(\sqrt{d})$. Then $E(K/F) = \{p \in \Omega(F) \mid d \notin F_p^2\}$. If either a or $b \in F^2$, then $D_F(\alpha) \cap D_F(\beta) \neq \emptyset$. If either $ab \in F^2$ or $K = F(\sqrt{ab})$, then $\alpha \perp -\beta$ is hyperbolic over K since $\det(\alpha \perp -\beta) = ab \in K^2$. Thus the ternary subform $\langle 1\rangle \perp -\beta$ is isotropic over K so $1 \in D_F(\alpha) \cap D_K(\beta)$. Also if $K = F(\sqrt{b})$, then $1 \in D_F(\alpha) \cap D_K(\beta)$. Therefore in each of these cases, $(\alpha, \beta, K/F)$ satisfies SCV and CV.

Now assume $a,b,ab \notin F^2$ and $K \neq F(\sqrt{b})$, $F(\sqrt{ab})$. Then $[F(\sqrt{a}, \sqrt{b}):F] = 4$. Suppose that $K = F(\sqrt{d}) \neq F(\sqrt{a})$. Then K is not a quadratic subfield of $F(\sqrt{a}, \sqrt{b})$ and hence $[F(\sqrt{a}, \sqrt{b}, \sqrt{d}):F] = 8$. It follows from (2.3) that there exists $p \in \Omega(F)$ such that $a \in F_p^2$ and $b,d \notin F_p^2$. Since $d \notin F_p^2$, $p \in E(K/F)$ and hence the set

B defined in theorem (2.5) is nonempty. Therefore $(\alpha, \beta, K/F)$ satisfies SCV and CV. Now suppose $K = F(\sqrt{a})$. Since $[F(\sqrt{a}, \sqrt{b}):F] = 4$, by (2.3) there exists $p \in \Omega(F)$ such that $a \notin F_p^2$ and $b \in F_p^2$. It follows $d \notin F_p^2$ because $ad \in F^2$. Therefore $p \in E(K/F)$ and set B' defined in corollary (2.6) is nonempty so $(\alpha, \beta, K/F)$ satisfies SCV' and hence CV.

The following proposition is a special case of (2.5).

(2.19) Proposition. Let $K = F(\sqrt{a})$ be a quadratic extension of a number field F. Let $\alpha = \langle 1, -a\rangle$ and $\beta = c\langle 1, -b\rangle$ where $a,b,c \in \dot{F}$. Then $(\alpha, \beta, K/F)$ fails to satisfy SCV if and only if $A = \emptyset$ and $|C|$ is odd where A and C are as in theorem (2.5).

Proof: The condition $D_K^{\cdot}(\alpha) \cap D_K(\beta) \neq \emptyset$ is satisfied because α is hyperbolic over K. Since $E(K/F) = \{p \in \Omega(F) \mid a \notin F_p^2\}$, the set B is empty.

(2.20) Proposition. Let F be a number field and suppose $a,b,ab \in \dot{F} - F^2$. Let $K = F(\sqrt{a})$ and let $A' = \{p \in \Omega(F) \mid a,b,ab \notin F_p^2\}$. Then $N_F(a)N_F(b)N_F(ab) = \dot{F}$ if and only if $A' \neq \emptyset$.

Proof: We first observe that the following numbered

statements are equivalent.

i) $N_F(a)N_F(b)N_F(ab) \neq \dot{F}$.

ii) There exists $c \in \dot{F}$ such that $c \notin N_F(a)N_F(b)N_F(ab)$.

iii) There exists $c \in \dot{F}$ such that $N_F(a) \cap cN_F(b)N_F(ab) = \emptyset$.

iv) There exists $c \in \dot{F}$ such that $D_F(\langle 1, -a\rangle) \cap (D_{F(\sqrt{a})}(c\langle 1, -b\rangle) \cap \dot{F}) = \emptyset$.

v) There exists $c \in \dot{F}$ such that $(\alpha, \beta, K/F)$ does not satisfy SCV where $\alpha = \langle 1, -a\rangle$ and $\beta = c\langle 1, -b\rangle$.

vi) $A' = \emptyset$ and $|C|$ is odd where C has its usual meaning. (Note that $A' = A$ when $K = F(\sqrt{a})$.)

This shows $A' \neq \emptyset$ implies $N_F(a)N_F(b)N_F(ab) = \dot{F}$. Suppose $A' = \emptyset$. By proposition (2.16), there exists $c \in \dot{F}$ such that $|C|$ is odd. Therefore $A' = \emptyset$ implies $N_F(a)N_F(b)N_F(ab) \neq \dot{F}$.

(2.21) Example. (Shapiro) Let $F = \mathbb{Q}$ and $a = -1$. Let b be a prime in $\mathbb{Z}$. If $b \equiv 1 \pmod 8$ then $N_F(-1)N_F(b)N_F(-b) \neq \dot{\mathbb{Q}}$. If $b \not\equiv 1 \pmod 8$, then

$N_F(-1)N_F(b)N_F(-b) = \dot{\mathcal{Q}}$.

Proof: If $b \equiv 3$ or $5 \pmod 8$, then $2 \in A'$ since none of -1 , b , $-b$ are squares in $\dot{\mathcal{Q}}_2$. If $b \equiv 7 \pmod 8$, then $b \in A'$ since none of -1 , b , $-b$ are squares in $\dot{\mathcal{Q}}_b$. If $b = 2$, then $2 \in A'$ since none of -1 , 2 , -2 are squares in $\dot{\mathcal{Q}}_2$. Therefore if $b \not\equiv 1 \pmod 8$ then $N_F(-1)N_F(b)N_F(-b) = \dot{\mathcal{Q}}$ because in each case $A' \neq \emptyset$.

If $b \equiv 1 \pmod 8$, then $A' = \emptyset$. This is because $p = 2$ and $p = b$ are the only possible primes in A' but $b \in \mathcal{Q}_2^2$ and $-1 \in \mathcal{Q}_b^2$. Therefore $N_F(-1)N_F(b)N_F(-b) \neq \dot{\mathcal{Q}}$ in this case.

(2.22) Lemma. Let α be a quadratic form defined over a number field F . For some finite set $T \subseteq \Omega(F)$, let $c_p \in D_{F_p}(\alpha)$ for each $p \in T$. Then there exists $c \in D_F(\alpha)$ such that $\langle c \rangle \cong_{F_p} \langle c_p \rangle$ for each $p \in T$.

Proof: Let $\alpha = \langle a_1, \ldots, a_n \rangle$ and let $c_p = \sum_{i=1}^{n} a_i x_{ip}^2$ where $x_{ip} \in F_p$. Using the approximation theorem, choose $x_i \in F$ so that for each $p \in T$, $\sum_{i=1}^{n} a_i x_i^2$ lies in the same square class in F_p as does $\sum_{i=1}^{n} a_i x_{ip}^2$. This can be done by a continuity argument be-

cause F is dense in each F_p and the group of squares in $\dot{F}_p$ forms an open set in F_p. Then $c = \sum_{i=1}^{n} a_i x_i^2 \in D_F(\alpha)$ and $\langle c \rangle \cong_{F_p} \langle c_p \rangle$ for each $p \in T$.

(2.23) Proposition. (Shapiro) Let $a \in \dot{F} - F^2$ where F is a number field. Then there exists $b \in \dot{F}$ such that $N_F(a)N_F(b)N_F(ab) \neq \dot{F}$.

Proof: The conclusion follows from (2.20) provided there exists $b, ab \in \dot{F} - F^2$ such that $A' = \emptyset$. Let $T = \{p \in \Omega(F) \mid \text{either } p \text{ is dyadic or } p \text{ divides } (a)\}$. Using lemma (2.22) applied to $\alpha = \langle 1, -a \rangle$, choose $b \in \dot{F}$ such that

1) $b \in F_b^2$ if $p \in T$

2) $b \in D_F(\langle 1, -a \rangle)$

3) $b \notin F^2 \cup aF^2$.

We show that $A' = \{p \in \Omega(F) \mid a, b, ab \notin F_p^2\}$ is empty. The only primes A' could contain are dyadic primes and primes that divide either (a) or (b). But $b \in F_p^2$ if p is dyadic or p divides (a). Suppose $p \mid (b)$. Then $p \notin T$ and so p is nondyadic and p doesn't divide (a). Since $\langle 1, -a, -b \rangle$ is isotropic over F and hence over F_p, it follows that $\langle 1, -a \rangle$ is isotropic over F_p and thus $a \in F_p^2$. Therefore $A' = \emptyset$.

(2.24) Proposition. Let $a \in \dot{F} - F^2$ where F is a number field. There exists $b \in \dot{F}$ such that $N_F(a)N_F(b)N_F(ab) = \dot{F}$ and $b, ab \notin F^2$.

Proof: By the global square theorem [OM, 65:15] there is a finite prime p such that $a \notin F_p^2$ and $p \nmid (a)$. Let $b \in \dot{F}$ such that $\mathrm{ord}_p(b) = 1$. One way to find b is to note that F is dense in F_p and to choose $b \in \dot{F}$ sufficiently close to a uniformizer π of F_p. Then $b, ab \notin F_p^2$ since $\mathrm{ord}_p(b) = \mathrm{ord}_p(ab) = 1$. Since $a \notin F_p^2$, we see that $p \in A'$. Since $A' \neq \emptyset$ for this choice of b, it follows from (2.20) that $N_F(a)N_F(b)N_F(ab) = \dot{F}$ and $b, ab \notin F^2$.

We now turn to the properties SCV(m,n) and CV(m,n) when $m, n \geq 2$ and $m+n \geq 5$.

(2.25) Theorem. (Shapiro) Let K/F be a finite extension of number fields. Then K/F satisfies SCV(m,n) when $n \geq 3$ and $m \geq 1$.

Proof: Let α and β be forms defined over F such that $\dim \alpha = m$ and $\dim \beta = n \geq 3$. Assume $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$. Since K/F satisfies SCV(1,n), we may assume $m \geq 2$.

Let $T = \{p \in \Omega(F) \mid \beta$ is anisotropic over $F_p\}$ and

let $T_0 = \{p \in \Omega(F) \mid \alpha \perp -\beta$ is anisotropic over $F_p\}$. Since $\dim \beta \geq 3$, β is anisotropic over F_p for any finite nondyadic prime p where β is a unit form, and this occurs for all but finitely many primes p. Therefore T is a finite set. Clearly T_0 is a subset of T and contains only real archimedean primes, since any form of dimension ≥ 5 is isotropic over a p-adic field or complex field.

For each $p \in T - T_0$, $\alpha \perp -\beta$ is isotropic over F_p so there exists $c_p \in D_{F_p}(\alpha) \cap D_{F_p}(\beta)$. By lemma (2.22) there exists $c \in D_F(\alpha)$ such that for $p \in T - T_0$, $\langle c \rangle \tilde{=}_{F_p} \langle c_p \rangle$. Since β is isotropic over F_p for p not in T, it follows $c \in D_{F_p}(\beta)$ for $p \notin T_0$. Since $\alpha \perp -\beta$ is isotropic over K and T_0 consists of real archimedean primes; if $P \in \Omega(K)$ and $P|p$ where $p \in T_0$, then P is a complex prime in $\Omega(K)$. It follows that $c \in D_{K_P}(\beta)$ for all $P \in \Omega(K)$ and hence by the Hasse-Minkowski theorem, $c \in D_K(\beta)$. Therefore $c \in D_F(\alpha) \cap D_K(\beta)$ and so K/F satisfies SCV(m,n) when $n \geq 3$.

(2.26) Corollary. Let K/F be a finite extension of number fields. Then K/F satisfies SCV'(m,n) for all ordered pairs of positive integers (m, n) except possibly

$(m, n) = (2, 2)$. The properties SCV' and CV are equivalent.

Proof: Let α , β be forms defined over F of dimensions m and n respectively and assume $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$. If $m+n \geq 5$, then one of m and n is ≥ 3 . It follows from the previous theorem that either $D_F(\alpha) \cap D_K(\beta) \neq \emptyset$ or $D_K(\alpha) \cap D_F(\beta) \neq \emptyset$ and thus $(\alpha, \beta, K/F)$ satisfies SCV'. If either m or n equals 1 , then $(\alpha, \beta, K/F)$ satisfies SCV'. Thus, unless $\dim \alpha = \dim \beta = 2$, it follows that $(\alpha, \beta, K/F)$ satisfies SCV'.

We have noted before that $(\alpha, \beta, K/F)$ satisfies SCV' implies $(\alpha, \beta, K/F)$ satisfies CV. Suppose $(\alpha, \beta, K/F)$ satisfies CV. Then $(\alpha, \beta, K/F)$ satisfies SCV' when $(m, n) \neq (2, 2)$ as shown above. If $(m, n) = (2, 2)$, then it follows from (2.7) that $(\alpha, \beta, K/F)$ satisfies SCV'.

(2.27) Theorem. Let K/F be a finite extension of number fields. Suppose K/F is excellent for 4-dimensional forms. Then K/F is excellent for arbitrary forms.

Proof: Let γ be a form defined over F that is isotropic over K . We must find a form δ defined over F such that $\gamma \cong_K H \perp \delta$. If $\dim \gamma = 2$, let $\delta = \langle 0 \rangle$. If $\dim \gamma = 3$, let $\delta = \langle -\det \gamma \rangle$. If $\dim \gamma = 4$, the form δ exists by hypothesis. Now assume $\dim \gamma \geq 5$.

Let $\gamma = \langle a_1, \ldots, a_n, -b_1, -b_2, -b_3 \rangle$, $\alpha = \langle a_1, \ldots, a_n \rangle$, and $\beta = \langle b_1, b_2, b_3 \rangle$. Thus $\alpha \perp -\beta$ is isotropic over K . By theorem (2.25) there exists $r \in D_F(\alpha) \cap D_K(\beta)$. Then $\alpha \cong_F \langle r, c_2, \ldots, c_n \rangle$ for some $c_i \in \dot{F}$ and $\delta' = \langle r, -b_1, -b_2, -b_3 \rangle$ is isotropic over K . Since K/F is excellent for 4-dimensional forms, there exists δ_1 defined over F such that $\delta' \cong_K H \perp \delta_1$. Letting $\delta_2 = \langle c_2, \ldots, c_n \rangle$, we have

$$\gamma \cong_K \alpha \perp -\beta \cong \delta_2 \perp \delta' \cong_K \delta_2 \perp H \perp \delta_1 \cong_K H \perp \delta$$

where $\delta = \delta_1 \perp \delta_2$ is defined over F .

(2.28) Theorem. Let K/F be a finite extension of number fields. Let α , β be forms defined over F where $\dim \alpha = m \geq 3$ and $\dim \beta = 2$. Suppose $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$ and let $D = \{p \in E(K/F) \mid b \notin F_p^2\}$ where $b = d(\beta)$. Then $(\alpha, \beta, K/F)$ fails to satisfy SCV if and only if all three of the following statements are satisfied.

i) The set D consists of real archimedean primes.

ii) If $p \in D$, α is anisotropic over F_p .

iii) The number of primes p in D such that $\alpha \perp -\beta$ is anisotropic over F_p is odd.

Proof: Let T_1 be the set of primes p in $\Omega(F)$ that contains all infinite primes, all dyadic primes, those

primes p such that α is anisotropic over F_p, and those primes p such that β is not a unit form over F_p. If there exists a finite prime $p' \in E(K/F)$ such that $b \notin F_{p'}^2$, then let $T = T_1 \cup \{p'\}$. If not, let $T = T_1$. Since $\dim \alpha \geq 3$, α is anisotropic over F_p for only finitely many primes p. In addition, β is a unit form over F_p for all but finitely many primes p. It follows that T is a finite set.

Let $m = \prod_{p \in T} p^{e(p)}$ be a modulus having sufficiently large exponents so that $F_{m,1} \subseteq F_p^2$ for each $p \in T$.

The same argument as in theorem (2.5) shows that for each $p \in \Omega(F)$ we can choose $r_p \in \dot{F}_p$ such that $r_p \in D_{F_p}(\alpha) \cap D_{K_P}(\beta)$ for each $P \in \Omega(K)$ where $P|p$. If $p \notin E(K/F)$, we choose $r_p \in D_{F_p}(\alpha) \cap D_{F_p}(\beta)$ and if $p \in E(K/F)$, then we have $r_p \in D_{F_p}(\alpha)$.

Using the approximation theorem, choose $r \in \dot{F}$ such that $\langle r \rangle \cong_{F_p} \langle r_p \rangle$ for each $p \in T$. Let $R = \{p_1, \ldots, p_n\}$ be the (possibly empty) set of primes p not in T such that $\mathrm{ord}_p(r)$ is odd. As in theorem (2.5) we conclude that there exists a prime $q \notin T \cup R$ and $x \in F_{m,1}$ such that $(x) = (p_1 \cdots p_n)q$. If $p \in T$, $\alpha \perp -\langle rx \rangle$ is isotropic over F_p since $r \in D_{F_p}(\alpha)$ and $x \in F_{m,1} \subseteq F_p^2$.

If $p \notin T$, α is isotropic over F_p and thus so is

$\alpha \perp -\langle rx \rangle$. By the Hasse-Minkowski theorem, $\alpha \perp -\langle rx \rangle$ is isotropic over F so $rx \in D_F(\alpha)$.

The reasoning in (2.5) also shows $\beta \perp -\langle rx \rangle$ is isotropic over F_p when $p \notin T \cup \{q\}$ and when $p \in T - E(K/F)$. Let $n(r)$ be the number of primes p in $T \cap E(K/F)$ such that $\beta \perp -\langle rx \rangle$ is anisotropic over F_p . Since $x \in F_p^2$ for $p \in T$, $n(r)$ is independent of x . By Hilbert reciprocity, $\beta \perp -\langle rx \rangle$ is anisotropic over F_p for an even number of primes p . Therefore, $n(r)$ is odd if and only if $\beta \perp -\langle rx \rangle$ is anisotropic over F_q . The argument in (2.5) shows this is equivalent to $b \notin F_q^2$.

Suppose $r \in \dot{F}$ is found subject to the requirements above such that $n(r)$ is even. Then $b \in F_q^2$ and so $\beta \perp -\langle rx \rangle$ is isotropic over F_q . It follows as in (2.5) that $rx \in D_F(\alpha) \cap D_K(\beta)$.

Suppose statement i) is not satisfied. If $D = \emptyset$, then $n(r) = 0$ because β is isotropic over F_p for each $p \in E(K/F)$ since $b \in F_p^2$ for these p . Thus $n(r)$ is even in this case. Now assume $D \neq \emptyset$. Then since i) does not hold, there exists a finite prime p' in $E(K/F)$ such that $b \notin F_{p'}^2$. According to the construction of T , we may assume $p' \in T$. Since β is a binary form and $b \notin F_{p'}^2$, β is anisotropic over $F_{p'}$ and represents over $F_{p'}$ exactly one half of the square classes of $\dot{F}_{p'}$ by the nondegeneracy of the Hilbert symbol. Since $\dim \alpha \geq 3$, α represents over $F_{p'}$ all but possibly one

square class of $\dot{F}_{p'}$, [L, p. 158]. Since p' is a finite prime, $\dot{F}_{p'}$ has at least four square classes. Therefore, $D_{F_{p'}}(\alpha) \cap D_{F_{p'}}(\beta)$ and $D_{F_{p'}}(\alpha) - D_{F_{p'}}(\beta)$ are both nonempty sets and it follows that $r_{p'} \in \dot{F}_{p}$ can be chosen from the appropriate set to make $n(r)$ even.

Suppose statement ii) is not satisfied. Then there exists $p \in D$ such that α is isotropic over F_p. Since $p \in D$, we have $b \notin F_p^2$ and so β is anisotropic over F_p. Noting that $D_{F_p}(\alpha) = \dot{F}_p$, we see as above that $D_{F_p}(\alpha) \cap D_{F_p}(\beta)$ and $D_{F_p}(\alpha) - D_{F_p}(\beta)$ are both nonempty sets and thus an appropriate choice of r_p in one of these sets makes $n(r)$ even.

Suppose statements i) and ii) are satisfied and statement iii) is not satisfied. Then $\alpha \perp -\beta$ is anisotropic over F_p for an even number of primes p in D. By i), the primes in D are real archimedean primes so $D \subseteq T \cap E(K/F)$. If $p \in T \cap E(K/F)$ and $\beta \perp -\langle rx \rangle$ is anisotropic over F_p, then $p \in D$. This follows since β is anisotropic over F_p and so $b \notin F_p^2$. Therefore $n(r)$ counts the number of primes $p \in D$ such that $\alpha \perp -\beta$ is anisotropic over F_p. For each $p \in D$, α is anisotropic over F_p by ii), β is anisotropic over F_p since $b \notin F_p^2$ and p is real by i). Thus α and β each represent over F_p exactly one square class. Since $rx \in D_{F_p}(\alpha)$,

we see that for $p \in D$, $\alpha \perp -\beta$ is anisotropic over F_p if and only if $\beta \perp -\langle rx \rangle$ is anisotropic over F_p. Since iii) fails, $\beta \perp -\langle rx \rangle$ is anisotropic over F_p for an even number of primes $p \in D$ and therefore $n(r)$ is even.

The previous three paragraphs show that if any of statements i)-iii) are not satisfied, then $n(r)$ can be made even and $(\alpha, \beta, K/F)$ satisfies SCV.

Now assume statements i)-iii) all hold. Suppose $r \in D_F(\alpha) \cap D_K(\beta)$. Let n be the number of primes $p \in \Omega(F)$ such that $\beta \perp -\langle r \rangle$ is anistropic over F_p. Then n is even by Hilbert reciprocity. If $p \notin E(K/F)$, then $r \in D_{F_p}(\alpha) \cap D_{F_p}(\beta)$ by Springer's theorem. If $p \in E(K/F)$ and $b \in F_p^2$, then $r \in D_{F_p}(\beta)$ since β is isotropic over F_p. If $p \in E(K/F)$ and $b \notin F_p^2$, then $p \in D$ and thus p is a real archimedean prime by i). For each $p \in D$, α and β are anisotropic over F_p by ii) and since $b \notin F_p^2$. Just as above, we conclude that for $p \in D$, $\alpha \perp -\beta$ is anisotropic over F_p if and only if $\beta \perp -\langle r \rangle$ is anisotropic over F_p. This occurs for an odd number of primes $p \in D$ by iii). Since $\beta \perp -\langle r \rangle$ is isotropic over F_p when $p \notin D$, this contradicts the fact that n is even. Therefore $D_F(\alpha) \cap D_K(\beta) = \emptyset$ and $(\alpha, \beta, K/F)$ doesn't satisfy SCV.

(2.29) Definition. Let F be a number field and let

$S \subseteq \Omega(F)$. A nonempty set S is a strong global square set if for any finite set $T \subseteq S$, $S - T$ is a global square set.

The global square theorem [OM, 65:15] implies that $\Omega(F)$ is a strong global square set. In Chapter III, we shall determine when $E(K/F)$ is a strong global square set.

It follows from definition (2.13) that if S is a global square set, then whenever $b \in \dot{F} - F^2$, there exists $p \in S$ such that $b \notin F_p^2$. If S is a strong global square set and $b \in \dot{F} - F^2$, then there exist infinitely many primes $p \in S$ such that $b \notin F_p^2$. Thus a strong global square set is infinite. It follows from the next lemma that a global square set is also infinite.

(2.30) Lemma. If $S \subseteq \Omega(F)$ is a global square set, then S is infinite.

Proof: Suppose $S = \{p_1, \ldots, p_n\}$. Let $q \in \Omega(F)-S$. Since F is dense in F_p for each $p \in \Omega(F)$, there exists by the approximation theorem $r \in \dot{F}$ such that $r \in F_p^2$ for $p \in S$ and $\mathrm{ord}_q(r) = 1$. Then $r \notin F^2$ since $r \notin F_q^2$. It follows S is not a global square set contradicting the hypothesis and therefore S is infinite.

(2.31) Theorem. Let K/F be a finite extension of

number fields. If $E(K/F) = \emptyset$ or if $E(K/F)$ is a strong global square set, then K/F satisfies $SCV(m,2)$, $m \geq 3$.

Proof: Let α and β be quadratic forms defined over F such that $\dim \alpha = m \geq 3$ and $\dim \beta = 2$. Assume $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$. If $E(K/F) = \emptyset$, then it follows from (2.12) that $D_F(\alpha) \cap D_F(\beta) \neq \emptyset$. Now assume $E(K/F)$ is a strong global square set. Let $\beta = c\langle 1, -b\rangle$. If $b \in F^2$, then β is isotropic over F and $D_F(\alpha) \cap D_F(\beta) \neq \emptyset$. If $b \notin F^2$, then $\{p \in E(K/F) \mid b \notin F_p^2\}$ is an infinite set by lemma (2.30) since $E(K/F) - T$ is a global square set for any finite set T. This shows set D defined in (2.28) is an infinite set and so it can't consist entirely of real archimedean primes. Therefore statement i) of (2.28) fails and so $D_F(\alpha) \cap D_K(\beta) \neq \emptyset$. It follows that K/F satisfies $SCV(m,2)$, $m \geq 3$.

The converse of this theorem does not hold. In fact very little can be concluded if K/F satisfies $SCV(m,2)$, $m \geq 3$. If F is a totally imaginary number field (that is, has no real archimedean primes) then K/F satisfies $SCV(m,2)$, $m \geq 3$ because statement i) of (2.28) fails. There exist nonexcellent extensions K/F where F is totally imaginary so $E(K/F)$ is not even a global square set. There are also nonexcellent extensions K/F where F is a number field that has a real archimedean prime such

that K/F satisfies SCV(m,2), $m \geq 3$. An example constructed by Waterhouse that appears in [Wr, p. 642] has this property. The extension is nonexcellent since $E(K/F)$ contains exactly one prime p and so $E(K/F)$ is not a global square set by lemma (2.30). The prime p is a finite prime so statement i) of (2.28) fails for each pair α, β and thus K/F satisfies SCV(m,2), $m \geq 3$.

In the next chapter we shall construct an excellent extension of number fields such that for each $m \geq 3$, there exists a form α_m defined over F of dimension m and a form β of dimension 2 defined over F such that $(\alpha_m, \beta, K/F)$ doesn't satisfy SCV. This will give an example of a set $E(K/F)$ that is a global square set but not a strong global square set, and also will show that the hypothesis in theorem (2.31) is necessary.

The results in (2.5), (2.6), (2.14), (2.25), (2.26), and (2.28) give complete characterizations of the properties SCV, SCV', and CV over number fields. We develop techniques in the next chapter to relate these properties to Galois theory.

We close this chapter by applying our results about number fields to the concepts introduced in Chapter I.

(2.32) Theorem. If K/F is a finite extension of number fields such that K contains a quadratic extension K' of F, then K/F satisfies CV(2,2). In particular,

every finite multiquadratic extension K/F of number fields satisfies CV(2,2).

Proof: The extension K'/F satisfies CV(2,2) by proposition (2.18). Since $E(K'/F) \neq \emptyset$ as is seen in the proof of (2.18), corollary (2.15) implies K/F satisfies CV(2,2). The last statement of the theorem is trivial.

(2.33) Theorem. Every subgroup G of a number field F has binary PE. Every number field F is 1-amenable for 4-dimensional forms.

Proof: This follows from theorems (2.32) and (1.24).

Remarks. The result in theorem (2.32) about 1-amenibility is not new. It has been shown in [ELW, p. 463] that number fields are 1-amenable for arbitrary forms.

For a field F, we have shown that if every finite multiquadratic extension K/F satisfies CV(2,2) then F is 1-amenable for 4-dimensional forms [theorem (1.24)] and K/F is excellent for 4-dimensional forms [proposition (2.8)]. In the case of number fields, we can make the stronger conclusion that K/F is excellent for arbitrary forms [theorem (2.27)]. It was shown in [ELW_I, p. 463] that for a field F, if every finite multiquadratic extension K/F is excellent, then F is 1-amenable for

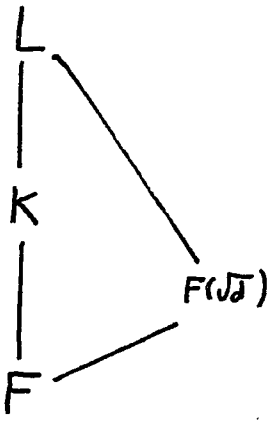
arbitrary forms. In [ELW_2, theorem (3.3)] it was shown that if F is 1-amenable for 4-dimensional forms, then any finite multiquadratic extension K/F is excellent for 4-dimensional forms.

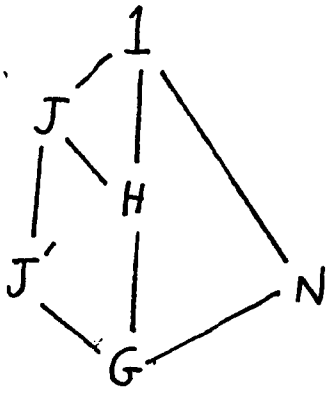
CHAPTER III

GALOIS THEORY AND COMMON VALUE PROPERTIES OVER NUMBER FIELDS

Let $F \subseteq K \subseteq L$ be a tower of number fields where L is normal over F and $G = Gal(L/F)$. The goal of Chapter III is to find sufficient conditions for G so that the common value properties hold for K/F. The principal tool is our "Main Theorem" (3.1). We use the techniques developed to construct several examples that show the Main Theorem cannot be improved.

We now set up assumptions and notation that will be fixed throughout this chapter, unless otherwise noted. Let K/F be a finite extension of number fields and L any finite normal extension of F containing K. Let $G = Gal(L/F)$ and H be the subgroup of G fixing K. Let J be a Sylow 2-group of H and J' a Sylow 2-group of G containing J. Let N be a subgroup of index 2 in G, if one exists, and let $F(\sqrt{d})$ be the quadratic extension of F corresponding to N. We continue to use notation from Chapter II.





(3.1) Main Theorem. With the assumptions and notation from above, assume $E(K/F) \neq \emptyset$ and consider the following statements:

1) For each subgroup N of index 2 in G, $J' \not\subseteq \bigcup_{g \in G} g^{-1}Jg \cup N$, or if no such N exists, $J' \not\subseteq \bigcup_{g \in G} g^{-1}Jg$.

2) For each finite set $T \subseteq \Omega(F)$ and for each $d \in \dot{F} - F^2$, there exists $p \in E(K/F) - T$ such that $d \notin F_p^2$. [That is, $E(K/F)$ is a strong global square set (see definitions (2.29) and (2.13).]

3) For each $d \in \dot{F} - F^2$, there exists $p \in E(K/F)$ such that $d \notin F_p^2$. [That is, $E(K/F)$ is a global square set.]

4) The set $E(K/F)$ is infinite.

5) $J' \not\subseteq \bigcup_{g \in G} g^{-1}Jg$.

The following implications hold: 1) $\Longleftrightarrow$ 2) $\not\Longleftrightarrow$ 3) $\not\Longleftrightarrow$ 4) $\Longleftrightarrow$ 5) .

(3.2) Remark. The equivalence of 1) and 2) and of 4) and 5) show that 1) and 5) are independent of the choice of L .

We show later that it is possible to have $[K:F]$ even and $E(K/F)$ either finite and nonempty or empty.

We see in (3.11) that the implication 4) $\longrightarrow$ 2) fails for a finite number of easily specified square classes.

The assumption $E(K/F) \neq \emptyset$ implies $[K:F]$ is even since $[K:F] = \sum_{P|p} [K_P:F_p]$.

Let us first recall the procedure to determine the factorization in K of a finite prime $p \in \Omega(F)$ that doesn't ramify in L [J, pp. 101-102]. Let $P \in \Omega(L)$ be a prime factor of p and $\sigma(L/F, P) = \sigma$ the Frobenius automorphism. If σ acts by right multiplication on the right cosets of H in G , it induces a permutation of these right cosets. This permutation can be expressed as a product of disjoint cycles, say of lengths $t_1, \ldots, t_s$, in which case p is a product of s distinct primes in K having relative degrees $t_1, \ldots, t_s$. In the case of an unramified prime, the relative degree (degree of the residue class field extension) equals the local degree. Thus an unramified finite prime p lies in $E(K/F)$ if

and only if the $t_1, \ldots, t_s$ defined above are all even. This is independent of the choice of L and of the prime factor P in $\Omega(L)$.

(3.3) Definition. An element $g \in G$ is even with respect to K/F if the permutation above induced by g on the right cosets of H in G is a product of disjoint cycles each of even length.

(3.4) Remark. It follows from (3.3) that if $p \in \Omega(F)$ is a finite prime unramified in L and P is a prime divisor of p in $\Omega(L)$, then $p \in E(K/F)$ if and only if $\sigma(L/F, P)$ is even.

(3.5) Proposition. An element $g \in G$ is even if and only if g^r is even for every odd number r .

Proof: The length of the cycle containing the coset Hg_1 is the smallest positive integer t such that $Hg_1 = Hg_1g^t$, i.e., such that $g^t \in g_1^{-1}Hg_1$. Suppose g is even and r is an odd number. If g^r is not even, then for some coset Hg_1 , $g^{rt} \in g_1^{-1}Hg_1$ for some odd t . Since rt is odd, the smallest power of g lying in $g_1^{-1}Hg_1$ divides rt and is odd, contradicting the evenness of g .

Now suppose g^r is even, r odd. If g isn't even, there exists a coset Hg_1 and an odd number t such that

$g^t \in g_1^{-1}Hg_1$. Then $g^{rt} = (g^r)^t \in g_1^{-1}Hg_1$. Let u be the smallest positive number such that $(g^r)^u \in g_1^{-1}Hg_1$. Then $u|t$. But u is even since g^r is even, contrary to the assumption that t is odd. This contradiction shows g is even.

(3.6) Corollary. The group G contains an even element if and only if G contains an even element whose order is a power of 2 .

Proof: Let $ord(g) = 2^n r$ where $g \in G$ and r is odd. Then $ord(g^r) = 2^n$ and if g is even, then g^r is even by (3.5).

Since the length of any cycle in the permutation induced by $g \in G$ divides $ord(g)$, if $ord(g)$ is a power of 2 , the length of a cycle is odd if and only if the length is one.

(3.7) Theorem. The group G contains an even element if and only if $J' \notin \bigcup_{g \in G} g^{-1}Jg$.

Proof: We observe from the preceding discussion that the following statements are equivalent.

a) G contains an even element.

b) G contains an even element g_1 whose order is a

power of 2 .

c) The permutation induced by g_1 has no cycles of length 1 and $\mathrm{ord}(g_1)$ is a power of 2 .

d) $Hg \neq Hgg_1$ for each $g \in G$ and some g_1 whose order is a power of 2 .

e) $g_1 \notin \bigcup_{g \in G} g^{-1}Hg$ and $\mathrm{ord}(g_1)$ is a power of 2 .

f) $g_1 \notin \bigcup_{g \in G} g^{-1}Jg$ and $\mathrm{ord}(g_1)$ is a power of 2 .

g) $J' \notin \bigcup_{g \in G} g^{-1}Jg$.

Statements e) and f) are equivalent because if $\mathrm{ord}(g_1)$ is a power of 2 and $g_1 = g^{-1}hg$, $h \in H$, then $\mathrm{ord}(h)$ is a power of 2 . Every such element h is contained in a Sylow 2-group of H and all such Sylow 2-groups are conjugate in H . Similarly, f) and g) are equivalent because if $\mathrm{ord}(g_1)$ is a power of 2 , then g_1 is contained in a Sylow 2-group of G and all Sylow 2-groups of G are conjugate in G .

(3.8) Theorem. The set $E(K/F)$ is infinite if and only if $J' \notin \bigcup_{g \in G} g^{-1}Jg$. Thus statements 4) and 5) of Theorem (3.1) are equivalent.

Proof: Suppose $J' \notin \bigcup_{g \in G} g^{-1}Jg$. Then G contains an even element g_1 by (3.7). By the Tchebotarev density theorem [J, p. 182], there are infinitely many primes $p \in \Omega(F)$ that have a prime divisor P in $\Omega(L)$ such that

$g_1 = \sigma(L/F, P)$. Since g_1 is even, it follows from (3.4) that these primes p lie in $E(K/F)$. Therefore $E(K/F)$ is an infinite set.

Suppose $E(K/F)$ is an infinite set. Then $E(K/F)$ contains a finite prime p that is unramified in L . Let P be a prime divisor of p in $\Omega(L)$ and let $g_1 = \sigma(L/F, P)$. Then g_1 is even by (3.4) and therefore $J' \not\subseteq \bigcup_{g \in G} g^{-1}Jg$ by (3.7).

(3.9) Theorem. Let $d \in \dot{F} - F^2$ and suppose $F(\sqrt{d}) \subsetneq L$. Let N be the subgroup of G corresponding to $F(\sqrt{d})$. There exist infinitely many primes $p \in E(K/F)$ that are unramified in L such that $d \notin F_p^2$ if and only if there exists $g \in G$ such that g is even and $g \notin N$.

Proof: Let $p \in E(K/F)$ be a prime that is unramified in L such that $d \notin F_p^2$. Let P be a prime divisor of p in $\Omega(L)$ and let $g = \sigma(L/F, P)$. Then g is even by (3.4) Since $d \notin F_p^2$ and p is unramified in $F(\sqrt{d})$, it follows that p is a prime in $\Omega(F(\sqrt{d}))$ with relative degree 2 . Therefore, the permutation induced by g on the cosets of N in G is a cycle of length 2 . This shows $g \notin N$.

Suppose $g \in G$ is even and $g \notin N$. By the Tchebotarev density theorem, there are infinitely many primes p in $\Omega(F)$ that are unramified in L and have a prime divisor

P in $\Omega(L)$ such that $g = \sigma(L/F, P)$. Since g is even, it follows any such prime p lies in $E(K/F)$ by (3.4). Since $g \notin N$, the action of g on the cosets of N in G yields a transposition. It follows that each such p is a prime in $\Omega(F(\sqrt{d}))$ with relative degree 2 and therefore $d \notin F_p^2$.

(3.10) Theorem. Let $d \in \dot{F}$, $d \notin L^2$. Suppose G contains an even element with respect to K/F. Then there exist infinitely many primes $p \in \Omega(F)$ such that p is unramified in L, $p \in E(K/F)$, and $d \notin F_p^2$.

Proof: Let $M = L(\sqrt{d})$. The hypothesis on d implies $[M:L] = 2$. It follows from Galois theory that M is normal over F, $L \cap F(\sqrt{d}) = F$, and $Gal(M/F) = Gal(L/F) \times Gal(F(\sqrt{d})/F) = G \times C_2$ where $C_2 = \{1, t\}$ is the group of order 2. The subgroup of $Gal(M/F)$ that corresponds to K is $H \times C_2$ and the subgroup that corresponds to $F(\sqrt{d})$ is $G \times 1$.

Let $g \in G$ be an even element with respect to K/F. It is clear that the permutation induced by the action of g on the right cosets of H in G has the same cycle structure as does the permutation induced by the action of $g \times t$ on the right cosets of $H \times C_2$ in $G \times C_2$. Therefore $g \times t$ is an even element with respect to K/F, i.e., with respect to its action on the right cosets of $H \times C_2$

in $G \times C_2$.

Since $g \times t \notin G \times 1$, the group corresponding to $F(\sqrt{d})$, it follows from (3.9) with M substituted for L , that there are infinitely many primes $p \in E(K/F)$ such that p is unramified in M , and thus in L , and $d \notin F_p^2$.

(3.11) Corollary. Suppose G contains an even element with respect to K/F . Then for all but finitely many square classes dF^2 in $\dot{F}$, there are infinitely many primes $p \in \Omega(F)$ such that $p \in E(K/F)$ and $d \notin F_p^2$. These exceptional square classes are contained in $\{dF^2 | d \in \dot{F} \cap L^2\}$.

Proof: This follows directly from (3.10) since L contains only finitely many quadratic extensions of F .

(3.12) Theorem. The following implications of Theorem (3.1) hold: 2) $\longrightarrow$ 3) $\longrightarrow$ 4) .

Proof: The implication 2) $\longrightarrow$ 3) is trivial. The implication 3) $\longrightarrow$ 4) follows from (2.30).

(3.13) Theorem. Statements 1) and 2) of Theorem (3.1) are equivalent.

Proof: Assume statement 1) is true. Let a finite

set $T \subseteq \Omega(F)$ be given and let $d \in \dot{F} - F^2$. Since $J' \notin \bigcup_{g \in G} g^{-1}Jg$, G contains an even element by (3.7). If $d \in \dot{L} - L^2$, then by (3.10) we can find a prime $p \in E(K/F) - T$ such that $d \notin F_p^2$. If $F(\sqrt{d}) \subseteq L$, let N be the subgroup of G corresponding to $F(\sqrt{d})$. Since $J' \notin \bigcup_{g \in G} g^{-1}Jg \cup N$, G contains an even element g_1 such that $g_1 \notin N$ by b) and f) of (3.7). It follows from (3.9) that we can find $p \in E(K/F) - T$ such that $d \notin F_p^2$.

Assume statement 2) is true. Let T be a finite set of primes in $\Omega(F)$ that contains the primes that ramify in L and the infinite primes in $\Omega(F)$. By (3.12), statement 4) of (3.1) holds so $E(K/F)$ is infinite and thus $J' \notin \bigcup_{g \in G} g^{-1}Jg$ by (3.8). Let N be a subgroup of index 2 in G, if one exists. Let $F(\sqrt{d})$ correspond to N. By statement 2) there exists a prime $p \in E(K/F) - T$ such that $d \notin F_p^2$. Thus p is unramified in L by the definition of T.

The first paragraph of the proof of (3.9) shows there exists $g \in G$ such that g is even and $g \notin N$. It follows from (3.5) that for some odd number r, $\mathrm{ord}(g^r)$ is a power of 2 and g^r is even. Thus $g^r \notin N$ since $[G:N] = 2$ and r is odd. Also, $g^r \notin \bigcup_{g \in G} g^{-1}Jg$ by (3.7), b) and f), since g^r is even and $\mathrm{ord}(g^r)$ is a power of 2. Therefore $J' \notin \bigcup_{g \in G} g^{-1}Jg \cup N$ since J' contains some conjugate of g^r and the right side is invariant under conjugation. This completes the proof.

The positive implications of the Main Theorem (3.1) follow from (3.8), (3.12), and (3.13). We show in (3.17) and (3.20) that 4) $\not\longrightarrow$ 3) and 3) $\not\longrightarrow$ 2) in general. The result in (3.11) shows how statement 4) can fail to imply statement 2) of (3.1). If 4) holds, then G contains an even element by (3.7), (3.8). Then by (3.11), statement 2) may not hold if $F(\sqrt{d}) \subseteq L$.

Whether or not statement 3) implies statement 2) depends on the primes in $\Omega(F)$ that ramify in L. This follows from (3.9) as follows: Assume 3) holds. Since 3) $\longrightarrow$ 4), we know G contains an even element by (3.7), (3.8). Let $d \in \dot{F} - F^2$. If $F(\sqrt{d}) \not\subseteq L$, then statement 2) holds for d by (3.10). Suppose $F(\sqrt{d}) \subseteq L$. Then by statement 3), there exists $p \in E(K/F)$ such that $d \notin F_p^2$. If p is unramified in L, then 2) holds for d since the first paragraph of the proof of (3.9) yields an even element g such that $g \notin N$ and then the rest of the proof shows there are infinitely many such p. If p is ramified in L, then we show in (3.20) that 2) may fail to hold for d. We note that statements 2) and 3) are equivalent if L/F is an unramified extension.

Since the connection with Galois theory has been through the Frobenius automorphism which is defined only for unramified primes it is to be expected that 3) has no equivalent condition in terms of the group G as 2) does in 1) and 4) does in 5).

It is possible that $E(K/F)$ is a finite nonempty set. As noted already in the remarks following (2.31), such an example was constructed by Waterhouse in [Wr, p. 642]. An example where $[K:F]$ is even and $E(K/F) = \emptyset$ will be constructed in (3.23). If $E(K/F)$ is finite and nonempty, then $E(K/F)$ consists of primes that ramify in L. This follows since if $p \in E(K/F)$ where p is unramified in L and $P \in \Omega(L)$ is a prime divisor of p, then $\sigma(L/F, P)$ is even by (3.4) and thus $E(K/F)$ is infinite by (3.7), (3.8).

In order to construct examples that show the non-implications of Theorem (3.1) hold and to exhibit other examples, we need to construct a group G having certain properties. The example in (3.14) of a group G satisfying these properties was found by R. Solomon [private communication].

(3.14) Theorem. There exists a chain of finite groups $G \supseteq J' \supsetneq J$ where J' is a Sylow 2-group of G and a subgroup N of index 2 in G such that

1) $J' \nsubseteq \bigcup_{g \in G} g^{-1}Jg$

2) $J' \subseteq \bigcup_{g \in G} g^{-1}Jg \cup N$.

Proof: Let C_6 be the cyclic group of order 6 with

generator σ . Let L be the abelian group of order 16 with generators a , b each of order 4 . There exists an embedding $\theta: C_6 \to \text{aut}(L)$ where $a^{\theta(\sigma)} = ab$ and $b^{\theta(\sigma)} = a^{-1}$. We shall now identify elements of C_6 with their images in aut(L) .

Let G be the semidirect product $L \times_\theta C_6$ [R, p. 137]. Multiplication is given by $(k, x)(m, y) = (km^x, xy)$ where $k, m \in L$ and $x, y \in C_6$. Let $s = \sigma^2$ and $t = \sigma^3$. Then

$$a^s = a^{\sigma^2} = (ab)^\sigma = b \qquad a^t = a^{s\sigma} = b^\sigma = a^{-1}$$

and

$$b^s = b^{\sigma^2} = (a^{-1})^\sigma = a^{-1}b^{-1} \qquad b^t = b^{s\sigma} = (a^{-1}b^{-1})^\sigma = b^{-1}$$

Let $N = [a, b, s]$, $J' = [a, b, t]$, and $J = [a, t]$ where [ ] means "the subgroup of G generated by". It follows that $|G| = 96$, $|N| = 48$, $|J'| = 32$, and $|J| = 8$. In order to calculate the conjugates of elements more easily, we derive the following formulas to simplify the work:

i) $(m, y)(k, x)(m, y)^{-1} = (m, y)(k, x)(m^{-1^{y^{-1}}}, y^{-1})$

$= (mk^y, yx)(m^{-1^{y^{-1}}}, y^{-1}) = (mk^y m^{-1^{yxy^{-1}}}, yxy^{-1})$

$= (mk^y m^{-1^x}, x)$ since C_6 is abelian.

ii) If $x = 1$, then i) reduces to

$(m, y)(k, 1)(m, y)^{-1} = (k^y, 1)$.

iii) If $x = t$ and $m = a^i b^j$, then

$$(a^ib^j, y)(k, t)(a^ib^j, y)^{-1} = (a^ib^jk^y(a^{-i}b^{-j})^t, t)$$
$$= (a^ib^jk^ya^ib^j, t) = (a^{2i}b^{2j}k^y, t) .$$

Now we calculate the conjugates of elements in J using these formulas. Let $C(m, y)$ denote the conjugacy class of (m, y) in G.

$$C(1, 1) = \{1, 1\} .$$

$$C(a, 1) = \{(a^y, 1) \mid y \in C_6\} = \{(a, 1), (ab, 1), (b, 1), (a^3, 1), (a^3b^3, 1), (b^3, 1)\} .$$

$$C(a^2, 1) = \{((a^2)^y, 1) \mid y \in C_6\} = \{(a^2, 1), (a^2b^2, 1), (b^2, 1)\} .$$

$$C(1, t) = \{(a^{2i}b^{2j}, t) \mid 0 \leq i, j \leq 1\} = \{(1, t), (a^2, t), (b^2, t), (a^2b^2, t)\} .$$

$$C(a, t) = \{(a^{2i}b^{2j}a^y, t) \mid 0 \leq i, j \leq 1, y \in C_6\} =$$
$$\{(a, t), (a^3, t), (ab^2, t), (a^3b^2, t), (ab, t), (a^3b, t), (ab^3, t), (a^3b^3, t), (b, t), (a^2b, t), (b^3, t), (a^2b^3, t)\} .$$

The union of these conjugacy classes $\{C(1,1), C(a, 1), C(a^2, 1), C(1, t), C(a, t)\}$ equals $\bigcup_{g \in G} g^{-1}Jg$. It follows that $J' - \bigcup_{g \in G} g^{-1}Jg = \{(a^2b, 1), (a^3b, 1), (ab^2, 1), (a^3b^2, 1), (ab^3, 1), (a^2b^3, 1)\}$. Since this last set is contained in N, the theorem is proved.

For later use, we record the following proposition.

(3.15) Proposition. Let G be the group constucted in (3.14).

1) The order of (b, t) is 2.

2) $\bigcap_{g \in G} g^{-1}Jg = (1, 1) = \{1\}$.

3) N is the unique subgroup of index 2 in G.

Proof: 1) $(b, t)(b, t) = (bb^t, t^2) = (bb^{-1}, 1) = (1, 1)$.

2) Let $g = (1, \sigma)$. Then $gJg^{-1} = (1, \sigma)J(1, \sigma)^{-1} = \{(k^\sigma, x) \mid (k, x) \in J\} = \{(1, 1), (ab, 1), (a^2b^2, 1), (a^3b^3, 1), (1, t), (ab, t), (a^2b^2, t), (a^3b^3, t)\}$. Thus $J \cap gJg^{-1} = \{(1, 1), (1, t)\}$. Now let $g = (b, t)$. Then $(1, t) \notin (b, t)J(b, t)^{-1}$ since $(b, t)(a^i, t)(b, t)^{-1} = (b(a^i)^t(b^{-1})^t, t) = (b^2a^{-i}, t) \neq (1, t)$ for each i.

3) Suppose $N' \neq N$ is another subgroup of index 2 in G. Then $N \cap N'$ is a normal subgroup of order 24 since $|N/N \cap N'| = 2$. It follows from the multiplication formula that $[a, b]$ is the unique Sylow 2-group of N because N has 16 elements whose order is a power of 2 and 32 elements whose order is divisible by 3. Therefore the Sylow 2-group J'' of order 8 in $N \cap N'$ is contained in $[a, b]$. It can be seen that J'' is the unique subgroup of order 8 in $N \cap N'$ since if $g \in N \cap N'$

has order 3 , then the multiplication formula shows each element of $J"g$ and $J"g^2$ has its order divisible by 3 . Therefore $J"$ is normal in G since any conjugate of $J"$ lies in $N \cap N'$ but $N \cap N'$ contains a unique subgroup of order 8 . Since $|J"| = 8$ and $J" \subseteq [a, b]$, it follows $J" \cong C_4 \times C_2$ and thus $J"$ contains exactly four elements of order 4 . We get a contradiction since every element in $[a, b]$ of order 4 has six conjugates: $C(a, 1)$ contains 6 elements as noted before and $C(ab^{-1}, 1) = \{((ab^{-1})^y, 1) | y \in C_6\} = \{(ab^{-1}, 1), (a^2b, 1), (ab^2, 1), (a^{-1}b, 1), (a^2b^{-1}, 1), (a^3b^2, 1)\}$. Thus $J"$ cannot contain complete conjugacy classes and so $J"$ can't be normal in G . Therefore the subgroup N' doesn't exist.

The proof of the following theorem is motivated by an idea from [Wr, p. 643].

(3.16) Theorem. Let L be an arbitrary finite normal extension of a number field F and let $G = Gal(L/F)$. Then there exists a number field F' and a normal extension L' of F' such that

1) $Gal(L'/F') \cong G$.

2) L'/F' is an unramified extension.

3) $F' \cap L = F$.

Proof: Let $q \in \Omega(F)$ be a finite prime that splits completely in L. There are infinitely many such primes [J, p. 134]. Let $L = F(\theta)$ and let $f \in F[x]$ be the irreducible monic polynomial satisfied by θ. Let $F_q(\phi)$ be the unramified extension of F_q of degree n, where $|G| = n$. Let $g \in F_q[x]$ be the irreducible monic polynomial satisfied by ϕ. Then deg f = deg g = n. Let $R = \{p \in \Omega(F) \mid p \text{ ramifies in } L\}$.

Using the approximation theorem, find $h \in F[x]$ of degree n sufficiently close to f over F_p for $p \in R$ and sufficiently close to g over F_q such that the following conditions hold [Ar, pp. 45-46].

i) Over F_q, h and g generate the same field, i.e., $F_q[x]/(h(x)) \cong F_q[x]/(g(x)) = F_q(\phi)$.

ii) For each $p \in R$, $F' \otimes_F F_p \cong L \otimes_F F_p$ where $F' = F[x]/(h(x))$ and $L = F[x]/(f(x))$.

If h and f factor over F_p into irreducible factors, say $h = \prod_{i=1}^{\ell} h_i$ and $f = \prod_{i=1}^{m} f_i$, then $F' \otimes_F F_p = \bigoplus_{i=1}^{\ell} F_p[x]/(h_i(x))$ and $L \otimes F_p = \bigoplus_{i=1}^{m} F_p[x]/(f_i(x))$. [Note that the f_i above are distinct since f has distinct roots in L.] Condition ii) requires $\ell = m$ and $F_p[x]/(h_i(x)) \cong F_p[x]/(f_i(x))$ for $1 \leq i \leq \ell$ for a suitable ordering.

Let $L' = F'L$. Since $[F_q(\phi):F_q] = n$, it follows from condition i) that h is irreducible over F_q . Since $F_q(\phi)/F$ is an unramified extension it follows that q remains prime in F' [J, p. 88]. Since q splits completely in L , we see that $L \cap F' = F$. Therefore $[L':F'] = [LF':F'] = [L:F' \cap L] = [L:F] = n$. Further, L' is normal over F' since L is normal over F and $\mathrm{Gal}(L'/F') = \mathrm{Gal}(L/F) = G$.

Any prime $P \in \Omega(F')$ lying over a prime $p \in \Omega(F) - R$ is unramified in L' since p is unramified in L . If $P \in \Omega(F')$ lies over $p \in R$, then P splits completely in L' . This is because f splits completely into linear factors over L and thus over each direct summand of $L \otimes_F F_p \cong F' \otimes_F F_p$ since L maps injectively into each $F_p[x]/(f_i(x))$. Therefore f splits completely into linear factors over F'_P since F'_P is one of the direct summands of $F' \otimes_F F_p$. Therefore P splits completely in L' (see [J, p. 88]). It follows that L'/F' is an unramified extension.

(3.17) Theorem. The nonimplication 4) $\not\Rightarrow$ 3) of Theorem (3.1) holds.

Proof: We shall assume there exists a normal extension of number fields L/F where $G = \mathrm{Gal}(L/F)$ is the group constructed in (3.14). The actual construction of such an

extension will be carried out in (3.19) below. It follows from (3.16) that we may assume L/F is an unramified extension.

Let $F(\sqrt{d})$, $d \in \dot{F}$, be the field corresponding to the subgroup N of index 2 in G. Let $H = J$, and let K be the fixed field of H. Since $J' \not\subseteq \bigcup_{g \in G} g^{-1}Jg$, $E(K/F)$ is infinite by (3.8) and so statement 4) of theorem (3.1) holds.

Suppose $g \in G$ is an even element such that $g \notin N$. Then for some odd number r, $\text{ord}(g^r)$ is a power of 2, g^r is even by (3.5) and $g^r \notin N$ since $[G:N] = 2$. Then $g_1 = g^r \notin \bigcup_{g \in G} g^{-1}Jg \cup N$ by (3.7) b) and f). Thus $J' \not\subseteq \bigcup_{g \in G} g^{-1}Jg \cup N$ since J' contains a conjugate of g_1. This contradiction shows there is no even element $g \in G$ not in N. It follows from the proof of (3.9) that there is no unramified prime $p \in E(K/F)$ such that $d \notin F_p^2$. Since L/F is an unramified extension, there is no prime $p \in E(K/F)$ such that $d \notin F_p^2$. Therefore statement 3) of (3.1) fails.

The following lemma appears in Van der Waerden's Algebra.

(3.18) Lemma. Suppose G is a subgroup of the symmetric group S_n such that

i) G is transitive.

ii) G contains an $(n-1)$-cycle.

iii) G contains a transposition.

Then $G = S_n$.

(3.19) Theorem. Let G be the group constructed in (3.14). There exists an extension of number fields L/F such that

i) L is normal over F and $Gal(L/F) = G$,

ii) there exists a real archimedean prime $p \in \Omega(F)$ such that $p \in E(K/F)$ and $p \in E(F(\sqrt{d})/F)$ where K is the field corresponding to J and $F(\sqrt{d})$ is the field corresponding to N .

Proof: Condition ii) means every prime P in $\Omega(K)$ or $\Omega(F(\sqrt{d}))$ that lies over p is a complex prime. This is equivalent to the condition that the ordering on F induced by p cannot be extended to either K or $F(\sqrt{d})$.

The group G can be embedded in S_n for some n . Since $\bigcap_{g \in G} g^{-1}Jg = \{1\}$ by (3.15) and $[G:J] = 12$, we could take $n = 12$ [R, p. 43].

Let g_1 be the image of (b, t) in S_n . Then g_1 has order 2 by (3.15) and so g_1 is a product of r disjoint transpositions in S_n where $r \leq \frac{n}{2}$. Let f be

a polynomial in $\mathbb{Z}[x]$ of degree n such that the following conditions hold. (Let $\mathbb{F}_q$ be the finite field with q elements and let $\overline{f_p}$ denote f reduced mod p.)

i) $\overline{f_2}$ is irreducible in $\mathbb{F}_2[x]$.

ii) $\overline{f_3}$ factors in $\mathbb{F}_3[x]$ as a linear factor and an irreducible factor of degree $n - 1$.

iii) $\overline{f_\ell}$ factors in $\mathbb{F}_\ell[x]$ as an irreducible quadratic and $n - 2$ distinct linear factors where ℓ is a prime number $\geq n - 2$.

iv) f factors in $\mathbb{R}[x]$ as r distinct irreducible quadratic factors and $n - 2r$ distinct linear factors.

This can be done using the approximation theorem.

Let L be the splitting field of f over $\mathbb{Q}$ and let us choose a fixed embedding of L into the complex numbers $\mathbb{C}$. Let $G' = \mathrm{Gal}(L/\mathbb{Q})$. We show that $G' = S_n$: By i), f is irreducible over $\mathbb{Q}$ so G' is a transitive group on the n roots of f . By ii), G' contains an $(n-1)$-cycle and by iii), G' contains a transposition. Therefore $G' = S_n$ by (3.18).

Let $\sigma \in G'$ be the automorphism of $L/\mathbb{Q}$ induced by complex conjugation. By iv), σ is a product of r disjoint transpositions. Since g_1 and σ have the same

cycle decomposition, they are conjugate in S_n . Therefore, some conjugate of G in S_n contains σ . Using this conjugate if necessary, we can assume $\sigma \in G$ and that $g_1 = \sigma$, i.e., σ is the image of (b, t) in S_n .

Let F be the subfield of L corresponding to the subgroup G of S_n , K the field corresponding to J , and $F(\sqrt{d})$ the field corresponding to the unique subgroup N of index 2 in G by (3.15). (In the original notation, K corresponds to a subgroup H . We are letting $H = J$ here.)

Since $\sigma \in G$, F is fixed by σ so $F \subseteq \mathbb{R}$. Let us fix the ordering of F that is induced by the ordering of $\mathbb{R}$. Since σ is the image of (b, t) , and using the notation of (3.14), $N = [a, b, s]$, we see $\sigma \notin N$ and so $F(\sqrt{d})$ is not fixed by σ . Therefore $d < 0$ otherwise $F(\sqrt{d}) \subseteq \mathbb{R}$ and $F(\sqrt{d})$ would be fixed by σ . Let $p \in \Omega(F)$ be the real archimedean prime corresponding to this fixed ordering of F . We have just shown that the ordering of F doesn't extend to $F(\sqrt{d})$ and thus $p \in E(F(\sqrt{d})/F)$.

This ordering on F also doesn't extend to K . To see this, observe $[G:J] = 12$ and that there is a chain of subgroups $J \subset J_0 \subset J' \subset G$ where $[J':J_0] = [J_0:J] = 2$ and $[G:J'] = 3$. It follows there is a chain of fields $K \supset K_0 \supset K' \supset F$ where $[K:K_0] = [K_0:K'] = 2$ and $[K':F] = 3$. Since $F \subseteq \mathbb{R}$ and K' is obtained by adjoin-

ing to F a root of an irreducible cubic over F, it follows that K' or one of its conjugates is contained in $\mathbb{R}$. But it is easy to check that J' is normal in G using the formulas in (3.14). Therefore K' is normal over F so K' has no conjugates other than itself so $K' \subseteq \mathbb{R}$. If the ordering of F extended to K, then K would lie in $\mathbb{R}$ since K is obtained from K' by adjoining square roots. We know $K \not\subseteq \mathbb{R}$ since K is not fixed by σ, i.e., $\sigma \notin J$. Since the ordering on F doesn't extend to K, it follows $p \in E(K/F)$.

(3.20) Theorem. The extension K/F constructed in (3.19) gives an example where the nonimplication 3) $\not\Rightarrow$ 2) of theorem (3.1) holds.

Proof: First we show that 3) holds. Let $c \in \dot{F} - F^2$ be given. Since $J' \not\subseteq \bigcup_{g \in G} g^{-1}Jg$, G contains an even element by (3.7). Suppose $F(\sqrt{c}) \not\subseteq L$. Then by (3.10) there exists $p \in E(K/F)$ such that $c \notin F_p^2$. Suppose $F(\sqrt{c}) \subseteq L$. Then the group corresponding to $F(\sqrt{c})$ has index 2 in G and must be N by (3.15). It follows $F(\sqrt{c}) = F(\sqrt{d})$ and c, d are in the same square class in $\dot{F}$. (Note that we can't finish by (3.9) because $J' \subseteq \bigcup_{g \in G} g^{-1}Jg \cup N$.) Theorem (3.19) shows that there exists a real archimedean prime $p \in E(K/F)$ such that

$d < 0$ with respect to the ordering induced by p. This means $d \notin F_p^2$ and so $c \notin F_p^2$ also. Therefore in all cases, there exists $p \in E(K/F)$ such that $c \notin F_p^2$ and so statement 3) of theorem (3.1) holds. Statement 2) fails, however, because the equivalent statement 1) fails by the construction of G.

Next we construct in (3.21) and (3.22) below an extension K'/F' such that $E(K'/F')$ is a global square set but for each $m \geq 3$, there exists a form α_m of dimension m and a binary form β each defined over F' such that $(\alpha_m, \beta, K'/F')$ fails to satisfy SCV. This will show that the hypothesis in (2.31) is necessary.

(3.21) Theorem. Let $F \subseteq K \subseteq L$ be the normal extension constructed in (3.19). Let p_0 be the prime that was called p in (3.19). Let $R' = \{p \in \Omega(F) \mid p$ is finite and p ramifies in $L\}$. Then there is a finite extension F'/F such that the following holds.

1) $F' \cap L = F$.

2) If $P \in \Omega(F')$ and P ramifies in $F'L$, then P is infinite.

3) The ordering of F induced by p_0 extends to F'.

4) $Gal(L'/F') = G$ where $L' = F'L$.

Proof: The proof is virtually the same as the proof of (3.16). The changes that should be made in the proof of

(3.16) are as follows:

The set R' should be used wherever R was used in (3.16). A third condition on the polynomial h should be added that reads: iii) h splits completely into linear factors over $F_{p_0}[x]$. The proof of (3.16) now gives us the result. Since $F' = F[x]/(h(x))$, it follows that the ordering on F induced by p_0 extends to F'.

(3.22) Theorem. Let L'/F' be the extension constructed in (3.21). Let K' be the field corresponding to $J \subseteq G$. Then $E(K'/F')$ is a global square set and there exist forms α_m, β, $m \geq 3$, defined over F' such that $\dim \alpha_m = m$, $\dim \beta = 2$ and $(\alpha_m, \beta, K'/F')$ fails to satisfy SCV.

Proof: Since K, as a subfield of L, corresponds to J we have $Gal(L/K) = Gal(L'/K') = Gal(L/K' \cap L)$ and so $K = K' \cap L$ and $K \subseteq K'$.

Let $P_0 \in \Omega(F')$ be a real archimedean prime lying over $p_0 \in \Omega(F)$. That is, the ordering on F' induced by P_0 extends the ordering on F induced by p_0. Let $d \in \dot{F}$ be as in (3.19) and (3.20). Since $d < 0$ in F_{p_0}, it follows that $d < 0$ in F'_{P_0} and thus $d \notin F'^2_{P_0}$. This ordering on F' doesn't extend to K' otherwise since

$K \subseteq K'$, the ordering would induce an ordering on K that would extend the given one on F . This is impossible by (3.19). Therefore $P_0 \in E(K'/F')$. The proof of (3.20) can now be applied to show $E(K'/F')$ is a global square set.

Let $\beta = \langle 1, -d \rangle$ and let $D = \{P \in E(K'/F') \mid d \notin F_P'^2\}$. The paragraph above shows $P_0 \in D$. Since $F'(\sqrt{d})$ corresponds to the subgroup $N \subseteq G = Gal(L'/F')$ and $J' \subseteq \bigcup_{g \in G} g^{-1}Jg \cup N$, it follows that D contains only primes in $\Omega(F')$ that ramify in L' . This follows from (3.9) since G contains no even elements not in N . According to condition 2 in (3.21), we see that D contains only infinite primes. This shows condition i) of theorem (2.28) is satisfied. We must consider two cases.

Case I. Suppose $|D|$ is odd. Let $\alpha_m = \langle -1, \ldots, -1 \rangle$ where $\dim \alpha_m = m \geq 3$. Then α_m is anisotropic over F_P' for each $P \in D$ so condition ii) of (2.28) is satisfied. Since $d < 0$ under each ordering of F' induced by $P \in D$, we see $\alpha_m \perp -\beta = \langle -1, \ldots, -1 \rangle \perp \langle -1, d \rangle$ is anisotropic over F_P' for each $P \in D$. Since $|D|$ is odd, condition iii) of (2.28) is satisfied so theorem (2.28) implies $(\alpha_m, \beta, K'/F')$ fails to satisfy SCV.

Case II. Suppose $|D|$ is even. Using the approximation theorem, choose $t \in F'$ such that $t < 0$ in F_P' for each $P \in D - \{P_0\}$ and $t > 0$ in F_{P_0}' . Let

$\alpha_m = \langle t, \ldots, t \rangle$ where $\dim \alpha_m = m \geq 3$. Then α_m is anisotropic over F'_P for each $P \in D$ so ii) of (2.28) holds. For each $P \in D - \{P_0\}$, $\alpha_m \perp -\beta = \langle t, \ldots, t \rangle \perp \langle -1, d \rangle$ is anisotropic over F'_P since $t,d < 0$. Over F'_{P_0} , $\alpha_m \perp -\beta$ is isotropic since $t > 0$. Since $|D - \{P_0\}|$ is odd, iii) of (2.28) holds so (2.28) implies $(\alpha_m, \beta, K'/F')$ fails to satisfy SCV.

The following proposition was stated in [Wr, p. 648] without proof.

(3.23) Proposition. There exists an extension of number fields K/F such that $[K:F]$ is even and $E(K/F) = \emptyset$.

Proof: Using our usual notations, we want an unramified normal extension L/F such that if $G = Gal(L/F)$, then there exists a Sylow 2-group J' of G containing a proper subgroup J such that $J' \subseteq \bigcup_{g \in G} g^{-1}Jg$. If K is the field corresponding to J , $p \in E(K/F)$, and $P \in \Omega(L)$ such that $P|p$, then since p is unramified, the Frobenius automorphism $\sigma(L/F, P)$ is even by (3.4). Then (3.7) implies $J' \not\subseteq \bigcup_{g \in G} g^{-1}Jg$ which is a contradiction. Therefore $E(K/F) = \emptyset$ and $[K:F]$ is even since $[G:J]$ is even.

We let $G = A_4$, J' the subgroup of A_4 of order 4 ,

and J a subgroup of order 2. Then $J' = \bigcup_{g\in G} g^{-1}Jg$. We can construct an extension L/F_0 such that $Gal(L/F_0) = S_4$ and L/F_0 is an unramified extension using the method in (3.19) and (3.16). Let F be the fixed field of A_4 and let K be the fixed field of J. Then L/F is an unramified extension, $[K:F] = 6$, and $E(K/F) = \emptyset$.

Now we show for a wide class of extensions of number fields K/F that $E(K/F)$ is a strong global square set and thus K/F is excellent and satisfies CV(2,2) by (2.14).

(3.24) Theorem. Let $F \subseteq K' \subseteq K$ be a tower of finite extensions of number fields such that K' is normal over F and $[K':F]$ is even. Then $E(K/F)$ is a strong global square set.

Proof: It is sufficient to show statement 1) of theorem (3.1) holds. Let L be a finite normal extension of F containing K. Let H' be the subgroup of G corresponding to K'. We continue to use our original notation.

Since K' is normal over F, H' is normal in G. Since $J \subseteq H \subseteq H'$, we have $\bigcup_{g\in G} g^{-1}Jg \subseteq \bigcup_{g\in G} g^{-1}H'g = H'$. Since J' is a Sylow 2-group of G and $[G:H']$ is even, we have $J' \not\subseteq H'$ since a higher power of 2 divides $|J'|$

than $|H'|$. Similarly $J' \not\subseteq N$ for any subgroup N of index 2 in G , if one exists. Therefore $J' \not\subseteq H' \cup N$ and this shows statement 1) of (3.1) holds and this in turn implies the conclusion.

$\lceil J' \subseteq H' \cup N \rightarrow J' = (J' \cap H') \cup (J' \cap N) \rightarrow J' = J' \cap H'$ or $J' = J' \cap N \rightarrow J' \subseteq H'$ or $J' \subseteq N$ which is a contradiction. $\rfloor$

(3.25) Theorem. (R. Solomon) If $[K:F] = 2^n$, then $E(K/F)$ is a strong global square set.

Proof: With our usual notation, we have $[G:H] = 2^n$ and $[G:J']$ is odd since J' is a Sylow 2-group of G . Let the greatest common divisor of $|H|$ and $|J'|$ be a . Then $|H| = ab$ and $|J'| = ac$ where $(b, c) = 1$. Since ab and ac divide $|G|$, we have $|G| = abcd$ for some $d \geq 1$. But $[G:H] = cd$ and $[G:J'] = bd$ are relatively prime so $d = 1$. Since $|HJ'| = |H| \cdot |J'|/|H \cap J'|$, $|HJ'| \leq |G| = abc$, $|H \cap J'| \leq a$, and $|H| \cdot |J'| = a^2bc$, we conclude that $|HJ'| = abc$ so $HJ' = G$.

It is clear that $J = J' \cap H$ and $J' \cap N \subsetneq J'$ since $J' \not\subseteq N$ (if N exists). Since J is contained in a subgroup J_0 of index 2 in J' and J_0 is normal in

J' , we see that $\bigcup_{g\in J'} g^{-1}Jg \cup (J' \cap N) \subseteq J_0 \cup (J' \cap N) \subsetneq J'$ since J' is not a union of two proper subgroups. Therefore there exists $g_1 \in J'$ such that $g_1 \notin \bigcup_{g\in J'} g^{-1}Jg \cup N$. Suppose $g_1 \in \bigcup_{g\in G} g^{-1}Jg$. Then $g_1 = g^{-1}jg$ for some $g \in G$, $j \in J$ and since $G = HJ'$, we have $g = hj'$ for some $h \in H$ and $j' \in J'$. Then $g_1 = j'^{-1}(h^{-1}jh)j'$. Since $g_1, j' \in J'$, we conclude $h^{-1}jh \in J'$. But $h^{-1}jh \in H$ so $h^{-1}jh \in H \cap J' = J$. Thus $g_1 \in j'^{-1}Jj'$ which is a contradiction. Therefore $g_1 \notin \bigcup_{g\in G} g^{-1}Jg \cup N$ and so statement 1) of theorem (3.1) holds for each N . Since statement 2) of (3.1) is equivalent to statement 1), we conclude $E(K/F)$ is a strong global square set.

CHAPTER IV

FIELDS WITH FINITE HASSE NUMBER

This chapter deals mainly with formally real fields that satisfy conditions that are analogous to the Hasse-Minkowski theorem where the orderings of the field take the place of the prime spots of the number field. In addition to studying the common value properties defined in Chapter II, we shall determine sufficient conditions for extensions of these fields to be excellent. We then apply these results to the question of whether a field is 1-amenable.

We first review some facts concerning formally real fields. A field F is formally real if -1 cannot be expressed as a sum of squares of elements from the field. This is equivalent to F possessing an ordering. Let P be the positive elements with respect to a given ordering of F. We shall also denote the ordering by P since the positive elements uniquely determine an ordering. We let F_P denote a real closure of F with respect to the ordering P. By a real closure F_P of a field F with respect to an ordering P, we mean a real closed field algebraic over F such that its unique ordering induces the given ordering on F. A real closed field F is a field such

that $F(\sqrt{-1})$ is algebraically closed. A real closure of an ordered field is unique up to order isomorphism. We write $a >_P 0$ if a is positive with respect to the ordering P. This is equivalent to the statement $a > 0$ in F_P.

We let $X(F)$ denote the set of all orderings of the field F. The set $X(F)$ is given a topology as follows: If $a \neq 0$, let $W_F(a) = \{P \in X(F) \mid a <_P 0\}$. The sets $W_F(a)$, $a \in \dot{F}$, form a subbasis of open sets for the topology of $X(F)$. The topology generated by this subbasis is a compact, Hausdorf, and totally disconnected space [KRW, theorem 8]. Since $W_F(a)$ and $W_F(-a)$ are complementary sets, it follows that $W_F(a)$ is a clopen set, i.e., both closed and open.

A field F satisfies the <u>strong approximation property</u>, SAP, if the following holds:

> SAP: If A and B are disjoint closed sets in $X(F)$, there exists $a \in \dot{F}$ such that $a >_P 0$ for $P \in A$ and $a <_P 0$ for $P \in B$.

A form $\alpha = \langle a_1, \ldots, a_n \rangle$ defined over a formally real field F is <u>effectively diagonalized</u> if $W_F(a_i) \subseteq W_F(a_{i+1})$, $1 \leq i \leq n-1$. A field F is an ED field if every form defined over F can be effectively diagonalized. Additional information on ED fields can be found in [Wr_2].

The <u>signature</u> of a form α with respect to an ordering P, written $sgn_P(\alpha)$, is defined to be the signature of

α in F_P, i.e., the number of positive entries in $\alpha = \langle a_1, \ldots, a_n \rangle$ minus the number of negative entries. This number is independent of the diagonalization of α.

An element $a \in \dot{F}$ is <u>totally positive</u> if $a >_P 0$ for each $P \in X(F)$. A form α is <u>totally indefinite</u> over F if α is indefinite over F_P for each $P \in X(F)$. The <u>Hasse number</u> of a field, $\tilde{u}(F)$, is the smallest integer n such that every totally indefinite form of dimension $> n$ is isotropic over F. If no such integer exists, one defines $\tilde{u}(F)$ to be ∞.

For example, if F is a number field, then $\tilde{u}(F) = 4$. This follows from the Hasse-Minkowski theorem since a totally indefinite form of dimension > 4 is isotropic over F_P for each $P \in \Omega(F)$. Examples of formally real fields F where $\tilde{u}(F) \leq 2$ are real fields of transcendence degree 1 over $\mathbb{R}$ and Pythagorean fields that satisfy SAP [ELP]. Other examples of fields with finite Hasse number can be found in [E], [ELP], and [P].

It is known that $\tilde{u}(F) < \infty$ implies F is an ED field which in turn implies F satisfies SAP. In neither instance is the converse valid. For more details and examples see [Wr_2, (2.5), (2.2), Ex. ii) p. 119] and [PW, p. 244].

Let $\alpha = \langle a_1, \ldots, a_n \rangle$ be defined over F and let $\mathbb{Z}$ have the discrete topology. The map $\hat{\alpha}: X(F) \to \mathbb{Z}$ where $\hat{\alpha}(P) = \operatorname{sgn}_P(\alpha)$ is a continuous map since $\hat{\alpha}$ is the sum of

the functions $\hat{a}_i : X(F) \to \mathbb{Z}$ where $\hat{a}_i(P) = \text{sgn}_P(\langle a_i \rangle)$. The function $\hat{a}$ is continuous since $\hat{a}^{-1}(\{1\}) = W_F(-a)$ and $\hat{a}^{-1}(\{-1\}) = W_F(a)$ are each open sets in $X(F)$. We see that the topology on $X(F)$ can be characterized as the weakest topology that makes the function $\hat{a}$ continuous for each $a \in \dot{F}$.

Let K/F be an extension of formally real fields. Let $\theta(K/F) = \theta : X(K) \to X(F)$ be defined by $\theta(P) = \text{res}_F(P)$ for $P \in X(K)$ where $\text{res}_F(P)$ is the ordering on F induced by P. Thus the image of θ is the subset of orderings of F that extend to K.

A field F is <u>linked</u> if the quaternion algebras defined over F form a subgroup of the Brauer group of F. If F is linked, then $\tilde{u}(F) \leq 8$. If $\tilde{u}(F) \leq 4$, then F is linked while if $\tilde{u}(F) = 8$, then F need not be linked. The Hasse number of a linked field can only be either 1, 2, 4, or 8. Several equivalent definitions of linked fields along with many of their properties are given in [E, section 4].

We shall assume all fields are formally real unless otherwise stated. If we let F be non-formally real, the results that follow remain valid if we adopt the convention that all non-formally real fields are ED and satisfy SAP and that all forms are totally indefinite. In many cases, the proofs become vacuous if F is non-formally real.

(4.1) Proposition. Let K/F be an extension of fields. Then $\theta(K/F) = \theta$ is continuous and $\mathrm{im}(\theta)$ is closed in $X(F)$.

Proof: To show θ is continuous, it is sufficient to show for each subbasis element $W_F(a) \subseteq X(F)$, $a \in \dot{F}$, that $\theta^{-1}(W_F(a))$ is a subbasis element of $X(K)$. But $\theta^{-1}(W_F(a))$ consists of the orderings of K that extend an ordering of F where $a < 0$. This is just the subbasis element $W_K(a)$. Therefore θ is continuous.

Since $X(K)$ is compact and $X(F)$ is Hausdorf, it follows that $\theta(X(K)) = \mathrm{im}(\theta)$ is closed in $X(F)$.

(4.2) Proposition. Let K/F be an arbitrary extension and suppose F is an ED field. Let α be a form defined over F that is isotropic over K. Then we can write $\alpha \cong_F \langle b_1, b_2\rangle \perp \beta$ where $b_1, b_2 \in \dot{F}$, b_1 is totally positive and b_2 is totally negative as elements of K, and β is defined over F.

Proof: Let $\alpha = \langle a_1, \ldots, a_n\rangle$ be an effective diagonalization of α. Thus $W_F(a_1) \subseteq \cdots \subseteq W_F(a_n)$. Let $Y \subseteq X(F)$ be the subset of orderings of F that extend to K. Then α is indefinite in F_P for each $P \in Y$ since α is totally indefinite in K. It follows that $W_F(a_1) \cap Y = \emptyset$ since $P \in W_F(a_1) \cap Y$ implies α is nega-

tive definite in F_P which is not true. Also, $Y \subseteq W_F(a_n)$ since $P \in Y - W(a_n)$ implies α is positive definite in F_P which is not true. Therefore a_1 is positive and a_n is negative for each ordering of Y. Then a_1 is positive and a_n is negative for each ordering of K. The proposition follows by letting $b_1 = a_1$, $b_2 = a_n$, and $\alpha = \langle a_2, \ldots, a_{n-1} \rangle$.

(4.3) Proposition. Let K/F be an arbitrary extension and suppose F satisfies ED and $\tilde{u}(K) = n < \infty$. Let α be a form defined over F that is isotropic over K. Then we can write $\alpha \cong_F \beta_1 \perp \beta_2$ where β_1, β_2 are defined over F, $\dim \beta_1 \leq n+1$, and β_1 is isotropic over K.

Proof: Let $\dim \alpha = m$. We may assume $m > n+1$; otherwise we let $\alpha = \beta_1$ and $\beta_2 = \langle 0 \rangle$. By (4.2) we can write $\alpha \cong_F \langle b_1, b_2 \rangle \perp \langle b_3, \ldots, b_m \rangle$ where $\langle b_1, b_2 \rangle$ is totally indefinite over K. Let $\beta_1 = \langle b_1, \ldots, b_{n+1} \rangle$ and $\beta_2 = \langle b_{n+2}, \ldots, b_m \rangle$. Since β_1 is totally indefinite over K and $\dim \beta_1 > \tilde{u}(K)$, we see that β_1 is isotropic over K.

(4.4) Theorem. Let K/F be such that F satisfies ED and $\tilde{u}(K) = n < \infty$. Then K/F is excellent if and only if K/F is excellent for forms of dimension $\leq n+1$.

Proof: Suppose K/F is excellent for forms of dimension $\leq n+1$. Let α be a form defined over F that is isotropic over K. Then by (4.3), we can write $\alpha \cong_F \beta_1 \perp \beta_2$ where $\dim \beta_1 \leq n+1$ and β_1 is isotropic over K. By the hypothesis on excellence, there exists a form β_3 defined over F such that $\beta_1 \cong_K H \perp \beta_3$. Thus $\alpha \cong_K H \perp \beta_3 \perp \beta_2$ and $\beta_3 \perp \beta_2$ is defined over F. Therefore K/F is an excellent extension.

The converse is trivial.

(4.5) Proposition. Let K/F be such that $\tilde{u}(F) \leq 4$. Then K/F is excellent for 5-dimensional forms.

Proof: Let α be a 5-dimensional form defined over F that is isotropic over K. Let $\det \alpha = r$ and let $\beta = r\alpha \perp \langle -1 \rangle$. Then β is totally indefinite over F since $\dim \beta$ is even and $\det \beta = -1$. Since $\dim \beta = 6 > \tilde{u}(F)$, it follows $1 \in D_F(r\alpha)$. We can write $r\alpha \cong_F \langle 1, a, b, c, abc \rangle$ since $\det r\alpha = 1$. Then $r\alpha$ is a subform $\delta = \langle\langle a, b, c \rangle\rangle$. (Recall that $\langle\langle a, b, c \rangle\rangle = \langle 1, a, b, c, ab, ac, bc, abc \rangle$.) Let $\delta \cong_F r\alpha \perp \gamma$ where γ is defined over F. Since α is isotropic over K, so also is $r\alpha \perp \gamma$. Since δ is a Pfister form, it follows that δ is hyperbolic over K [L, p. 279]. In the Witt ring $W(K)$, the following equations hold: $r\alpha \perp \gamma = 0$, $r\alpha = -\gamma$, $\alpha = -r\gamma$. Then $\alpha \cong_K H \perp -r\gamma$ since both have the

same dimension. Since $-r\gamma$ is defined over F, it follows that K/F is excellent for 5-dimensional forms.

The conclusion of proposition (4.5) holds for an arbitrary linked field. This more general result is essentially contained in [K, p. 10].

(4.6) Theorem. Suppose $\tilde{u}(F) = 4$ and that $\tilde{u}(K) = 4$ for every finite multiquadratic extension K of F. Then the following statements are equivalent.

1) F is 1-amenable.

2) F is 1-amenable for 4-dimensional forms.

3) Each multiquadratic extension K/F is excellent for 4-dimensional forms.

Proof: 1)$\longrightarrow$2). This is trivial.

2)$\longrightarrow$3). This is proven in [ELW_2, (3.3)] for an arbitrary field F.

3)$\longrightarrow$1). To show F is 1-amenable, it is sufficient by [ELW_1, (3.2)] to show that every finite multiquadratic extension K/F is excellent. Since $\tilde{u}(F) < \infty$, F is an ED field, so by (4.4) it is sufficient to show such extensions K/F are excellent for forms of dimension ≤ 5. Any extension is excellent for forms of dimension ≤ 3 (see the proof of (2.27)). By (4.5), K/F is excellent for 5-dimensional forms and by hypothesis, K/F is excellent for

4-dimensional forms. Therefore K/F is excellent so 1) holds.

We strengthen theorem (4.6) in (4.10).

(4.7) Theorem. If $\tilde{u}(F) \leq 2$, then

1) Every finite multiquadratic extension K/F is excellent; and

2) F is 1-amenable.

Proof: 1) If $\tilde{u}(F) \leq 2$, and K is a finite multiquadratic extension of F, then $\tilde{u}(K) \leq 2$ (see [ELP, theorem F] and [EL, (4.3)]). Since F is an ED field, it is sufficient by (4.4) to show K/F is excellent for forms of dimension ≤ 3. This holds for all field extensions.

2) This follows from [ELW_1, (3.2)] and 1).

This theorem has appeared in [ELW_2] with a different proof.

It seems to be an open question if $\tilde{u}(F) = 4$ implies $\tilde{u}(K) = 4$ for every finite multiquadratic extension K of F. This conditions is needed in theorem (4.6) because the proof of the implication 3)$\longrightarrow$1) is based on (4.4) which gives a criterion for an arbitrary extension K/F

to be excellent. As noted in the proof of 3)$\longrightarrow$1), it was enough to show finite multiquadratic extensions are excellent. There is a result in [ELW$_2$] that applies to certain types of extensions including multiquadratic extensions which lets us remove the assumption on multiquadratic extensions in (4.6) and obtain a result that holds for any field with finite Hasse number. The next proposition is a special case of one that appears in [ELW$_2$]. Recall that if G is a subgroup of $\dot{F}$ containing F^2, then $\mathcal{I}_G$ is the ideal in the Witt ring generated by all forms $\langle 1, -g\rangle$, $g \in G$.

(4.8) Proposition. [ELW$_2$, (5.1)] Suppose F satisfies SAP and $K = F(\sqrt{G})$ is a finite multiquadratic extension of F. Let s be an integer ≥ 3 and α a form defined over F such that $|\mathrm{sgn}_P(\alpha)| \leq s$ for each ordering P of F that extends to K. Then there exists a form β defined over F such that $\alpha \equiv \beta \pmod{\mathcal{I}_G}$ and $|\mathrm{sgn}_P(\beta)| < s$ for each $P \in X(F)$.

Proposition (4.8) is the key to the proof of the next theorem. Our proof is quite similar to that given in [ELW$_2$, (6.1)] for a related result.

(4.9) Theorem. Suppose $\tilde{u}(F) = n$ is finite. Let $K = F(\sqrt{G})$ be a finite multiquadratic extension of F.

Then K/F is excellent if and only if K/F is excellent for forms of dimension $\leq n$.

Proof: Suppose K/F is excellent for forms of dimension $\leq n$. Let α be a form defined over F that is isotropic over K. Let $\dim \alpha = m$. Since all extensions are excellent for forms of dimension ≤ 3, we may assume $m \geq 4$ and we may assume $m \geq n+1$. Let $Y \subseteq X(F)$ be the subset of orderings of F that extend to K. Since α is isotropic over K, it follows α is indefinite over F_P for each $P \in Y$. Therefore $|\mathrm{sgn}_P(\alpha)| < m$ for each $P \in Y$. By letting $s = m$, (4.8) implies there exists a form β defined over F such that $\alpha \equiv \beta \pmod{\mathcal{I}_G}$ and $|\mathrm{sgn}_P(\beta)| < m$ for each $P \in X(F)$.

We may assume β is anisotropic over F. Since $\alpha \equiv \beta \pmod{\mathcal{I}_G}$, we have $\alpha = \beta$ in the Witt ring $W(K)$. If $\dim \beta \leq \tilde{u}(F)$, then we are done since then $\dim \beta < n+1 \leq m = \dim \alpha$ and so $\alpha \cong_K \beta \perp rH$ for some r. If $\dim \beta > \tilde{u}(F)$, then since β is anisotropic over F it follows that β is not totally indefinite over F. Therefore $\dim \beta = \max_{P \in X(F)} |\mathrm{sgn}_P(\beta)| < m = \dim \alpha$. Since $\alpha = \beta$ in $W(K)$, we see again that $\alpha \cong_K \beta \perp rH$ for some r. Therefore K/F is excellent.

The converse is trivial.

If we use (4.9) instead of (4.4) we can prove (4.6)

without the assumption $\tilde{u}(K) = 4$ for finite multiquadratic extensions K/F .

(4.10) Corollary. If $\tilde{u}(F) = 4$, then the following are equivalent:

1) F is 1-amenable.

2) F is 1-amenable for 4-dimensional forms.

3) Each finite multiquadratic extension K/F is excellent for 4-dimensional forms.

4) Each finite multiquadratic extension K/F is excellent.

Proof: 1)$\longrightarrow$2) and 2)$\longrightarrow$3) are shown as in (4.6).

3)$\longrightarrow$4). This follows from (4.9) along with the fact that all extensions are excellent for forms of dimension ≤ 3 .

4)$\longrightarrow$1). This follows from [ELW_1, (3.2)].

Shapiro (in private communication) has shown that statments 2) and 3) in corollary (4.10) are equivalent in any linked field.

(4.11) Theorem. Let K/F be given.

1) If F satisfies SAP and $\tilde{u}(K) < \infty$, then K/F satisfies CV(m,n) whenever $m,n \geq \tilde{u}(K)$.

2) If F satisfies ED and $\tilde{u}(K) < \infty$, then K/F

satisfies SCV(m,n) whenever $n \geq \tilde{u}(K)$.

Proof: Let α , β be forms defined over F where $\dim \alpha = m$, $\dim \beta = n$, and suppose $\alpha \perp -\beta$ is isotropic over K . Let $Y \subseteq X(F)$ be the subset of orderings of F that extend to K . Let

$$C_1 = \{P \in Y | \alpha \text{ is positive definite over } F_P\} ,$$

$$C_2 = \{P \in Y | \alpha \text{ is negative definite over } F_P\} ,$$

$$C_3 = \{P \in Y | \beta \text{ is positive definite over } F_P\} ,$$

$$C_4 = \{P \in Y | \beta \text{ is negative definite over } F_P\} .$$

We see that $C_1 = Y \cap \hat{\alpha}^{-1}(m)$ and thus C_1 is closed since Y is closed by (4.1) and $\hat{\alpha}^{-1}(m)$ is the inverse image of a closed set in $\mathbb{Z}$. Similarly, each C_i is closed.

Clearly the sets $C_1 \cup C_3$ and $C_2 \cup C_4$ are closed. The two sets are disjoint for if $P \in C_1 \cap C_4$ or if $P \in C_2 \cap C_3$, then $\alpha \perp -\beta$ is definite over F_P . This can't occur since $\alpha \perp -\beta$ is totally indefinite over K and hence is indefinite over F_P for each $P \in Y$.

If F satisfies SAP, there exists $r \in \dot{F}$ such that $r >_P 0$ if $P \in C_1 \cup C_3$ and $r <_P 0$ if $P \in C_2 \cup C_4$. Then $\alpha \perp -\langle r \rangle$ and $\beta \perp -\langle r \rangle$ are indefinite over F_P for each $P \in Y$ and thus totally indefinite over K .

If $m,n \geq \tilde{u}(K)$, then $r \in D_K(\alpha) \cap D_K(\beta) \cap \dot{F}$ and so K/F satisfies $CV(m,n)$.

Suppose F satisfies ED. Then F also satisfies SAP. Since C_3 and C_4 are disjoint closed sets, we can choose $a \in \dot{F}$ by SAP such that $a >_P 0$ if $P \in C_3$ and $a <_P 0$ if $P \in C_4$. Let $\langle a_1, \ldots, a_m \rangle$ be an effective diagonalization of $a\alpha$. Since $a\alpha \perp -a\beta$ is indefinite over F_P if $P \in Y$ and $a\beta$ is positive definite over F_P if $P \in C_3 \cup C_4$, it follows that $a\alpha$ represents a positive number over F_P for each $P \in C_3 \cup C_4$. Since $W_F(a_1) \subseteq \cdots \subseteq W_F(a_m)$, we see that $a_1 >_P 0$ for each $P \in C_3 \cup C_4$. Then $\langle a_1 \rangle \perp -a\beta$ is indefinite over F_P for each $P \in Y$ since β is indefinite if $P \in Y - (C_3 \cup C_4)$. Let $r = aa_1$. Then $r \in D_F(\alpha)$ and $\langle r \rangle \perp -\beta$ is totally indefinite over K . If $n \geq \tilde{u}(K)$, then $\langle r \rangle \perp -\beta$ is isotropic over K so $r \in D_F(\alpha) \cap D_K(\beta)$. Therefore K/F satisfies $SCV(m,n)$ if $n \geq \tilde{u}(K)$.

(4.12) Corollary. Let $\tilde{u}(F) \leq 2$ and let K be a finite multiquadratic extension of F . Then K/F satisfies $SCV(m,n)$ if $n \geq 2$.

Proof: As noted in (4.7), $\tilde{u}(K) \leq 2$. Since $\tilde{u}(F) < \infty$, F is an ED field, so the result follows from (4.11) 2).

(4.13) Theorem. Let $K = F(\sqrt{G})$ be a finite multiquadratic extension of F and assume F satisfies SAP. Let α be a form defined over F and suppose $\alpha \in I^n(F)$ for some $n \geq 2$. If α is hyperbolic over K, then there exists a form β defined over F such that

1) $\beta \in I^n(F) \cap \mathcal{O}_G$,

2) $\operatorname{sgn}_P(\alpha) = \operatorname{sgn}_P(\beta)$ for each $P \in X(F)$.

Proof: Let $[K:F] = 2^n$ and suppose G is generated by $\{g_1, \ldots, g_n\}$ over F^2. Let $F_i = F(\sqrt{g_1}, \ldots, \sqrt{g_i})$ and let G_i be the subgroup of G generated by $\{g_1, \ldots, g_i\}$ over F^2. Then $F_n = K$ and $F_i = F(\sqrt{G_i})$, and we set $F_0 = F$.

Let C_i be the subset of orderings of F that extend to F_i. Since $\theta_i : X(F_i) \to X(F)$ maps $X(F_i)$ onto C_i, it follows from [ELW$_4$, (4.2)] that C_i is a clopen set.

Let $\gamma_i = \langle 1, -g_i \rangle \otimes \langle 1, 1 \rangle^{n-2}$. Then $\dim \gamma_i = 2^{n-1}$ and $\gamma_i \in I^{n-1}(F)$. Since $\alpha \in I^n(F)$ and $I^n(F)$ is generated by n-fold Pfister forms, we have $\alpha = \perp a_\ell \phi_\ell$ where equality is in the Witt ring $W(F)$, $a_\ell \in \dot{F}$, and the ϕ_ℓ are n-fold Pfister forms. Since $\operatorname{sgn}_P(\phi_\ell)$ equals either 0 or 2^n for each $P \in X(F)$, it follows that $\operatorname{sgn}_P(\alpha)$ is a multiple of 2^n for each $P \in X(F)$.

Suppose by induction that we have constructed a form β_i for some i, $0 \leq i < n$, where β_i is defined over F and is such that

1) $\beta_i \in \mathcal{A}_{G_i} \subseteq \mathcal{A}_G$,

2) $\beta_i \in I^n(F)$,

3) $\operatorname{sgn}_P(\alpha) = \operatorname{sgn}_P(\beta_i)$ for each $P \notin C_i$.

We let $\beta_0 = \langle 0 \rangle$, the zero form. It follows from 1) that $\operatorname{sgn}_P(\beta_i) = 0$ if $P \in C_i$ since $\mathcal{A}_{G_i}$ is generated by $\{\langle 1, -g_j \rangle\}$, $1 \leq j \leq i$, and each $g_j >_P 0$ if $P \in C_i$ since the orderings in C_i extend to $F(\sqrt{G_i})$.

We see that $C_i - C_{i+1}$ consists of the orderings of F that extend to F_i but not to F_{i+1} and thus $g_{i+1} <_P 0$ if $P \in C_i - C_{i+1}$ since $F_{i+1} = F_i(\sqrt{g_{i+1}})$.

For each $P \in X(F)$, $\operatorname{sgn}_P(\alpha)/2^{n-1}$ is even by a remark above. Since F satisfies SAP, every continuous function $X(F) \to 2\mathbb{Z}$ is the signature function of some quadratic form defined over F [KRW, theorem 12]. Thus we can find a form δ_{i+1} defined over F such that

$$\operatorname{sgn}_P(\delta_{i+1}) = \begin{cases} \operatorname{sgn}_P(\alpha)/2^{n-1} & \text{if } P \in C_i \\ 0 & \text{if } P \notin C_i \end{cases} .$$

We are using the fact that C_i is a clopen set so we can patch together the two continuous functions to obtain another continuous function. We see that $\delta_{i+1} \in I(F)$ since $\operatorname{sgn}_P(\delta_{i+1})$ is even.

We note that $\gamma_{i+1} = \langle 1, -g_{i+1} \rangle \otimes \langle 1, 1 \rangle^{n-2}$ and

$$\mathrm{sgn}_P(\gamma_{i+1}) = \begin{cases} 2^{n-1} & \text{if } P \in C_i - C_{i+1} \\ 0 & \text{if } P \in C_{i+1} \end{cases}$$

Then,

$$\mathrm{sgn}_P(\beta_i \perp \gamma_{i+1} \otimes \delta_{i+1}) = \begin{cases} \mathrm{sgn}_P(\alpha) & \text{if } P \notin C_i \,. \\ 0+2^{n-1}(\mathrm{sgn}_P(\alpha)/2^{n-1}) = \mathrm{sgn}_P(\alpha) & \\ \text{if } P \in C_i - C_{i+1} \,. & \\ 0 + 0 \cdot (\quad) = 0 & \text{if } P \in C_{i+1}. \end{cases}$$

We let $\beta_{i+1} = \beta_i \perp \gamma_{i+1} \otimes \delta_{i+1}$ and observe that

1) $\beta_{i+1} \in \mathcal{M}_{G_{i+1}}$ since $\gamma_{i+1} \in \mathcal{M}_{G_{i+1}}$,

2) $\beta_{i+1} \in I^n(F)$ since $\gamma_{i+1} \in I^{n-1}(F)$ and $\delta_{i+1} \in I(F)$,

3) $\mathrm{sgn}_P(\alpha) = \mathrm{sgn}_P(\beta_{i+1})$ for $P \notin C_{i+1}$.

By induction $\beta_n \in \mathcal{M}_G$ and $\mathrm{sgn}_P(\alpha) = \mathrm{sgn}_P(\beta_n)$ for each $P \notin C_n$. As noted earlier, if $P \in C_n$, then $\mathrm{sgn}_P(\beta_n) = 0$. Since α is hyperbolic over K and C_n consists of the orderings of F that extend to $F_n = K$, we see that $\mathrm{sgn}_P(\alpha) = 0$ if $P \in C_n$. Therefore

$\operatorname{sgn}_P(\alpha) = \operatorname{sgn}_P(\beta_n)$ for each $P \in X(F)$. Then setting $\beta = \beta_n$ gives the desired form.

(4.14) Theorem. Let $K = F(\sqrt{G})$ be a finite multiquadratic extension of F. Assume F satisfies SAP and that $I^n(F)$ is torsion free for some $n \geq 2$. Let α be a form defined over F and suppose $\alpha \in I^n(F)$. If α is hyperbolic over K, then $\alpha \in \sigma_G$.

Proof: By theorem (4.13), there exists β defined over F such that $\beta \in I^n(F) \cap \sigma_G$ and $\operatorname{sgn}_P(\alpha \perp -\beta) = 0$ for each $P \in X(F)$. Then $\alpha \perp -\beta$ is a torsion element of $W(F)$ by Pfister's local-global principle [L, p. 240]. Since $\alpha \perp -\beta \in I^n(F)$, it follows that $\alpha \perp -\beta = 0$ in $W(F)$ since $I^n(F)$ is torsion free. Therefore $\alpha = \beta \in \sigma_G$.

(4.15) Theorem. Let F be a linked field.

1) The field F is 1-amenable if and only if F is 1-amenable for 2-fold and 3-fold Pfister forms.
2) If $\tilde{u}(F) = 4$, then F is 1-amenable if and only if F is 1-amenable for 2-fold Pfister forms.
3) If $\tilde{u}(F) \leq 2$, then F is 1-amenable.

Proof: Let $K = F(\sqrt{G})$ be a finite multiquadratic extension of F. Let α be a form defined over F that is hyperbolic over K. Then $\dim \alpha$ is even and since F

is linked we have by [E, (4.4 vi)] $\alpha = \perp_{i=1}^{n} a_i\beta_i$ for some n where $a_i \in F$, β_i is an i-fold Pfister form defined over F, and equality is in the Witt ring $W(F)$.

We show that $a_i\beta_i = 0$ in $W(K)$ for each i. By induction suppose $a_i\beta_i = 0$ in $W(K)$ for $i < j$. We may assume $a_j \neq 0$. Then since $\alpha = 0$ in $W(K)$, we have $a_j\beta_j = -a_{j+1}\beta_{j+1} - \cdots - a_n\beta_n$. The right hand side lies in $I^{j+1}(F)$. Since $\dim a_j\beta_j = 2^j < 2^{j+1}$, it follows from the Arason-Pfister Hauptsatz (see [L, p. 289)] that $a_j\beta_j = 0$ in $W(K)$. Thus by induction, each $a_i\beta_i = 0$.

Since F is linked, it follows from [E, (4.7)] that $\tilde{u}(F) \leq 8$ and $I^m(F)$ is torsion free for $m \geq 4$. Therefore by theorem (4.14), we conclude that $a_i\beta_i \in \mathcal{N}_G$ for $i \geq 4$. If $i = 1$, then $\beta_1 = b\langle 1, -c\rangle$ for some $b,c \in F$. We may assume $a_1 \neq 0$. Since $a_1\beta_1 = 0$ in $W(K)$ implies $a_1b\langle 1, -c\rangle$ is hyperbolic over K, we see that $c \in \dot{F} \cap K^2$ and therefore $c \in G$. It follows $a_1\beta_1 \in \mathcal{N}_G$.

1) If F is 1-amenable for 2-fold and 3-fold Pfister forms, then $a_2\beta_2$ and $a_3\beta_3$ lie in $\mathcal{N}_G$ and so $\alpha \in \mathcal{N}_G$. This shows F is 1-amenable. The converse of 1) is trivial.

2) If $\tilde{u}(F) = 4$, then $I^3(F)$ is torsion free by [E, (4.7)] and the same argument as above gives the result.

3) If $\tilde{u}(F) \leq 2$, then $I^2(F)$ and $I^3(F)$ are torsion free by [E, (4.7)] so F is 1-amenable.

Next we drop the assumption that F is a formally real field and consider how p-adic fields behave with respect to the properties already studied.

(4.16) Theorem. Let K/F be a finite extension of p-adic fields.

1) K/F is excellent.

2) F is 1-amenable.

3) K/F satisfies $SCV(m,n)$ whenever $n \geq 2$ and satisfies $SCV(m,1)$ if $m \neq 2,3$.

4) K/F satisfies $SCV(3,1)$ if $p \neq 2$.

5) K/F satisfies $SCV'(m,n)$ and $CV(m,n)$ for all (m, n) .

Proof: We note for any form α defined over F that if $\dim \alpha \geq 5$ then α is isotropic over F [L, p. 156] and if $\dim \alpha = 4$ and $\det \alpha \neq 1$ then α is isotropic over F [L, p. 158]. If $\dim \alpha = 4$, $\det \alpha = 1$, and α is isotropic, then α is hyperbolic over F .

1) Let α be defined over F and suppose α is isotropic over K . We may assume α is anisotropic over K so $\dim \alpha \leq 4$. Since all extensions are excellent for forms of dimension ≤ 3 , we assume $\dim \alpha = 4$. It follows $\det \alpha = 1$ since α is anistropic. Since α is isotropic over K , we see α is hyperbolic over K so $\alpha \cong_K H \perp H$.

2) By 1) each finite multiquadratic extension is excellent, hence it follows from [ELW_1, (3.2)] that F is

1-amenable.

3) If $m = 1$, K/F satisfies SCV(1,n) trivially for all n. Let α, β be forms defined over F where $\dim \alpha = m$ and $\dim \beta = n$. Assume $D_K(\alpha) \cap D_K(\beta) \neq \emptyset$ and $m,n \geq 2$. If $\alpha \perp -\beta$ is isotropic over F, then $D_F(\alpha) \cap D_F(\beta) \neq \emptyset$. We may assume $\alpha \perp -\beta$ is anistropic over F so $(m, n) = (2, 2)$ and $\det(\alpha \perp -\beta) = 1$. Since $\alpha \perp -\beta$ is isotropic over K, it is actually hyperbolic over K and thus any ternary subform of $\alpha \perp -\beta$ is isotropic over K. If $\alpha = \langle a_1, a_2 \rangle$, it follows that $\langle a_2 \rangle \perp -\beta$ is isotropic over K so $a_2 \in D_F(\alpha) \cap D_K(\beta)$.

If $m \geq 4$, K/F satisfies SCV(m,1) since $\dim(\alpha \perp -\beta) \geq 5$ and so $D_F(\alpha) \cap D_F(\beta) \neq \emptyset$. Thus 3) is shown. We see that 5) follows immediately from 3) since SCV $\rightarrow$ SCV' $\rightarrow$ CV and since K/F satisfies SCV'(m,n) whenever either m or $n \geq 2$ and whenever m or n equals 1.

4) Let α, β be defined over F where $\dim \alpha = 3$ and $\dim \beta = 1$. As before we may assume $\alpha \perp -\beta$ and α are anisotropic over F. It follows from [L, p. 158] that α represents all but exactly one square class of $\dot{F}$ (even if $p = 2$). By (2.2) it is sufficient to show there exists $d \in (\dot{F} - F^2) \cap K^2$ for then $\alpha \perp -d\beta$ is isotropic over F and if $\beta = \langle b \rangle$, then $db \in D_F(\alpha) \cap D_K(\beta)$. Since $\alpha \perp -\beta$ is anisotropic over F and isotropic over K, it follows from Springer's theorem that $[K:F]$ is even.

The result follows from the next proposition.

(4.17) Proposition. Let F be a p-adic field and suppose $[K:F]$ is even. If F is nondyadic ($p \neq 2$), then $(\dot{F} - F^2) \cap K^2 \neq \emptyset$. If F is dyadic, this intersection may be empty.

Proof: Suppose F is nondyadic and $a \in \dot{F} - F^2$. Since $[K:F]$ is even, every ternary form defined over F is isotropic over K, and thus $\dot{F} \subseteq D_K(\langle 1, -a\rangle)$. By the nondegeneracy of the Hilbert symbol, either $D_K(\langle 1, -a\rangle)$ contains exactly one half of the square classes of K or $a \in K^2$. If $a \in K^2$, then we are done. Assume $a \notin K^2$. Since F is nondyadic, we have $|\dot{F}/F^2| = |\dot{K}/K^2| = 4$. Then since $\dot{F} \subseteq D_K(\langle 1, -a\rangle)$ and $D_K(\langle 1, -a\rangle)$ contains exactly two square classes of $\dot{K}$, we see that some nonsquare element of $\dot{F}$ becomes a square in $\dot{K}$.

Suppose now that F is the dyadic field $\mathbb{Q}_2$. Let E be a finite extension of F of odd degree > 1. Let t be an element of $\dot{E}$ such that $\langle t\rangle$ is not defined over F, i.e., $t \in \dot{E} - \dot{F}E^2$. Such an element exists since $|\dot{E}/E^2| > |\dot{F}/F^2|$ by [L, p. 162]. Let $K = E(\sqrt{t})$. Then $[K:F]$ is even. (Note $t \notin E^2$ otherwise $\langle t\rangle \cong_E \langle 1\rangle$.) Suppose $d \in (\dot{F} - F^2) \cap K^2$. Then $d \in \dot{E} - E^2$ since $[E:F]$ is odd. The only nonsquare elements of E that are squares in K are those in the same square class as t.

Then d and t are in the same square class in E which contradicts the choice of t. Therefore $(\dot{F} - F^2) \cap K^2 = \emptyset$ in this example.

We record without proof the following easy result.

(4.18) Proposition. The field of real numbers $\mathbb{R}$ is 1-amenable, $\mathbb{C}/\mathbb{R}$ is excellent, and $\mathbb{C}/R$ satisfies SCV(m,n) for all positive integers m, n.

We close this chapter by considering several other theorems that deal with represented values of quadratic forms over fields with finite Hasse number.

(4.19) Theorem. Let F be a formally real field such that $\tilde{u}(F) < \infty$. Let Y be a closed subset of $X(F)$ and let $G = \bigcap_{P \in Y} P$. Then there exists a form α defined over F such that $D_F(\alpha) = G$ if and only if Y is a clopen set.

Proof: Assume Y is a clopen set. Since Y and $X - Y$ are disjoint closed sets and since F satisfies SAP because $\tilde{u}(F) < \infty$, there exists $a \in \dot{F}$ such that $a >_P 0$ if $P \in Y$ and $a <_P 0$ if $P \in X - Y$. Let $\alpha = \langle a, \ldots, a \rangle \perp \langle 1 \rangle$ where $\dim \alpha = m > \tilde{u}(F)$. Then $D_F(\alpha) \subseteq G$ since α is positive definite over F_P for

each $P \in Y$. Let $b \in G$. Then $\alpha \perp -\langle b \rangle$ is totally indefinite since α is indefinite over F_p for each $P \in X - Y$ and $\alpha \perp -\langle b \rangle$ is indefinite over F_P for each $P \in Y$ since $b >_p 0$ if $P \in Y$. Since $\dim(\alpha \perp -\langle b \rangle) > \tilde{u}(F)$, it follows $\alpha \perp -\langle b \rangle$ is isotropic over F so $b \in D_F(\alpha)$. Therefore $D_F(\alpha) = G$.

Now assume there exists $\alpha = \langle a_1, \ldots, a_n \rangle$ such that $D_F(\alpha) = G$. The function $\hat{\alpha}: X(F) \to \mathbb{Z}$ is continuous where $\hat{\alpha}(P) = \operatorname{sgn}_P(\alpha)$. If $P \in Y$, then $\operatorname{sgn}_P(\alpha) = n$ since $a_i >_P 0$ for each $P \in Y$. If $P \in X - Y$, then since Y is closed, there exists by SAP an element $b \in \dot{F}$ such that $b <_P 0$ and $b >_{P'} 0$ for each $P' \in Y$. Therefore $b \in G = D_F(\alpha)$. Since $b <_P 0$ it follows that α is not positive definite over F_P so $\operatorname{sgn}_P(\alpha) < n$. Therefore $\hat{\alpha}(P) = n$ if $P \in Y$ and $\hat{\alpha}(P) < n$ if $P \in X(F) - Y$. This shows Y is clopen since $Y = \hat{\alpha}^{-1}(n)$ and $\{n\}$ is a clopen set in $\mathbb{Z}$.

The following proposition shows we can replace the hypothesis in (4.19) that Y is closed with the condition that $G \nsubseteq P$ if $P \notin Y$, i.e., $G = \bigcap_{P \in Y} P$ is a "maximal" intersection.

(4.20) If F satisfies SAP, then the following statements are equivalent.

1) $Y \subseteq X(F)$ is closed.

2) If $G = \bigcap_{P \in Y} P$, then $G \not\subseteq P$ if $P \notin Y$.

Proof: Suppose 1) holds and let $P \notin Y$. Pick b using SAP such that $b <_P 0$ and $b >_{P'} 0$ if $P' \in Y$. Then $b \in G$ and $b \notin P$ so $G \not\subseteq P$.

Suppose 2) holds and let $P \notin Y$. Then $G \not\subseteq P$ so there exists $b \in G$ such that $b \notin P$, i.e., $b <_P 0$. Thus $W_F(b)$ is an open set containing P such that $W_F(b) \cap Y = \emptyset$. Therefore $P \notin \overline{Y}$. This is true for each $P \notin Y$ so $Y = \overline{Y}$ and Y is closed.

(4.21) Theorem. Suppose $\tilde{u}(F) \leq m$ and $\alpha_1, \ldots, \alpha_n$ are forms defined over F such that $\dim \alpha_i \geq m$ for each i and $\alpha_1, \ldots, \alpha_n$ represent a common value in each real closure F_P of F. Let $C_1, \ldots, C_t$ be disjoint closed sets in $X(F)$. Assume each α_i is indefinite in F_P for $P \in C_j$, $1 \leq j \leq t$. Then $\alpha_1, \ldots, \alpha_n$ represent a common value r over F such that for each C_j, r has a constant prescribed sign in F_P for each $P \in C_j$.

Proof: Let $A = \{P \in X(F) \mid$ for some i, the form α_i is positive definite over $F_P\}$ and let $B = \{P \in X(F) \mid$ for some i, the form α_i is negative definite over $F_P\}$. Then A and B are disjoint closed sets since each is a union of n closed sets and $P \in A \cap B$ implies some α_i

and α_j don't represent a common value in F_P. It follows A, B, C_1, ..., C_t are mutually disjoint closed sets. Since $\tilde{u}(F) < \infty$, it follows F satisfies SAP. Using SAP, pick $r \in \dot{F}$ such that

1) $r <_P 0$ if $P \in B$,

2) $r >_P 0$ if $P \in A$,

3) r has the prescribed sign in F_P for $P \in C_j$, $1 \leq j \leq t$.

Each $\alpha_i \perp -\langle r \rangle$ is totally indefinite over F since if α_i is not indefinite over F_P, then $\alpha_i \perp -\langle r \rangle$ is indefinite over F_P by the construction of r. Since $\dim(\alpha_i \perp -\langle r \rangle) \geq m+1 > \tilde{u}(F)$, it follows $r \in D_F(\alpha_i)$, $1 \leq i \leq n$, and r has the prescribed signs in F_P, $P \in C_j$, $1 \leq j \leq t$.

(4.22) Theorem. Let F be a number field and let α_1, ..., α_n be forms defined over F such that for each $p \in \Omega(F)$, α_1, ..., α_n represent a common value over F_p. Let $S = \{p_1, \ldots, p_m\}$ be a finite nonempty subset of $\Omega(F)$. For each $p \in S$, let $r_p \in \dot{F}_p$ denote a common value represented by each α_i over F_p. Then α_1, ..., α_n each represent over F a common value r such that $\langle r \rangle \cong_{F_p} \langle r_p \rangle$ for each $p \in S$.

Proof: Suppose $\dim \alpha_i = 1$ for some i. Then $\alpha_i = \langle r \rangle$ for some $r \in \dot{F}$ and $\langle r \rangle \cong_{F_p} \langle r_p \rangle$ for each

$p \in S$. By hypothesis, $\alpha_1, \ldots, \alpha_n$ each represent r over F_p for each $p \in \Omega(F)$ because α_i represents exactly one square class over each F_p . It follows from the Hasse-Minkowski theorem that $\alpha_1, \ldots, \alpha_n$ each represent r over F .

Now assume $\dim \alpha_i \geq 2$, $1 \leq i \leq n$. Let T be the set of primes p in $\Omega(F) - S$ that contains all dyadic primes, all infinite primes, and those primes p for which some α_i is not isometric to a unit form over F_p . For each $p \in T$, we also let r_p denote a common value represented by $\alpha_1, \ldots, \alpha_n$ over F_p . Since T is a finite set, we can use the approximation theorem to find $r_1 \in \dot{F}$ such that $r_1 \cong_{F_p} \langle r_p \rangle$ for each $p \in T \cup S$.

Let the modulus $m = \prod_{p \in T \cup S} p^{e(p)}$ have sufficiently large exponents such that $F_{m,1} \subseteq F_p^2$ for each $p \in T \cup S$. Let $\{p_1, \ldots, p_t\}$ be the (possibly empty) set of primes p not in $T \cup S$ such that $\operatorname{ord}_p(r_1)$ is odd. Using the generalized Dirichlet theorem on primes, choose a prime ideal $q \in i(F_{m,1})(p_1 \cdots p_t)^{-1}$ such that $q \notin T \cup S$. Then there exists $x \in F_{m,1}$ such that $(x) = (p_1 \cdots p_t)q$. We show $r = r_1 x$ is represented by $\alpha_1, \ldots, \alpha_n$ over F and $\langle r \rangle \cong_{F_p} \langle r_p \rangle$ for each $p \in S$.

If $p \in T \cup S$, each $\alpha_i \perp -\langle r \rangle$ is isotropic over F_p because $x \in F_p^2$ and $r_1 \in D_{F_p}(\alpha_i)$. If $p \notin T \cup S$ and

dim $\alpha_i \geq 3$, then α_i is isotropic over F_p because p is nondyadic and α_i is isometric to a unit form, and so $\alpha_i \perp -\langle r \rangle$ is also isotropic over F_p . If $p \notin T \cup S$ and dim $\alpha_i = 2$, then $\alpha_i \perp -\langle r \rangle$ could be anisotropic over F_p only if $ord_p(r)$ is odd. If $p \notin T \cup S$, we see that $ord_p(r) = ord_p(r_1 x)$ is odd only if $p = q$. Thus $\alpha_i \perp -\langle r \rangle$ is anisotropic over F_p for at most one prime p in $\Omega(F)$. Since the Hilbert reciprocity theorem implies a ternary form is anisotropic over F_p for an even number of primes, it follows $\alpha_i \perp -\langle r \rangle$ is isotropic over F_p for all $p \in \Omega(F)$. Therefore by the Hasse-Minkowski theorem, $\alpha_i \perp -\langle r \rangle$ is isotropic over F for all i . We see $r \in D_F(\alpha_i)$ for each i and for each $p \in S$ we have $\langle r \rangle \cong_{F_p} \langle r_1 x \rangle \cong_{F_p} \langle r_1 \rangle \cong_{F_p} \langle r_p \rangle$.

(4.23) Corollary. With the same assumptions as in (4.22), suppose also that $\alpha_1, \ldots, \alpha_n$ are isotropic over F_p for each $p \in S$. Let $r_p \in \dot{F}_p$ be given for each $p \in S$. Then $\alpha_1, \ldots, \alpha_n$ represent over F a common value r such that $\langle r \rangle \cong_{F_p} \langle r_p \rangle$ for each $p \in S$.

Proof: This follows immediately from (4.22) since $\alpha_1, \ldots, \alpha_n$ represent over F_p all square classes of $\dot{F}_p$ for each $p \in S$.

BIBLIOGRAPHY

BIBLIOGRAPHY

[Ar] E. Artin. Algebraic Numbers and Algebraic Functions. Gordon and Breach: New York, 1967.

[E] R. Elman. Quadratic Forms and the u-Invariant III. Conference of Quadratic Forms, 1976 (G. Orzech, ed.), Queen's Papers in Pure and Applied Mathematics, 46: 422-444. Queen's University, Kingston, Ontario, Canada, 1977.

[EL] R. Elman and T.Y. Lam. Quadratic forms and the u-invariant I . Math. Zeit. 131:283-304 (1973).

[ELP] R. Elman, T.Y. Lam and A. Prestel. On some Hasse principles over formally real fields. Math Zeit. 134:291-301 (1973).

[ELW_1] R. Elman, T.Y. Lam and A. Wadsworth. Amenable Fields and Pfister Extensions. Conference on Quadratic Forms, 1976 (G. Orzech, ed.), Queen's Papers in Pure and Applied Mathematics, 46:445-492. Queen's University, Kingston, Ontario, Canada, 1977.

[ELW_2] R. Elman, T.Y. Lam and A. Wadsworth. Function fields of Pfister forms. Invent. Math. 51:61-75 (1979).

[ELW_3] R. Elman, T.Y. Lam and A. Wadsworth. Pfister ideals in Witt rings. Math. Ann. 245:219-245 (1979).

[ELW_4] R. Elman, T.Y. Lam and A. Wadsworth. Orderings under field extensions. J. reine angew. Math. 306:7-27 (1979).

[J] G. Janusz. Algebraic Number Fields. Academic Press: New York, 1973.

[K] M. Knebusch. Generic splitting of quadratic forms, II. Proc. London Math. Soc. (3)34:1-31 (1977).

[KRW] M. Knebusch, A. Rosenberg and R. Ware. Structures of Witt rings, quotients of abelian group rings, and orderings of fields. Bull. Amer. Soc. 77:205-210 (1971).

[L] T.Y. Lam. The Algebraic Theory of Quadratic Forms. W.A. Benjamin: Reading, Mass., 1973.

[OM] O.T. O'Meara. Introduction to Quadratic Forms. Springer: Heidelberg, 1963.

[P] A. Prestel. Remarks on the Pythagoras and Hasse number of real fields. J. reine angew. Math. 303: 284-294 (1978).

[PW] A. Prestel and R. Ware. Almost isotropic quadratic forms. J. London Math. Soc. (2)19:241-244 (1979).

[R] J. Rotman. The Theory of Groups. Allyn and Bacon, Inc.: Boston, 1973.

[S] J.P. Serre. Local Fields. Springer-Verlag: Heidelberg, 1979.

[W] A. Weil. Basic Number Theory. Springer-Verlag: Heidelberg, 1974.

[Wi] E. Witt. Theorie der quadratischen Formen in beliebigen Körpern. J. reine angew. Math. 176:31-44 (1937).

[Wr_1] R. Ware. Some Remarks on the Map Between Witt Rings of an Algebraic Extension. Conference on Quadratic Forms, 1976 (G. Orzech, ed.), Queen's Papers in Pure and Applied Mathematics, 46:634-649. Queen's University, Kingston, Ontario, Canada, 1977.

[Wr_2] R. Ware. Hasse principles and the u-invariant over formally real fields. Nagoya Math. J. 61:117-125 (1976).

[WS] A. Wadsworth and D. Shapiro. On multiples of round and Pfister forms. Math. Zeit. 157:53-62 (1977).

[Ww] A Wadsworth, private communication.