POLSKA AKADEMIA NAUK, INSTYTUT MATEMATYCZNY

DISSERTATIONES MATHEMATICAE

(ROZPRAWY MATEMATYCZNE)

CLII

K. SZYMICZEK

Quadratic forms over fields

WARSZAWA 1977
PAŃSTWOWE WYDAWNICTWO NAUKOWE

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

CONTENTS

Introduction

This paper is concerned with some aspects of the theory of quadratic forms over fields of characteristic other than 2. We are primarily interested in investigating the behaviour of the totality of quadratic forms over a field rather than the properties of some particular forms. Thus we are led to consider the set $M(F)$ of equivalence classes of non-singular quadratic forms over the field F, equipped with two binary operations induced by the orthogonal sum and the tensor product of quadratic forms. Since the algebraic structure of $M(F)$ is not quite satisfactory ($M(F)$ is a semi-ring, although the cancellation law holds for addition), we extend it by a universal construction to obtain the Grothendieck ring $G(F)$ containing $M(F)$ and additively generated by $M(F)$. We consider the ring $G(F)$ as an object reflecting and characterizing the behaviour of equivalence classes of quadratic forms over the field F and we focus our attention almost exclusively on the properties of $G(F)$.

Another possibility is to consider the behaviour of similarity classes of quadratic forms over F and the Witt ring $W(F)$ characterizing this behaviour. $W(F)$ can be defined as the factor ring $G(F)/H$, where H denotes the principal ideal generated by the hyperbolic plane. The Witt ring has become far more popular than the Grothendieck ring and this seems to be caused by two reasons. Firstly, $W(F)$ is always "smaller" than $G(F)$, and secondly, its elements can be naturally interpreted as similarity classes of anisotropic forms, while in $G(F)$ we have to deal with formal differences of equivalence classes.

Our first concern in the present paper is to formulate and prove the basic properties of the ring $G(F)$. We describe all prime ideals of the ring $G(F)$ and then we use the obtained information to give full descriptions of nilpotents, units, torsion elements, divisors of zero and idempotents in $G(F)$. We also show that torsionness, nilpotency and invertibility of an element are local properties of $G(F)$. This is done in Chapter II, where our purpose is to develop the general theory of the ring $G(F)$ approximately as far as it has been expanded for the Witt ring $W(F)$ and to give proofs based exclusively on quadratic form theory. Some of the results in Chapter II, §§1, 2, have been proved by M. Knebusch, A. Rosenberg, and R. Ware [12] by unified purely ring theoretical methods for a class of rings containing Grothendieck and Witt rings.

In Chapter III we study the group structure of $G(F)$ and $W(F)$, the main objective being decompositions into direct sums of cyclic groups. We prove two general decomposition theorems giving, for any field F, two cyclic direct summands of the additive group $G(F)$. This makes the transition from a direct sum decomposition of $G(F)$ to a similar decomposition of $W(F)$ quite clear and, in particular, this enables us to simplify the determination of the Grothendieck group of a local field. Further applications of the decomposition theorems are presented in Chapter III, §2, where the Grothendieck and Witt groups are decomposed into direct sums of cyclic groups for a number of classes of fields with prescribed value sets of binary forms. We also give exact bounds for the rank of the Grothendieck group of a field with given square class number. The decomposition theorems allow us to carry over the results automatically for the case of Witt groups.

The fourth chapter contains a systematic study of the methods of classifying fields with respect to the behaviour of quadratic forms. The main idea consists in considering two fields to be equivalent if the corresponding Grothendieck (or Witt) rings (or groups) are isomorphic.

In Chapter V we introduce and discuss a certain Galois correspondence between the value sets of binary forms over a field and some groups of binary forms. A generalization to the case of linked Pfister forms is also sketched.

In Chapter VI a particular problem, which has been left unsolved in [29], is discussed. The problem consists in constructing two fields with prescribed behaviour of quadratic forms. We show that the existence of one of them implies the existence of the other.

At the end of the paper we collect 10 problems arising from the context of the paper.

A general reference for notions and facts used in the paper is T. Y. Lam's book [15]. Also W. Scharlau [24] gives many details of the theory of the Grothendieck and Witt rings; see also F. Lorenz [17] for the theory of Witt rings. A more general approach is presented by J. Milnor and D. Husemoller [21]. However, two basic papers for the algebraic theory of quadratic forms are E. Witt [31] and A. Pfister [23]. The results of these two papers are often quoted without explicitly mentioning the source (cancellation, piecewise equivalence, properties of Pfister forms and their consequences for the Witt ring).

We use standard terminology and notation. The orthogonal sum and the tensor product of quadratic forms are denoted by $\perp$ and $\otimes$, respectively, but in $M(F)$, $G(F)$ and $W(F)$ we use the usual plus and dot. For a natural number n and a form φ we write $n \times \varphi$ for the orthogonal sum $\varphi \perp \ldots \perp \varphi$ (n times). This is to be distinguished from the scalar multiple $a\varphi$ of the form φ by an element a of F. The diagonalized form

$\varphi = \sum a_i x_i^2$ will be denoted by $\varphi = (a_1, \ldots, a_n)$ and its equivalence class by $\langle\varphi\rangle = \langle a_1, \ldots, a_n\rangle$. We denote by $g(F)$ the factor group F^*/F^{*2} and by $q = q(F)$ the cardinality $|g(F)|$ of $g(F)$. If φ represents $a \in F^*$, we write $\varphi \approx a$. The set of all elements of F^* represented by φ is denoted by $D_F(\varphi)$ and the set of square classes (i.e., elements of $g(F)$) represented by φ is denoted by $D(\varphi)$ or $D_{g(F)}(\varphi)$. The square class aF^{*2} will be always written simply as a. We use $\cong$ to denote the equivalence of quadratic forms; thus $\varphi \cong \psi$ is equivalent to $\langle\varphi\rangle = \langle\psi\rangle$.

The form $\varphi = (1, a_1) \otimes \ldots \otimes (1, a_n)$ is called n-fold Pfister form; we write also briefly $\varphi = ((a_1, \ldots, a_n))$ and $\langle\varphi\rangle = \langle\langle a_1, \ldots, a_n\rangle\rangle$.

For an abelian group G and a natural number n the symbol G^n denotes direct sum of n copies of the group G.

If I is a set, $G^{(I)}$ denotes direct sum of $|I|$ copies of the group G (this is to be distinguished from G^I, the direct product of $|I|$ copies of G).

If R is a ring and T is a subset of R, then the ideal generated by T will be denoted by (T).

We use the standard symbols $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{C}$ for the integers, the rationals, the reals and the complex numbers.

We make two general assumptions to be in force throughout the paper: all fields considered are assumed to have characteristic different from two and all quadratic forms are assumed to be non-singular.

Chapter I

Preliminaries on round and Pfister forms

A quadratic form ϱ over F is said to be *round* if either ϱ is anisotropic and $\varrho \cong a\varrho$ for every $a \in D_F(\varrho)$ or ϱ is hyperbolic. Any Pfister form is round, but, in general, a round form need not be Pfister. All round forms have been determined over global fields and over $\boldsymbol{R}(t)$ and its algebraic extensions (see Hsia and Johnson [10] and Elman [3]) and also over some other fields (Marshall [19]). We shall prove here the following result which generalizes the Main Lemma 2.1 of [30]. A special case will be used in Chapter III.

PROPOSITION 1. *Let ϱ be a round anisotropic form and let φ be an arbitrary form of dimension at least two. The form $\varrho \otimes \varphi$ is isotropic if and only if there exists a form ψ such that*

$$\varrho \otimes \varphi \cong \varrho \otimes (1, -1) \perp \varrho \otimes \psi. \tag{1.1}$$

Proof. The "if" part is trivial and we prove the converse by induction on $t = \dim\varphi$. So assume $\varrho \otimes \varphi$ is isotropic. On scaling φ we may assume that φ has the diagonalization

$$\varphi = (1, a_2, a_3, \ldots, a_t),$$

where for brevity we shall write a instead of a_2. If $t = 2$, then $\varrho \otimes \varphi$ is isotropic and round (by Scharlau [24], Lemma 2.1.2), hence hyperbolic, hence (1.1) holds for $\psi = 0$. Now assume $t \geqslant 3$ and write $\beta = (1, a)$, so that $\varphi = \beta \perp \tau$, where $\tau = (a_3, \ldots, a_t)$. Since $\varrho \otimes \beta \perp \varrho \otimes \tau$ is isotropic, there exists $b \in F^*$ such that

$$b \in D_F(\varrho \otimes \beta) \quad \text{and} \quad -b \in D_F(\varrho \otimes \tau).$$

Now $\varrho \otimes \beta$ is round, hence

$$\varrho \otimes \beta \cong b \cdot \varrho \otimes \beta \cong \varrho \otimes (b, ab). \tag{1.2}$$

On the other hand, $-b \in D_F(\varrho \otimes \tau)$ implies that $\varrho \otimes (\tau \perp (b))$ is isotropic; moreover, $\dim(\tau \perp (b)) = t-1$, hence by the induction hypothesis there exists a form ψ_1 such that

$$\varrho \otimes (\tau \perp (b)) \cong \varrho \otimes (1, -1) \perp \varrho \otimes \psi_1 \cong \varrho \otimes (b, -b) \perp \varrho \otimes \psi_1.$$

By Witt's cancellation theorem (Witt [31], Satz 4), we get

$$\varrho \otimes \tau \cong \varrho \otimes (-b) \perp \varrho \otimes \psi_1. \tag{1.3}$$

Now (1.2) and (1.3) give

$$\varrho \otimes \varphi \cong \varrho \otimes \beta \perp \varrho \otimes \tau \cong \varrho \otimes (b, -b) \perp \varrho \otimes \big(\psi_1 \perp (ab)\big) \cong \varrho \otimes (1, -1) \perp \varrho \otimes \psi,$$

as required.

COROLLARY 2. *Retain the hypothesis of the proposition. Then*

(i) *The Witt index i of the form $\varrho \otimes \varphi$ is either* 0 *or a multiple of* $\dim \varrho$ *and there exists a form σ such that*

$$\varrho \otimes \varphi \cong i \times (1, -1) \perp \varrho \otimes \sigma.$$

(ii) *If $\varrho \otimes \varphi$ represents $b \in F^*$, then there exists a form ψ such that*

$$\varrho \otimes \varphi \cong \varrho \otimes \big((b) \perp \psi\big). \tag{2.1}$$

Proof. (i) is proved by easy induction on $t = \dim \varphi$.

(ii) If $b \in D_F(\varrho \otimes \varphi)$, then $\varrho \otimes \big(\varphi \perp (-b)\big)$ is isotropic, so there exists a form ψ such that $\varrho \otimes \big(\varphi \perp (-b)\big) \cong \varrho \otimes (b, -b) \perp \varrho \otimes \psi$. On cancelling $\varrho \otimes (-b)$ we obtain (2.1).

Remark 3. In Chapter III we shall use Proposition 1 in the special case where $\varrho = 2^n \times (1)$: if $2^n \times \varphi$ is isotropic, then $2^n \times \varphi \cong 2^n \times (1, -1) \perp 2^n \times \psi$.

The following result is used repeteadly in the papers [4] and [5] of Elman and Lam and is proved there by using the techniques of the paper of Arason and Pfister [1]. We shall show that it is a simple consequence of Proposition 1, thus giving a new proof for the result. We state the result in a slightly more general setting, with round forms instead of Pfister forms.

PROPOSITION 4 (Elman and Lam [4], Theorem 1.4). *Let ϱ be a round form and let q be an anisotropic form over F. If q lies in the principal ideal $\varrho \cdot W(F)$, then there exists a form σ such that $q \cong \varrho \otimes \sigma$. If $a \in D_F(q)$, then σ can be chosen so that $a \in D_F(\sigma)$ also.*

Proof. There exist a non-negative integer m and a form φ such that $\varrho \otimes \varphi \cong q \perp m \times (1, -1)$. If $m = 0$, we are finished. If $m > 0$, the form $\varrho \otimes \varphi$ is isotropic and by Corollary 2(i) there exists a form σ such that

$$\varrho \otimes \varphi \cong \varrho \otimes \sigma \perp i \times (1, -1),$$

where i is the Witt index of $\varrho \otimes \varphi$. Since q is anisotropic, we have $m = i$, and hence $q \cong \varrho \otimes \sigma$.

We prove the last statement by using an idea due to J. Wuwer. First observe that for any round form ϱ and any $b_1, \ldots, b_n \in D_F(\varrho)$ and

arbitrary $c_1, \ldots, c_n \in F^*$, we have

$$\varrho \otimes (c_1, \ldots, c_n) \cong \varrho \otimes (b_1 c_1, \ldots, b_n c_n).$$

Now, if $a \in D_F(q) = D_F(\varrho \otimes \sigma)$ and $\sigma = (c_1, \ldots, c_n)$, then $a = b_1 c_1 + \ldots + b_n c_n$, where either $b_i \in D_F(\varrho)$ or $b_i = 0$. Put $d_i = b_i$ if $b_i \neq 0$ and $d_i = 1$ if $b_i = 0$. Then $d_i \in D_F(\varrho)$, $1 \leqslant i \leqslant n$, and $q \cong \varrho \otimes \sigma \cong \varrho \otimes (d_1 c_1, \ldots, d_n c_n)$. Thus $q \cong \varrho \otimes \sigma_1$, where $\sigma_1 = (d_1 c_1, \ldots, d_n c_n)$ certainly represents a.

Remark 5. In the case of $\dim \varrho = 2$ it is possible to prove a stronger result than Proposition 1. In fact, if ϱ is an arbitrary binary form and φ is any form of dimension $\geqslant 2$, then $\varrho \otimes \varphi$ isotropic implies that φ contains a binary subform β such that $\varrho \otimes \beta$ is hyperbolic, that is, we have again

$$\varrho \otimes \varphi \cong \varrho \otimes \beta \perp \varrho \otimes \psi, \quad \text{where} \quad \varrho \otimes \beta \cong \varrho \otimes (1, -1),$$

but now $\beta \perp \psi = \varphi$.

This is Elman and Lam's Proposition 2.2 of [6], which is the basis for the β-decomposition of φ (cf. [6], p. 289).

Chapter II

Basic properties of the Grothendieck ring

§ 1. Prime ideals in $G(F)$. The dimension homomorphism $\dim: G(F) \to \mathbf{Z}$ enables us to find a family of prime ideals in $G(F)$. These are the inverse images of prime ideals of $\mathbf{Z}$. We denote them by

$$J_0 = \dim^{-1}(0) = \{A \in G(F): \dim A = 0\}$$

and

$$J_p = \dim^{-1}(p) = \{A \in G(F): \dim A \equiv 0 \pmod{p}\},$$

for any prime number p. It turns out that these are all prime ideals in $G(F)$ if F is a non-real field (cf. Theorem 1.6 below). If F is a real field and P is an ordering on F, we consider the signature homomorphism $\sigma_P: G(F) \to \mathbf{Z}$ defined by P. Here also the inverse images of prime ideals of $\mathbf{Z}$ are prime ideals of $G(F)$, and we shall prove that every prime ideal in $G(F)$ different from J_0 and J_p can be obtained in that way.

We begin with the following observation.

PROPOSITION 1.1. *If* $\mathfrak{p}$ *is a prime ideal in* $G(F)$, *then either* $G(F)/\mathfrak{p} \cong \mathbf{Z}$ *or* $G(F)/\mathfrak{p} \cong \mathbf{Z}/p\mathbf{Z}$ *for a prime number* p. *In the first case* $\mathfrak{p}$ *is a minimal prime ideal and in the second case* $\mathfrak{p}$ *is maximal.*

Proof. For any $a \in F^*$ we have $(\langle 1\rangle + \langle a\rangle)(\langle 1\rangle - \langle a\rangle) = 0$ in $G(F)$, hence for any prime ideal $\mathfrak{p}$ we have either $\langle a\rangle \equiv \langle 1\rangle \bmod \mathfrak{p}$ or $\langle a\rangle \equiv -\langle 1\rangle \bmod \mathfrak{p}$. Since $G(F)$ is additively generated by $\{\langle a\rangle: a \in F^*\}$, it follows that the unique ring homomorphism

$$\mathbf{Z} \to G(F) \to G(F)/\mathfrak{p}$$

is surjective, and since $G(F)/\mathfrak{p}$ is an integral domain, we obtain the alternative of the proposition. The prime ideals of the second type are obviously maximal. Now let $\mathfrak{p}$ be a prime ideal with $G(F)/\mathfrak{p} \cong \mathbf{Z}$. Suppose there exists another prime ideal $\mathfrak{p}'$ such that $\mathfrak{p}' \subset \mathfrak{p}$. Since $\mathfrak{p}'$ is not maximal, we must have $G(F)/\mathfrak{p}' \cong \mathbf{Z}$. Hence the canonical homomorphism $G(F)/\mathfrak{p}' \to G(F)/\mathfrak{p}$ has zero kernel and so $\mathfrak{p} \subset \mathfrak{p}'$, whence $\mathfrak{p}' = \mathfrak{p}$. Thus $\mathfrak{p}$ is minimal.

EXAMPLE 1.2. J_0 is a minimal prime ideal and J_p is maximal, for any prime number p. Moreover, if F is a real field, then for every ordering P on F, $\operatorname{Ker}\sigma_P = \mathfrak{p}_0$ is a minimal prime ideal, and for every prime number p the ideal

$$\mathfrak{p}_p = \{A \in G(F): \sigma_P(A) \equiv 0 \pmod{p}\}$$

is maximal.

PROPOSITION 1.3. (i) *J_0 is additively generated by the elements $\langle 1\rangle - \langle a\rangle$, $a \in F^*$.*

(ii) *J_0 is the unique minimal prime ideal $\mathfrak{p}$ with the property*

$$\langle 1\rangle \equiv \langle -1\rangle \bmod \mathfrak{p}.$$

Proof. (i) is well known (cf. Lam [15], p. 35).

(ii) Suppose $\mathfrak{p}$ is a minimal prime ideal and $\langle 1\rangle \equiv \langle -1\rangle \bmod \mathfrak{p}$. As observed in the proof of Proposition 1.1, for every $a \in F^*$ we have $\langle a\rangle \equiv \pm\langle 1\rangle \bmod \mathfrak{p}$. If for every $a \in F^*$ we have $\langle a\rangle \equiv \langle 1\rangle \bmod \mathfrak{p}$, then by (i), $J_0 \subset \mathfrak{p}$ and so $J_0 = \mathfrak{p}$. If there is an $a \in F^*$ such that $\langle a\rangle \not\equiv \langle 1\rangle \bmod \mathfrak{p}$, then from the equality $(\langle 1\rangle - \langle a\rangle)(\langle 1\rangle - \langle -a\rangle) = 0$ we obtain $\langle 1\rangle - \langle -a\rangle \equiv 0 \bmod \mathfrak{p}$. But then $\langle 1\rangle - \langle a\rangle = \langle 1\rangle - \langle -1\rangle - (\langle 1\rangle - \langle -a\rangle) \equiv 0 \bmod \mathfrak{p}$, a contradiction. Hence such an a cannot exist and (ii) is proved.

The above proof shows that the following holds true.

COROLLARY 1.4. *If $\mathfrak{p}$ is a prime ideal in $G(F)$ and $\langle 1\rangle \equiv \langle -1\rangle \bmod \mathfrak{p}$, then $J_0 \subset \mathfrak{p}$.*

PROPOSITION 1.5. *Suppose F is a real field, P is an ordering on F and σ_P is the signature homomorphism defined by P. Then*

(i) *$\operatorname{Ker}\sigma_P$ is a minimal prime ideal in $G(F)$;*

(ii) *$\operatorname{Ker}\sigma_P$ is additively generated by $\langle 1, -1\rangle$ and all the elements $\langle 1\rangle - \langle a\rangle$, where $a \in P$.*

Proof. (i) has already been noticed (cf. Example 1.2).

(ii) We shall use the following three identities:

$$\langle a\rangle - \langle b\rangle = \langle 1\rangle - \langle b\rangle - (\langle 1\rangle - \langle a\rangle), \tag{1.5.1}$$

$$\langle a\rangle - \langle b\rangle = \langle -b\rangle - \langle -a\rangle, \tag{1.5.2}$$

$$\langle a, b\rangle = \langle a\rangle - \langle -b\rangle + \langle 1, -1\rangle. \tag{1.5.3}$$

Assume $A - B \in \operatorname{Ker}\sigma_P$, where $A = \langle a_1, \ldots, a_n\rangle$, $B = \langle b_1, \ldots, b_m\rangle$ and without loss of generality let $n \geqslant m$. Write

$$A - B = \langle a_1\rangle - \langle b_1\rangle + \ldots + \langle a_m\rangle - \langle b_m\rangle + \langle a_{m+1}, \ldots, a_n\rangle.$$

If a_i and b_i are both positive at P, we use (1.5.1) to represent $\langle a_i\rangle - \langle b_i\rangle$ through the elements specified in (ii). Similarly when a_i and b_i are both negative at P, we use first (1.5.2) and then (1.5.1). If a_i and b_i are of opposite signs at P, use (1.5.3) to obtain $\langle a_i\rangle - \langle b_i\rangle = \langle a_i, -b_i\rangle - \langle 1, -1\rangle$.

After doing that for $i = 1, \ldots, m$, we obtain

$$A - B = C + \langle c_1, \ldots, c_r \rangle,$$

where C is expressed in terms of the elements specified in (ii). Here $\sigma_P \langle c_1, \ldots, c_r \rangle = 0$, so that r is even and the number of positive c_i's equals to the number of negative c_i's. Hence we can write

$$\langle c_1, \ldots, c_r \rangle = \langle d_1, e_1 \rangle + \ldots + \langle d_t, e_t \rangle,$$

where all the d's are positive (and all the e's are negative) at P. Now we use (1.5.3) and (1.5.1) to express $\langle c_1, \ldots, c_r \rangle$ in terms of the elements specified in (ii). Hence $\operatorname{Ker} \sigma_P$ is contained in the ideal generated by $\langle 1, -1 \rangle$ and $\langle 1 \rangle - \langle a \rangle$, $a \in P$. Since any of these has signature 0, we are finished.

Now we are in a position to describe completely the prime ideals in the ring $G(F)$, for any field F.

THEOREM 1.6. (i) *If F is a non-real field, then J_0 and J_p (for all prime numbers p) are the only prime ideals in $G(F)$. J_0 is the unique minimal prime ideal and all the J_p are maximal ideals containing J_0.*

(ii) *If $\mathfrak{p}$ is a prime ideal in $G(F)$ different from J_0 and all the J_p, then F is a real field and*

$$P = \{a \in F^* : \langle a \rangle \equiv \langle 1 \rangle \bmod \mathfrak{p}\}$$

constitutes an ordering on F.

(iii) *If $\mathfrak{p}$ is a minimal prime ideal in $G(F)$ different from J_0 and P is as in* (ii), *then $\mathfrak{p} = \operatorname{Ker} \sigma_P$.*

(iv) *If $\mathfrak{p}$ is a prime ideal in $G(F)$ different from all the J_p and $\mathfrak{p}$ is not minimal, then $\mathfrak{p}$ is maximal and there exists a prime number p such that*

$$\mathfrak{p} = \{A \in G(F) : \sigma_P(A) \equiv 0 \bmod p\},$$

where P denotes the ordering on F defined in (ii).

Proof. (i) follows from (ii) and Example 1.2. So we start the proof with (ii). We have to prove the following:

$$P \cdot P \subset P, \tag{1.6.1}$$

$$P \cup -P = F^*, \tag{1.6.2}$$

$$P + P \subset P. \tag{1.6.3}$$

Here (1.6.1) is obvious and to prove (1.6.2) we once again make use of the equality $(\langle 1 \rangle - \langle a \rangle)(\langle 1 \rangle - \langle -a \rangle) = 0$. The proof of (1.6.3) is a bit harder. First we shall prove that under the hypotheses (ii),

$$\langle 1 \rangle \not\equiv \langle -1 \rangle \bmod \mathfrak{p}. \tag{1.6.4}$$

Contrary to this, let us assume that $\langle 1 \rangle \equiv \langle -1 \rangle \bmod \mathfrak{p}$. Then $J_0 \subset \mathfrak{p}$ by Corollary 1.4. Now if $\mathfrak{p}$ is minimal, this implies $J_0 = \mathfrak{p}$, contrary to

(ii). If $\mathfrak{p}$ is not minimal, then it is maximal and $G(F)/\mathfrak{p} \cong \boldsymbol{Z}/p\boldsymbol{Z}$ for a prime number p (Proposition 1.1). Then $p\langle 1\rangle \in \mathfrak{p}$ and so $J_p = (p\langle 1\rangle) + J_0 \subset \mathfrak{p}$ (here and below $(p\langle 1\rangle)$ denotes the principal ideal generated by $p\langle 1\rangle$). Since J_p is maximal, this gives $J_p = \mathfrak{p}$, contrary to (ii). Thus (1.6.4) has been established. Now we can prove (1.6.3). Take $a, b \in P$. Then $a+b \neq 0$ since otherwise $\langle a, b\rangle = \langle 1, -1\rangle$, whence $\langle 1, 1\rangle \equiv \langle a, b\rangle \equiv \langle 1, -1\rangle \bmod \mathfrak{p}$, contrary to (1.6.4). Hence $a+b = c \neq 0$ and $\langle a, b\rangle = \langle c, abc\rangle$. We have $\langle 1, 1\rangle \equiv \langle a, b\rangle \equiv \langle c, abc\rangle \equiv \langle c, c\rangle \equiv \langle c\rangle \cdot \langle 1, 1\rangle \bmod \mathfrak{p}$. Now if $\langle c\rangle \not\equiv \langle 1\rangle \bmod \mathfrak{p}$, then $\langle c\rangle \equiv -\langle 1\rangle \bmod \mathfrak{p}$ (see the proof of Proposition 1.1) and so $4\langle 1\rangle \equiv 0 \bmod \mathfrak{p}$. But $4\langle 1\rangle = \langle 1, 1\rangle \cdot \langle 1, 1\rangle$, so that $\langle 1, 1\rangle \equiv 0 \bmod \mathfrak{p}$. This gives $\langle 1\rangle \equiv -\langle 1\rangle \bmod \mathfrak{p}$. On the other hand, by (1.6.4) we must have $\langle -1\rangle \equiv -\langle 1\rangle \bmod \mathfrak{p}$. Putting the two congruences together we obtain $\langle 1\rangle \equiv \langle -1\rangle \bmod \mathfrak{p}$, contrary to (1.6.4). Thus $\langle c\rangle \equiv -\langle 1\rangle \bmod \mathfrak{p}$ is impossible, so we get $\langle c\rangle \equiv \langle 1\rangle \bmod \mathfrak{p}$ and $a+b = c \in P$, as desired. This proves that P is an ordering on F and that F is a real field. Thus (ii) is proved.

(iii) Since $\mathfrak{p}$ is minimal and $\operatorname{Ker}\sigma_P$ is a prime ideal, it is sufficient to prove that $\operatorname{Ker}\sigma_P \subset \mathfrak{p}$. If $a \in P$, then $\langle 1\rangle - \langle a\rangle \in \mathfrak{p}$, by the definition of P. Because of (1.6.4), we have $\langle 1\rangle \equiv -\langle -1\rangle \bmod \mathfrak{p}$, so that $\langle 1, -1\rangle \in \mathfrak{p}$. Thus $\mathfrak{p}$ contains all the generators of $\operatorname{Ker}\sigma_P$ (Proposition 1.5) and so $\operatorname{Ker}\sigma_P \subset \mathfrak{p}$.

(iv) If $\mathfrak{p}$ is a non-minimal prime ideal, then $G(F)/\mathfrak{p} \cong \boldsymbol{Z}/p\boldsymbol{Z}$ for a suitable prime number p (Proposition 1.1). Since $\mathfrak{p} \neq J_p$ and $\mathfrak{p} \neq J_0$, the set P defined in (ii) constitutes an ordering of F and as in (iii) we check that $\operatorname{Ker}\sigma_P \subset \mathfrak{p}$. But here equality is impossible, since $\operatorname{Ker}\sigma_P$ is a minimal prime ideal, while $\mathfrak{p}$ is not. From the above isomorphism we conclude that $p\langle 1\rangle \in \mathfrak{p}$, and so $(p\langle 1\rangle) + \operatorname{Ker}\sigma_P \subset \mathfrak{p}$. We shall prove that $T = (p\langle 1\rangle) + \operatorname{Ker}\sigma_P$ is the maximal ideal $\mathfrak{p}_p = \{A \in G(F)\colon \sigma_P(A) \equiv 0 \bmod p\}$, which will prove that $\mathfrak{p} = \mathfrak{p}_p$, as required in (iv). First note the trivial inclusion $T \subset \mathfrak{p}_p$. On the other hand, if $A \in \mathfrak{p}_p$ and $\sigma_P(A) = np$, then $\sigma_P(A - np\langle 1\rangle) = 0$, i.e., $A - np\langle 1\rangle \in \operatorname{Ker}\sigma_P$, $A \in T$. Thus $\mathfrak{p}_p \subset T$ and Theorem 1.6 is completely proved.

Corollary 1.7. *Denote by $X = X(F)$ the family of all orderings on the field F and by $Y = Y(F)$ the family of all minimal prime ideals of $G(F)$ different from J_0. Then the mapping $\varkappa\colon X \to Y$ defined by $\varkappa(P) = \operatorname{Ker}\sigma_P$ is bijective.*

Proof. We only need to prove the injectivity of $\varkappa$. If $P, P' \in X$ and $P \neq P'$, then there exists an a in P which does not belong to P'. Then $\langle 1\rangle - \langle a\rangle \in \operatorname{Ker}\sigma_P$ and $\langle 1\rangle - \langle a\rangle \notin \operatorname{Ker}\sigma_{P'}$, so that $\varkappa(P) \neq \varkappa(P')$.

Corollary 1.8. *For any ordering P on F, the ideals*

$$\mathfrak{p}_2 = \mathfrak{p}_2(P) = \{A \in G(F)\colon \sigma_P(A) \equiv 0 \bmod 2\}$$

and

$$J_2 = J_2(F) = \{A \in G(F) : \dim A \equiv 0 \bmod 2\}$$

coincide.

In other words, J_2 is the unique ideal in $G(F)$ which has index two.

Proof. For $A \in G(F)$, if $\sigma_P(A)$ is even, then necessarily $\dim A$ is even, hence $\mathfrak{p}_2 \subset J_2$. By the maximality of $\mathfrak{p}_2$, we have $\mathfrak{p}_2 = J_2$. If an ideal has index 2 in $G(F)$, then it is necessarily maximal, hence, by Theorem 1.6, the ideal coincides with J_2 or with $\mathfrak{p}_2(P)$ for an ordering P. By the first statement, the ideal equals to J_2.

§ 2. Elements of special types. In this section we use the results of § 1 to determine completely nilpotents, units, torsion elements, divisors of zero and idempotents of the Grothendieck ring $G(F)$, for any field F.

Let $X = X(F)$ be the family of all orderings of the field F and denote by $\mathbf{Z}^X$ the direct product of $|X|$ copies of the ring $\mathbf{Z}$ of integers. If F is a non-real field, so that X is empty, $\mathbf{Z}^X$ denotes the zero ring. We shall use the total signature σ on the ring $G(F)$, which is the homomorphism

$$\sigma = \prod_{P \in X} \sigma_P : G(F) \to \mathbf{Z}^X .$$

First we characterize the nil-radical $\mathcal{N}$ of $G(F)$. This is the ideal consisting of all nilpotent elements of the ring.

THEOREM 2.1. *For any field F, the nil-radical $\mathcal{N}$ of the ring $G(F)$ is precisely equal to the kernel of the homomorphism*

$$(\dim, \sigma) : G(F) \to \mathbf{Z} \times \mathbf{Z}^X .$$

In other words, $A \in G(F)$ is nilpotent if and only if $\dim A = 0$ and $\sigma_P(A) = 0$ for every ordering P on F (if there are any). In particular, if F is non-real, $\mathcal{N} = J_0$.

Proof. $\mathcal{N}$ is known to be the intersection of all prime ideals of the ring, or of all minimal prime ideals. Hence, by Theorem 1.6,

$$\mathcal{N} = J_0 \cap \bigcap_P \operatorname{Ker} \sigma_P . \tag{2.1.1}$$

But the intersection on the right clearly coincides with the kernel of $(\dim, \sigma)$. Thus $\mathcal{N} = \operatorname{Ker}(\dim, \sigma)$. ∎

THEOREM 2.2. *For any field F, the element $A \in G(F)$ is a unit in the ring $G(F)$ if and only if $(\dim, \sigma)(A)$ is a unit in $\mathbf{Z} \times \mathbf{Z}^X$. In other words, A is a unit if and only if $\dim A = \pm 1$ and $\sigma_P(A) = \pm 1$ for every ordering P on F (if there are any).*

Proof. Suppose $(\dim, \sigma)(A)$ is a unit. Then $(\dim, \sigma)(A^2) = 1$. Hence by Theorem 2.1, $A^2 \equiv \langle 1 \rangle \bmod \mathcal{N}$, from which it follows easily that

A is a unit (from $(A^2-\langle 1\rangle)^n = 0$ one obtains a $B \in G(F)$ such that $A \cdot B = \langle 1\rangle$). Conversely, if A is a unit, then obviously $(\dim, \sigma)(A)$ is a unit, too. ■

THEOREM 2.3. *For any real field F, the torsion ideal $G_t(F)$ of $G(F)$ is precisely equal to the kernel of the homomorphism*

$$(\dim, \sigma)\colon G(F) \to \mathbf{Z} \times \mathbf{Z}^X.$$

The order of every torsion element of $G(F)$ is a power of 2.

Proof. The proof of Satz 2 in the paper [18] of Lorenz and Leicht works *mutatis mutandis* in the case of the Grothendieck ring (the argument is repeated in Milnor–Husemoller [21], pp. 69–71). The lemma used there is to be replaced by the statement (2.3.1) below and then the only fact needed for the proof and not stated explicitly here is the following: if $G(F)$ possesses non-zero nilpotents, then $q = |g(F)| \geqslant 4$. This can be checked in the following way. If $q = 2$ and F is real, then F has only one ordering P and $\operatorname{Ker}\sigma_P$ is generated by $\langle 1, -1\rangle$ (cf. Proposition 1.5). Thus $\mathcal{N} = J_0 \cap \operatorname{Ker}\sigma_P = 0$. It remains to state the substitute for the above mentioned lemma. Suppose $K = F(\sqrt{d})$ is a quadratic extension of F. Consider the canonical homomorphism $h\colon G(F) \to G(K)$. We assert

(2.3.1) $\operatorname{Ker} h$ *coincides with the principal ideal generated by* $\langle 1\rangle - \langle d\rangle$.

The lemma of Lorenz and Leicht states that the kernel of the canonical homomorphism $h^*\colon W(F) \to W(K)$ is the principal ideal generated by the form $(1, -d)$. Since the diagram

$$\begin{array}{ccc} G(F) & \xrightarrow{\ h\ } & G(K) \\ \downarrow & & \downarrow \\ W(F) & \xrightarrow{\ h^*\ } & W(K) \end{array}$$

commutes, for any $A \in \operatorname{Ker} h$ and its image A' in $W(F)$, we have $A' = \langle 1, -d\rangle \cdot \langle \varphi\rangle$, for a form φ over F. Thus $A = (\langle 1\rangle - \langle d\rangle)\cdot\langle\varphi\rangle + m\langle 1, -1\rangle$, where m is an integer, and since $A \in \operatorname{Ker} h$ implies $\dim A = 0$, we get $m = 0$ and A belongs to the ideal generated by $\langle 1\rangle - \langle d\rangle$. Thus one inclusion is proved and the other is trivial. ■

THEOREM 2.4. *For any non-real field F, the torsion ideal $G_t(F)$ of $G(F)$ is precisely equal to the kernel of the dimension homomorphism* dim: $G(F) \to \mathbf{Z}$, *that is,* $G_t(F) = J_0$.

The order of every torsion element of $G(F)$ is a power of 2.

Proof. We know from Theorem 2.1 that $J_0 = \mathcal{N}$, hence for any $a \in F^*$ there exists a positive integer n such that $(\langle 1\rangle - \langle a\rangle)^n = 0$. By the binomial theorem, $(\langle 1\rangle - \langle a\rangle)^n = 2^{n-1}(\langle 1\rangle - \langle a\rangle)$. Hence every generator

of J_0 is torsion and so $J_0 \subset G_t(F)$. On the other hand, $nA = 0$ implies $\dim A = 0$, hence $G_t(F) \subset J_0$. Since the additive generators of J_0 have 2-power orders, every torsion element of $G(F)$ has a 2-power order. ∎

COROLLARY 2.5. *For any field F, $G_t(F) = \mathcal{N}$, that is, $A \in G(F)$ is torsion if and only if A is nilpotent. Also $G_t(F)$ is the intersection of all minimal prime ideals of $G(F)$.*

COROLLARY 2.6 (Pfister's Local-Global Principle). *For each ordering P on the real field F, denote by F_P a real closed field containing F and inducing the ordering P on F. Let $j_P\colon G(F) \to G(F_P)$ be the canonical homomorphism. Then the following sequence is exact:*

$$0 \to G_t(F) \to G(F) \xrightarrow{\Pi j_P} \prod G(F_P). \tag{2.6.1}$$

In other words, $A \in G(F)$ is torsion if and only if $j_P(A) = 0$ for every ordering P on F.

Proof. Over a real closed field F_P dimension and signature classify quadratic forms. Hence, for A in $G(F)$,

$$\begin{aligned} A \in \operatorname{Ker} j_P &\Leftrightarrow \dim A = 0 \text{ and } \sigma_P(A) = 0 \\ &\Leftrightarrow A \in J_0 \cap \operatorname{Ker} \sigma_P. \end{aligned}$$

Thus

$$\begin{aligned} G_t(F) = \mathcal{N} &= J_0 \cap \bigcap_P \operatorname{Ker} \sigma_P \quad \text{(by Theorem 2.1)} \\ &= \operatorname{Ker} \prod_P j_P, \end{aligned}$$

which establishes the exactness of the sequence (2.6.1). ∎

Now we describe completely the divisors of zero in $G(F)$.

THEOREM 2.7. *Let $\mathcal{D}$ be the set of all divisors of zero in $G(F)$.*

(i) *If the field F is not pythagorean, then $\mathcal{D} = J_2$, i.e., $\mathcal{D}$ coincides with the ideal of all even-dimensional elements of $G(F)$.*

(ii) *If the field F is pythagorean, then $\mathcal{D} = J_0 \cup \bigcup_P \operatorname{Ker} \sigma_P$, i.e., $\mathcal{D}$ is the union of all minimal prime ideals of $G(F)$. In this case, $\mathcal{D} \subset J_2$.*

Proof. It is known that in any commutative ring R the set $\mathcal{D}$ of zero divisors is the union of a certain family of prime ideals in R (cf. Lorenz [17], 11.10 or Lam [15], p. 249), and moreover, that the minimal prime ideals necessarily occur in the family. In the case $R = G(F)$ the latter can be proved directly as follows.

We have the identity

$$(\langle 1\rangle - \langle a\rangle)\langle 1, a\rangle = 0 \quad \text{for} \quad a \in F^*. \tag{2.7.1}$$

The minimal prime ideal J_0 is additively generated by all the elements $\langle 1\rangle - \langle a\rangle$, $a \in F^*$ (Proposition 1.3), hence the identity

$$\sum \pm(\langle 1\rangle - \langle a_i\rangle) \prod \langle 1, a_i\rangle = 0,$$

which is a simple consequence of (2.7.1), implies that $J_0 \subset \mathscr{D}$. Similarly if $\mathfrak{p} = \operatorname{Ker}\sigma_P$ is any other minimal prime ideal, then it is generated additively by $\langle 1, -1\rangle$ and the elements $\langle 1\rangle - \langle a\rangle$, $a \in P$. But from (2.7.1) we obtain

$$\left[n\langle 1, -1\rangle + \sum \pm(\langle 1\rangle - \langle a_i\rangle)\right] \cdot (\langle 1\rangle - \langle -1\rangle) \prod \langle 1, a_i\rangle = 0,$$

where the second factor is $\neq 0$, since its signature is a power of 2. Hence $\mathfrak{p} \subset \mathscr{D}$ and we have proved that

$$J_0 \cup \bigcup_P \operatorname{Ker}\sigma_P \subset \mathscr{D}. \tag{2.7.2}$$

Now we shall prove the following: if $\mathfrak{p}$ is a prime ideal in $G(F)$ and the index $[G(F)\colon \mathfrak{p}]$ is finite and odd, then $\mathfrak{p}$ is not contained in $\mathscr{D}$. For any such prime ideal $\mathfrak{p}$ is in fact maximal and the index $[G(F)\colon \mathfrak{p}] = p$, where p is a prime number $\neq 2$. Then $p\langle 1\rangle \equiv 0 \bmod \mathfrak{p}$ and if $\mathfrak{p} \subset \mathscr{D}$, then there exists $A \in G(F)$, $A \neq 0$, such that $pA = p\langle 1\rangle \cdot A = 0$, that is, there is an odd torsion in $G(F)$, contrary to Theorems 2.3 and 2.4. Now Theorem 1.6 and Corollary 1.8 imply that $\mathscr{D}$, being the union of prime ideals, must be equal either to the union of all minimal prime ideals or to the union of J_2 and all minimal prime ideals.

If J_2 is going to occur in the union, then $\langle 1, 1\rangle \in J_2$ is a divisor of zero, hence $2A = 0$ for an $A \neq 0$. This cannot happen if F is pythagorean (cf. [29], Proposition 1.19) and so (ii) is proved.

If F is not pythagorean, there is a non-trivial torsion in $G(F)$, hence $2A = 0$ for an $A \neq 0$, hence $\langle 1, 1\rangle \in \mathscr{D}$. But $\langle 1, 1\rangle$ does not belong to any of the minimal prime ideals (its dimension and signatures are always 2), hence another ideal must occur in the union and by the above, it is J_2. Since J_2 contains all the minimal prime ideals, we have $\mathscr{D} = J_2$ which proves (i) and the theorem.

THEOREM 2.8. *For any field F, the only idempotents of $G(F)$ are 0 and $\langle 1\rangle$.*

Proof. Assume $E \in G(F)$ is an idempotent different from 0 and $\langle 1\rangle$. Then $E' = \langle 1\rangle - E$ is also an idempotent different from 0 and $\langle 1\rangle$ and we have $E \cdot E' = 0$, that is, E and E' are divisors of zero in $G(F)$. By Theorem 2.7, E and E' belong to J_2, and so also $\langle 1\rangle = E + E' \in J_2$, a contradiction. This proves Theorem 2.8.

We end this section with two further results concerning the nil-radical $\mathscr{N}$ of the Grothendieck ring. First we determine a set of generators

for $\mathcal{N}$ and then we show that the nil-radical of $G(F)$ coincides with the Jacobson radical of the ring (the intersection of all maximal ideals of the ring).

THEOREM 2.9. *Let* $S = \bigcap_{P \in X} P$ *be the set of all totally positive elements of the real field* F *and* $T = \{\langle 1\rangle - \langle a\rangle \in G(F) : a \in S\}$. *Then the nil-radical* $\mathcal{N}$ *of* $G(F)$ *is generated by* T, *i.e.*, $\mathcal{N} = (T)$.

Proof. It is easy to see that $(T) \subset \mathcal{N}$. Indeed, from Propositions 1.3 (i) and 1.5 (ii) it follows that for any $a \in S$, $\langle 1\rangle - \langle a\rangle$ belongs to every minimal prime ideal of $G(F)$, hence to their intersection known to be $\mathcal{N}$. Thus $(T) \subset \mathcal{N}$.

The proof of the converse inclusion is much harder and we shall supply a proof by modifying Pfister's argument used in the proof of Satz 22 of his Habilitationsschrift [23].

Let us assume that $C \in \mathcal{N}$. Then C is nilpotent, hence $\dim C = 0$ and C can be written in the form $C = A - B$, where A and B are equivalence classes of equal dimension. We induct on $r = \dim A = \dim B$. If $r = 1$, then $C = \langle a\rangle - \langle b\rangle$ and since C is nilpotent, we have $\sigma_P(C) = 0$ at every ordering P of F. Hence $\operatorname{sgn}_P a = \operatorname{sgn}_P b$ at every ordering P, and so $ab \in S$, and further,

$$C = \langle a\rangle(\langle 1\rangle - \langle ab\rangle) \in (T).$$

Now assume that $r > 1$. We know that $\mathcal{N} = G_t(F)$ (Corollary 2.5), hence C is torsion and $2^n C = 0$ for a certain $n > 0$. Choose some diagonalizations for A and B, $A = \langle a_1, \ldots, a_r\rangle$, $B = \langle b_1, \ldots, b_r\rangle$, say. Since $2^n A = 2^n B$, the class $2^n A$ represents b_1, that is

$$b_1 = a_1 c_1 + \ldots + a_t c_t, \quad 1 \leqslant t \leqslant r, \tag{2.9.1}$$

where $0 \neq c_i \in D_F(2^n\langle 1\rangle)$. We rearrange the $a_1, \ldots, a_r$, if necessary, to obtain in (2.9.1) the number of summands minimal. Now we proceed by induction on t. If $t = 1$, $b_1 = a_1 c_1$, where $c_1 \in S$ (any sum of squares is totally positive), hence

$$C = A - B = \langle a_1\rangle(\langle 1\rangle - \langle c_1\rangle) + A' - B', \tag{2.9.2}$$

where $\dim A' = \dim B' = r-1$ and $C' = A' - B' \in \mathcal{N}$, since $\langle 1\rangle - \langle c_1\rangle \in T \subset \mathcal{N}$. Thus the induction on r applies and we get $C' \in (T)$ and so (2.9.2) yields $C \in (T)$.

Now suppose $t > 1$. Put $a_2 c_2 + \ldots + a_t c_t = b_1'$ so that

$$b_1 = a_1 c_1 + b_1'.$$

Hence

$$0 = (b_1 - a_1 c_1 - b_1') a_1 c_1 b_1',$$

and it follows that $(a_1b_1c_1b_1', -b_1', -a_1c_1)$ is isotropic. Put $a_1' = a_1b_1c_1b_1'$; then

$$\langle a_1', -b_1', -a_1c_1\rangle = \langle 1, -1, -b_1\rangle,$$

or else,

$$\langle -a_1', b_1', a_1c_1\rangle = \langle 1, -1, b_1\rangle.$$

Hence

$$\begin{aligned} C &= A-B = \langle 1, -1, a_1, \ldots, a_r\rangle - \langle -a_1', b_1', a_1c_1, b_2, \ldots, b_r\rangle \\ &= \langle a_1\rangle(\langle 1\rangle - \langle c_1\rangle) + \langle a_1', -a_1', a_2, \ldots, a_r\rangle - \langle -a_1', b_1', b_2, \ldots, b_r\rangle \\ &= \langle a_1\rangle(\langle 1\rangle - \langle c_1\rangle) + \langle a_1', a_2, \ldots, a_r\rangle - \langle b_1', b_2, \ldots, b_r\rangle. \end{aligned}$$

Put

$$A'' = \langle a_1', a_2, \ldots, a_r\rangle, \quad B'' = \langle b_1', b_2, \ldots, b_r\rangle.$$

We recall that $2^nC = 0$ and also $2^n(\langle 1\rangle - \langle c_1\rangle) = 0$, since $c_1 \in D_F(2^n\langle 1\rangle)$. Hence the above representation of C implies

$$2^n(A''-B'') = 0,$$

i.e., $A''-B'' \in G_t(F) = \mathcal{N}$. But here $b_1' = a_2c_2 + \ldots + a_tc_t$, that is, a shorter expression than (2.9.1). Thus the induction on t applies and yields $A''-B'' \in (T)$, whence $C = \langle a_1\rangle(\langle 1\rangle - \langle c_1\rangle) + A''-B'' \in (T)$ and the theorem is proved.

Remark 2.10. The above proof makes it clear that T generates $\mathcal{N}$ as an ideal and not as an abelian group.

Proposition 2.11. *For any field F, the Jacobson radical of $G(F)$ coincides with the nil-radical of $G(F)$.*

Proof. If F is a non-real field, then from Theorem 1.6(i) we know that the Jacobson radical $\mathcal{R}$ is equal to $\bigcap_p J_p$. Thus if $A \in \mathcal{R}$, $\dim A$ is divisible by each prime number p, hence $\dim A = 0$ and $A \in J_0$. Conversely, $J_0 \subset J_p$, for every prime number p, hence $\mathcal{R} = J_0 = \mathcal{N}$, by Theorem 2.1.

If F is a real field and $A \in \mathcal{R}$, then $\dim A$ and $\sigma_P(A)$ are divisible by every prime number, hence they are both zero (for every ordering P), hence by Theorem 2.1, $A \in \mathcal{N}$, hence $\mathcal{R} \subset \mathcal{N}$. This argument reverses and so we get $\mathcal{R} = \mathcal{N}$.

§ 3. Local properties of $G(F)$. Let $\mathfrak{p}$ be a prime ideal in $G(F)$ and denote by $G(F)_{\mathfrak{p}}$ the localization of $G(F)$ at $\mathfrak{p}$, i.e., the ring of fractions with respect to the multiplicative system $S_{\mathfrak{p}} = G(F)\setminus\mathfrak{p}$.

Let $f_{\mathfrak{p}}: G(F) \to G(F)_{\mathfrak{p}}$ be the canonical homomorphism defined by $f_{\mathfrak{p}}(x) = x/1$. Recall that $x/1 = y/1$ if and only if there exists an $a \in S_{\mathfrak{p}}$ such that $a(x-y) = 0$ in $G(F)$.

In this section we give some characterizations of the elements of $G(F)$ considered in § 2 by using their behaviour under localization. Let us begin with the following theorem.

THEOREM 3.1. *For any field F, the following statements are equivalent.*

(i) $A \in G(F)$ *is torsion.*

(ii) $f_{\mathfrak{p}}(A) \in G(F)_{\mathfrak{p}}$ *is torsion, for every prime ideal* $\mathfrak{p}$ *of* $G(F)$.

(iii) $f_{\mathfrak{p}}(A) \in G(F)_{\mathfrak{p}}$ *is torsion, for every minimal prime ideal* $\mathfrak{p}$ *of* $G(F)$.

Proof. Obviously, (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii). So assume (iii). Then for every minimal prime ideal $\mathfrak{p}$ there exists a positive integer $n_{\mathfrak{p}}$ such that $n_{\mathfrak{p}} \cdot A/1 = 0$ in $G(F)_{\mathfrak{p}}$, that is, there exists $B_{\mathfrak{p}} \in S_{\mathfrak{p}}$ such that $n_{\mathfrak{p}} A \cdot B_{\mathfrak{p}} = 0$ in $G(F)$. Thus $A \cdot B_{\mathfrak{p}}$ is torsion in $G(F)$ and by Corollary 2.5 we have $A \cdot B_{\mathfrak{p}} \in \mathfrak{p}$, whence $A \in \mathfrak{p}$. Thus A is in the intersection of all minimal prime ideals of $G(F)$ and by Corollary 2.5, A is torsion. Hence (iii) $\Rightarrow$ (i), which proves the theorem.

The next theorem can be proved similarly.

THEOREM 3.2. *For any field F, the following statements are equivalent.*

(i) $A \in G(F)$ *is nilpotent.*

(ii) $f_{\mathfrak{p}}(A) \in G(F)_{\mathfrak{p}}$ *is nilpotent, for every prime ideal* $\mathfrak{p}$ *of* $G(F)$.

(iii) $f_{\mathfrak{p}}(A) \in G(F)_{\mathfrak{p}}$ *is nilpotent, for every minimal prime ideal* $\mathfrak{p}$ *of* $G(F)$.

Now consider the units of $G(F)$.

THEOREM 3.3. *For any field F, the following statements are equivalent.*

(i) $A \in G(F)$ *is a unit.*

(ii) $f_{\mathfrak{p}}(A) \in G(F)_{\mathfrak{p}}$ *is a unit for every prime ideal* $\mathfrak{p}$ *of* $G(F)$.

(iii) $f_{\mathfrak{p}}(A) \in G(F)_{\mathfrak{p}}$ *is a unit for every maximal ideal* $\mathfrak{p}$ *of* $G(F)$.

Proof. Obviously, (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii). Assume (iii). Then A does not belong to any maximal ideal of $G(F)$. Hence, by Theorem 1.6, $\dim A \not\equiv 0 \bmod p$, for every prime number p, and if F is real, $\sigma_P(A) \not\equiv 0 \bmod p$, for any ordering P of F and every prime number p. Thus $\dim A = \pm 1$ and $\sigma_P(A) = \pm 1$ for every ordering P of F, an so, by Theorem 2.2, A is a unit in $G(F)$, which proves the theorem.

Remark 3.4. If $f_{\mathfrak{p}}(A) \in G(F)_{\mathfrak{p}}$ is a unit for every minimal prime ideal $\mathfrak{p}$ of $G(F)$, then A need not be a unit in $G(F)$. For example, if $F = \boldsymbol{R}$, the field of real numbers, we have just two minimal prime ideals in $G(\boldsymbol{R})$, namely, J_0 and $\operatorname{Ker}\sigma$. Now, $A = \langle 1, 1\rangle$ does not belong to any of them and so its images in the corresponding local rings are units. But obviously A is not a unit in $G(\boldsymbol{R})$.

THEOREM 3.5. *For any field F, the following statements are equivalent.*

(i) $A \in G(F)$ *is a divisor of zero.*

(ii) *There exists a prime ideal* $\mathfrak{p}$ *in* $G(F)$ *such that* $f_{\mathfrak{p}}(A)$ *is a divisor of zero in* $G(F)_{\mathfrak{p}}$.

Proof. Assume (i). We choose $\mathfrak{p}$ to be J_2, the ideal of even-dimensional

elements of $G(F)$. By Theorem 2.7, there exists a non-zero B in J_2 such that $A \cdot B = 0$. Then $f_{J_2}(A) \cdot f_{J_2}(B) = 0$ and $f_{J_2}(B) \neq 0$, since otherwise there exists $C \in G(F) \setminus J_2$ such that $B \cdot C = 0$, which is impossible (Theorem 2.7 implies $C \in J_2$). Thus we have (ii).

Conversely, assume (ii). Then there exist $B, C \in G(F)$ such that $A/1 \cdot B/C = 0$ and $B/C \neq 0$ in $G(F)_\mathfrak{p}$, that is, for every $D \in G(F) \setminus \mathfrak{p}$ we have $B \cdot D \neq 0$ in $G(F)$. Now, $A/1 \cdot B/C = 0$ implies that $ABD = 0$ for an element $D \in G(F) \setminus \mathfrak{p}$, and since $BD \neq 0$, we conclude that A is a divisor of zero in $G(F)$. ∎

Chapter III

Group structure of $G(F)$ and $W(F)$

§ 1. General decomposition theorems. In this chapter we are concerned with decompositions of the additive groups $G(F)$ and $W(F)$ into direct sums. The first section contains four general theorems of this kind and the second section provides decompositions of $G(F)$ and $W(F)$ into direct sums of cyclic groups for a number of classes of fields F with prescribed behaviour of binary forms. These results will be used in § 3 to obtain bounds for the rank of $G(F)$ and $W(F)$.

We begin with two results which arose from investigating decompositions of $G(F)$ of the type $G(F) = \mathbf{Z}\langle 1\rangle \oplus J$. One such decomposition with $J = J_0$ is well known to exist (cf. Scharlau [24], p. 30). We recall our notation: $J_0 = J_0(F)$ is the kernel of the dimension homomorphism and $\mathfrak{p}_0 = \mathfrak{p}_0(P, F)$ is the kernel of the signature homomorphism defined by the ordering P on F.

THEOREM 1.1 (First Decomposition Theorem, FDT).

(i) *For any field F, the Grothendieck group $G(F)$ has the following decompositions into the direct sum of subgroups:*

$$G(F) = \mathbf{Z}\langle 1\rangle \oplus J_0(F) = \mathbf{Z}\langle 1\rangle \oplus \mathfrak{p}_0(P, F),$$

where P is an arbitrary ordering of F (if there are any).

(ii) *$J_0(F)$ is the subgroup generated by the set $\{\langle 1\rangle - \langle a\rangle : a \in F^*\}$. $\mathfrak{p}_0(P, F)$ is the subgroup generated by the set $\{\langle 1, -1\rangle, \langle 1\rangle - \langle a\rangle : a \in P\}$.*

(iii) *The intersection of all direct summands of $G(F)$ which are complementary to the subgroup $\mathbf{Z}\langle 1\rangle$ is equal to the torsion subgroup $G_t(F)$ of $G(F)$. In particular, for a non-real field F, $J_0(F) = G_t(F)$ is the unique direct summand of $G(F)$ complementary to $\mathbf{Z}\langle 1\rangle$.*

In the next theorem, $[1]$ denotes the identity element of the Witt ring and $f\colon G(F) \to W(F)$ is the canonical surjection. Recall that f restricted to $J_0(F)$ is injective, so that in the theorem below the groups U_0 and fU_0 are isomorphic.

THEOREM 1.2 (Second Decomposition Theorem, SDT).

(i) *For any field F, the element $\langle 1\rangle - \langle -1\rangle$ of $G(F)$ generates a direct*

summand E in the group $J_0(F)$. If F is non-real with the stufe s, the order of E is s. If F is real, E is infinite.

(ii) *For a non-real field F with the stufe s, there exists a subgroup U_0 of $J_0(F)$ such that $2sU_0 = 0$ and*

$$G(F) = \mathbf{Z}\langle 1\rangle \oplus \mathbf{Z}/s\mathbf{Z}(\langle 1\rangle - \langle -1\rangle) \oplus U_0,$$

and

$$W(F) = \mathbf{Z}/2s\mathbf{Z}[1] \oplus fU_0.$$

(iii) *For a real field F, we put $U_0(P) = J_0(F) \cap \mathfrak{p}_0(P, F)$, for each ordering P of F. Then the subgroup $U_0(P)$ is generated by the set $\{\langle 1\rangle - \langle a\rangle : a \in P\}$ and*

$$G(F) = \mathbf{Z}\langle 1\rangle \oplus \mathbf{Z}(\langle 1\rangle - \langle -1\rangle) \oplus U_0(P) = \mathbf{Z}\langle 1\rangle \oplus \mathbf{Z}\langle 1, -1\rangle \oplus U_0(P),$$

and

$$W(F) = \mathbf{Z}[1] \oplus fU_0(P).$$

(iv) *For a real field F, the intersection of all direct summands of $G(F)$ which are complementary to the subgroup $S(F) = \mathbf{Z}\langle 1\rangle \oplus \mathbf{Z}(\langle 1\rangle - \langle -1\rangle) = \mathbf{Z}\langle 1\rangle \oplus \mathbf{Z}\langle 1, -1\rangle$ is equal to $G_t(F)$. In particular, for a field F with exactly one ordering, the torsion subgroup $G_t(F)$ is the unique direct summand complementary to $S(F)$.*

Moreover, for any real field F, the intersection of all direct summands of $W(F)$ which are complementary to $\mathbf{Z}[1]$, is equal to $W_t(F)$, the torsion subgroup of $W(F)$.

Proof of Theorem 1.1. (i) The first decomposition is well known. The second one can be obtained analogously. Namely, the exact sequence

$$0 \to \mathfrak{p}_0(P, F) \to G(F) \xrightarrow{\sigma_P} \mathbf{Z} \to 0$$

is split by the homomorphism $\mathbf{Z} \to G(F)$ defined by $1 \mapsto \langle 1\rangle$. Thus $G(F) = \mathbf{Z}\langle 1\rangle \oplus \mathfrak{p}_0(P, F)$ (cf. Lang [16], p. 83). This proves (i).

(ii) This is proved in Chapter II, Propositions 1.3 and 1.5.

(iii) By a theorem of G. Grätzer and E. T. Schmidt (cf. Fuchs [8], Theorem II.9.6) the intersection $\mathscr{C}$ of all direct summands of $G(F)$ which are complementary to $\mathbf{Z}\langle 1\rangle$ is a maximal fully invariant subgroup of $G(F)$ disjoint with $\mathbf{Z}\langle 1\rangle$ (fully invariant means invariant under every group endomorphism). By (i), we know that $J_0(F) \cap \bigcap \mathfrak{p}_0(P, F) \supseteq \mathscr{C}$, and by (II.2.1.1) and Corollary II.2.5, we obtain $G_t(F) \supseteq \mathscr{C}$. But $G_t(F)$ is certainly a fully invariant subgroup and it is disjoint with $\mathbf{Z}\langle 1\rangle$, hence, by the maximality of $\mathscr{C}$, we have $G_t(F) = \mathscr{C}$, as required. If F is non-real, $\mathscr{C} = G_t(F) = J_0(F)$, by Theorem II.2.4, so $\mathscr{C}$ is itself a direct summand complementary to $\mathbf{Z}\langle 1\rangle$. Clearly, this implies the uniqueness statement of (iii). ∎

Remarks. (1.1.1) At the Oberwolfach conference on quadratic forms in April 1975 Professor M. Kneser pointed out that in the above proof one can avoid the use of Grätzer–Schmidt theorem. We obtain $G_t(F) \supset \mathscr{C}$ as above and to prove the converse inclusion one considers any decomposition $G(F) = \boldsymbol{Z}\langle 1\rangle \oplus U$ and the projection p onto the first summand. Certainly $p\big(G_t(F)\big)$ is the torsion subgroup of $\boldsymbol{Z}\langle 1\rangle$, hence $p\big(G_t(F)\big) = 0$. Thus $G_t(F) \subset \mathrm{Ker}\, p = U$ and consequently $G_t(F) \subset \mathscr{C}$.

(1.1.2) One might hope to improve on the statement (iii) by saying that in the case of a real field F, the subgroups $J_0(F)$ and $\mathrm{p}_0(P, F)$ are the only direct summands complementary to $\boldsymbol{Z}\langle 1\rangle$. Unfortunately, this fails to hold even in the simplest case of a real closed field (e.g., $\boldsymbol{R}$) as is witnessed by the decompositions

$$G(\boldsymbol{R}) = \boldsymbol{Z}\langle 1\rangle \oplus \boldsymbol{Z}(\langle 1\rangle - \langle -1\rangle) = \boldsymbol{Z}\langle 1\rangle \oplus \boldsymbol{Z}\langle 1, -1\rangle = \boldsymbol{Z}\langle 1\rangle \oplus \boldsymbol{Z}\langle -1\rangle.$$

However, see Theorem 1.2 (iv) for a corresponding uniqueness statement.

Proof of Theorem 1.2. (i) In the case of a real field F, this has been proved in [29], Lemma 1.10. The non-real case is harder and has been settled in [30]. We outline here this proof. Let s be the stufe of F, then $\langle 1\rangle - \langle -1\rangle$ is of order s, that is, the subgroup E is a cyclic 2-group. Now, by a theorem of T. Szele (cf. Fuchs [8], Proposition V.27.1), E is a direct summand of $J_0(F)$ if and only if

$$E \cap sJ_0(F) = 0. \tag{1.2.1}$$

The group $J_0(F)$ has exponent $2s$, hence $sJ_0(F)$ has exponent 2. If (1.2.1) fails to hold, then we must have

$$\tfrac{1}{2}s(\langle 1\rangle - \langle -1\rangle) = s\sum_{i=1}^{t}(\langle 1\rangle - \langle a_i\rangle), \tag{1.2.2}$$

for some $a_i \in F^*$, since $\frac{1}{2}s(\langle 1\rangle - \langle -1\rangle)$ is the only element of E of order 2. From (1.2.2) we obtain

$$s\langle a_1, \ldots, a_t\rangle = (t-1)s\langle 1\rangle + \tfrac{1}{2}s\langle 1, -1\rangle. \tag{1.2.3}$$

Now we show that (1.2.3) is impossible for any $a_1, \ldots, a_t \in F^*$. We induct on t. If $t = 1$, then (1.2.3) implies that $s\langle 1\rangle$ is isotropic, a contradiction. If $t = 2$, then from Remark I.3 we conclude that $s\langle a_1, a_2\rangle = s\langle 1, -1\rangle$ which put into (1.2.3) again implies that $s\langle 1\rangle$ is isotropic.

Assume that $t > 2$. Then $s\langle a_1, \ldots, a_t\rangle$ is isotropic and by Remark I.3 we obtain

$$s\langle a_1, \ldots, a_t\rangle = s\langle 1, -1\rangle + s\langle b_1, \ldots, b_{t-2}\rangle = 2s\langle 1\rangle + s\langle b_1, \ldots, b_{t-2}\rangle,$$

for some $b_1, \ldots, b_{t-2} \in F^*$. Substituting this into (1.2.3) we obtain

$$s\langle b_1, \ldots, b_{t-2}\rangle = (t-3)s\langle 1\rangle + \tfrac{1}{2}s\langle 1, -1\rangle,$$

which is impossible by the induction hypothesis. This finishes the proof of (i).

(ii) This is the first part of Theorem 4.1 in [30]. The decomposition of $G(F)$ follows directly from (i). Since $\mathbf{Z}\langle 1\rangle \oplus E$ contains $\mathbf{Z}\langle 1, -1\rangle = \mathrm{Ker} f$, the decomposition of $W(F)$ follows from that of $G(F)$ (for details, see the beginning of Section 3 in [29]).

(iii) The set $\{\langle 1\rangle - \langle a\rangle : a \in P\}$ is contained both in $J_0(F)$ and $\mathrm{p}_0(P, F)$, hence it is contained in their intersection $U_0(P)$. On the other hand, by Theorem 1.1(ii), every A in $\mathrm{p}_0(P, F)$ can be written in the form

$$A = n\langle 1, -1\rangle + \sum \pm(\langle 1\rangle - \langle a_i\rangle), \quad \text{where} \quad a_i \in P.$$

Here n is determined uniquely, since $\dim A = 2n$. Thus, if $A \in U_0(P)$, then $\dim A = 0$, i.e., $A = \sum \pm(\langle 1\rangle - \langle a_i\rangle)$, where $a_i \in P$. This proves that the set $\{\langle 1\rangle - \langle a\rangle : a \in P\}$ generates $U_0(P)$.

The two decompositions of $G(F)$ follow now from Lemma 1.10 in [29] and from the fact that $\mathbf{Z}\langle 1\rangle \oplus \mathbf{Z}(\langle 1\rangle - \langle -1\rangle) = \mathbf{Z}\langle 1\rangle \oplus \mathbf{Z}\langle 1, -1\rangle$. Since $\mathbf{Z}\langle 1, -1\rangle = \mathrm{Ker} f$, the last statement follows trivially from the decomposition $G(F) = \mathbf{Z}\langle 1\rangle \oplus \mathbf{Z}\langle 1, -1\rangle \oplus U_0(P)$.

(iv) Since $\bigcap_P U_0(P) = G_t(F)$, the argument used in the proof of 1.1(iii) applies and gives the first result stated in (iv). If F has just one ordering, then $U_0(P) = G_t(F)$, and so this is the unique direct summand complementary to $S(F)$. If $G(F) = S(F) \oplus U$, where U is a subgroup of $G(F)$, then the canonical surjection $f: G(F) \to W(F)$ restricted to U is injective (since $\mathbf{Z}\langle 1, -1\rangle = \mathrm{Ker} f \subset S(F)$). Hence any such decomposition of $G(F)$ implies the decomposition of $W(F)$, namely $W(F) = \mathbf{Z}[1] \oplus fU$. Denote by $\mathscr{D}$ the intersection of all direct summands of $W(F)$ which are complementary to $\mathbf{Z}[1]$. Then

$$\mathscr{D} \subset \bigcap fU = f(\bigcap U) \subset f(G_t(F)) \subset W_t(F),$$

where U runs through all the direct summands of $G(F)$ complementary to $S(F)$. Since $W_t(F)$ is fully invariant and disjoint with $\mathbf{Z}[1]$, this implies that $\mathscr{D} = W_t(F)$, as desired. ∎

We now present an application of the SDT (cf. [30], Theorem 4.2).

THEOREM 1.3. *Let K be a local field with residue class field F and assume that* $\mathrm{char} F \neq 2$. *Then*

$$G(K) \cong G(F) \oplus W(F) \quad \text{and} \quad W(K) \cong W(F) \oplus W(F).$$

Proof. The result concerning the Witt group is the well-known theorem of Springer [26]. We derive the result for $G(K)$ from Springer's theorem. Assume that K is a real field. Then also F is a real field and by SDT (iii) we have

$$\mathbf{Z} \oplus U_0(K) \cong W(K) \cong W(F) \oplus W(F) \cong \mathbf{Z} \oplus U_0(F) \oplus W(F),$$

where we have written $U_0(K)$ instead of $U_0(P)$, where P is an ordering on K, and similarly with F. Cancelling the summand $\boldsymbol{Z}$ (cf. Fuchs [8], Ex. III.15.24) we obtain

$$U_0(K) \cong U_0(F) \oplus W(F),$$

and again by SDT(ii),

$$G(K) \cong \boldsymbol{Z} \oplus \boldsymbol{Z} \oplus U_0(K) \cong \boldsymbol{Z} \oplus \boldsymbol{Z} \oplus U_0(F) \oplus W(F) \cong G(F) \oplus W(F).$$

If K is non-real, the proof runs analogously. ∎

Remark. W. Scharlau ([24], Theorem 4.2.1) proved that

$$G(K) \cong G(F)[t]/(t^2 = 1, t\langle 1, -1\rangle = \langle 1, -1\rangle) \quad \text{(ring isomorphism)}$$

and T. Y. Lam ([15], Theorem 1.4, p. 145) proved that

$$G(K) \cong G(F) \oplus G(F)/\boldsymbol{Z}(\langle 1, -1\rangle, -\langle 1, -1\rangle) \quad \text{(group isomorphism)}.$$

In order to obtain from these results the simpler form of Springer's theorem for $G(K)$ stated in Theorem 1.3, one has to know the location of the subgroup $\boldsymbol{Z}\langle 1, -1\rangle$ in the direct sum decomposition of $G(F)$, since otherwise it is impossible to clear out the "denominators" in the above presentations of $G(K)$. This information is supplied by the SDT (ii) and (iii), since $\langle 1, -1\rangle = 2\langle 1\rangle - (\langle 1\rangle - \langle -1\rangle)$ belongs to $\boldsymbol{Z}\langle 1\rangle \oplus E$, where E is generated by $\langle 1\rangle - \langle -1\rangle$.

The following theorem has been first explicitly stated by A. Sładek [25]. It is implicit in the paper of Knebusch–Rosenberg–Ware [12] and in two special cases it follows easily from the results of Elman and Lam ([5], Proposition 5.8 and Theorem 5.13).

THEOREM 1.4. *Let F be a real field with a finite number r of orderings. Then*

$$G(F) \cong \boldsymbol{Z}^{r+1} \oplus G_t(F) \quad \text{and} \quad W(F) \cong \boldsymbol{Z}^r \oplus W_t(F).$$

Moreover,

$$G_t(F) \cong W_t(F).$$

Proof. We give here a proof by modifying slightly the proof of Proposition 1.23 in [29]. By FDT, $G(F) \cong \boldsymbol{Z} \oplus J_0(F)$, so it is sufficient to prove that $J_0(F) \cong \boldsymbol{Z}^r \oplus G_t(F)$. First we want to prove that $J_0(F)$ contains at least r linearly independent elements of infinite order. Let T be the subgroup of totally positive elements of $g(F)$ and write $g(F) = S \times T$, where S is a subgroup of $g(F)$. Then S is finite (cf. Proposition 1.12 in [29]) and we choose a basis $\{-1, a_1, \ldots, a_n\}$ for S. For any ordering P on F we choose $\varepsilon_i = \pm 1$ satisfying $\varepsilon_i a_i \in P$, $i = 1, \ldots, n$, and put

$$A_P = (\langle 1\rangle - \langle -\varepsilon_1 a_1\rangle) \cdot \ldots \cdot (\langle 1\rangle - \langle -\varepsilon_n a_n\rangle).$$

Then $\sigma_P(A_P) = 2^n$. On the other hand, $\sigma_{P'}(A_P) = 0$ for any ordering $P' \neq P$. Thus $\sigma(A_{P_j}) = (\sigma_{P_1}(A_{P_j}), \ldots, \sigma_{P_r}(A_{P_j}))$, $j = 1, \ldots, r$, are linearly independent elements of $\boldsymbol{Z}^r$ and so $A_{P_1}, \ldots, A_{P_r}$ are linearly independent elements of $J_0(F)$.

Now we will use the Theorem II.2.3 re-stated in the following way: For any real field F, the group $G_t(F)$ is precisely equal to the kernel of the homomorphism $\sigma\colon J_0(F) \to \boldsymbol{Z}^X$, where σ denotes the total signature restricted to $J_0(F)$. In our case X is finite and $|X| = r$. Thus σ maps $J_0(F)$ into the free abelian group $\boldsymbol{Z}^r$ and by a standard theorem (cf. Lang [16], p. 44) we conclude that

$$J_0(F) \cong \operatorname{Im}\sigma \oplus \operatorname{Ker}\sigma.$$

By the above, $\operatorname{Im}\sigma \cong \boldsymbol{Z}^r$, and $\operatorname{Ker}\sigma = G_t(F)$, and we get the desired decomposition of $G(F)$. The other statements follow directly from what has just been proved and from SDT (iii).

§ 2. Value sets of binary forms and the group structure of $G(F)$ and $W(F)$. The structure of additive groups $G(F)$ and $W(F)$ depends strongly on the behaviour of binary quadratic forms over the field F. In this section we will demonstrate this assertion by decomposing the groups $G(F)$ and $W(F)$ into direct sums of cyclic groups in a number of cases where the binary forms over F have prescribed value sets. We begin with a well-known result.

THEOREM 2.1. *Let F be a field with the property that every binary form over F is universal. Then:*

(i) $G(F) \cong \boldsymbol{Z} \oplus g(F)$.

(ii) $W(F) \cong \boldsymbol{Z}/2\boldsymbol{Z} \oplus g(F)$, *if the stufe* $s(F) = 1$.

(iii) *If* $s(F) = 2$ *and* h *is any subgroup of* $g(F)$ *of index* 2, *then* $W(F) \cong \boldsymbol{Z}/4\boldsymbol{Z} \oplus h$.

(iv) *If* $\{a_i\colon i \in I\}$ *is any basis for* $g(F)$, *then* $\{\langle 1\rangle - \langle a_i\rangle\colon i \in I\}$ *is a basis for* $J_0(F)$.

Proof. (i) This result is due to Scharlau ([24], Theorem 4.1.1), see also [28], Theorems 2.1 and 2.2.

(ii) and (iii) have been proved by Cordes [2], Theorem 4.1. These statements follow easily from (i) and the SDT.

(iv) is proved in [29], Proposition 1.7. From (iv) and the SDT we obtain also a basis for the group $W(F)$.

THEOREM 2.2. *Let F be a real field with the basis $\{-1, a_i\colon i \in I\}$ for the group $g(F)$ and assume that all the binary forms $(1, a_i)$, $i \in I$, are universal. Then*

$$G(F) \cong \boldsymbol{Z} \oplus \boldsymbol{Z} \oplus (\boldsymbol{Z}/2\boldsymbol{Z})^{(I)} \quad \text{and} \quad W(F) \cong \boldsymbol{Z} \oplus (\boldsymbol{Z}/2\boldsymbol{Z})^{(I)}.$$

In the case of $G(F)$, the two infinite direct summands are generated by $\langle 1\rangle$ and $\langle 1\rangle - \langle -1\rangle$, respectively, and the remaining summands are generated by the elements $\langle 1\rangle - \langle -a_i\rangle$, $i \in I$.

Proof. This is proved in [29], Proposition 1.11, for the group $G(F)$ and the statement concerning $W(F)$ follows by applying SDT (iii).

Now consider a class of fields with the property that binary forms represent extremely few elements of $g(F)$.

A field F is said to be *rigid* if $|D(\varphi)| \leqslant 2$ for any anisotropic binary quadratic form φ over F.

First observe that a rigid field with $|D(\varphi)| = 2$ for every anisotropic binary form φ, is necessarily non-real and has stufe $s \leqslant 2$. Indeed, $|D(1,1)| = 2$ implies the existence of a non-square b in $D_F(1,1)$, and so $(1, -b)$ represents -1 and also 1 and $-b$. Since $(1, -b)$ is anisotropic, we have $|D(1, -b)| = 2$, hence $b = -1$, hence $s \leqslant 2$, as asserted. Such fields have been considered by Cordes [2] who called them $\bar{C}$-fields. He proved that a $\bar{C}$-field has necessarily a finite square class number q.

On the other hand, if F is rigid and $|D(\varphi)| < 2$ for an anisotropic form φ, then clearly $\det\varphi = 1$, i.e., $|D(1,1)| = 1$ and the field is pythagorean. If it is also non-real, then $q = 1$ and so $|D(\varphi)| = 1$ for any quadratic form φ. If the field is real, then it must be super-pythagorean, as proved in [29], Proposition 1.22, for fields with finite q, and by M. Kula [13], Theorem 3.1, for the general case. Summarizing we have the following three classes of rigid fields:

I. Fields with $q = 1$,

II. Non-real rigid fields with $q > 1$ ($\bar{C}$-fields),

III. Real rigid fields (super-pythagorean fields).

We determine here the groups $G(F)$ and $W(F)$ for any rigid field of the type II and III, the case I being trivial (cf. [29], Theorem 2.1). We begin with the type II. The theorem below generalizes the cases IV and VII of the Classification Theorem 2.4 in [29], where the theorem was proved for fields with $q = 8$.

THEOREM 2.3. *Let F be a non-real rigid field with square class number $q > 1$. Then*

$$G(F) \cong \mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})^{q-1} \quad \text{and} \quad W(F) \cong (\mathbf{Z}/2\mathbf{Z})^q, \quad \text{if} \quad s = 1,$$

and

$$G(F) \cong \mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \oplus (\mathbf{Z}/4\mathbf{Z})^{q/2-1} \quad \text{and} \quad W(F) \cong (\mathbf{Z}/4\mathbf{Z})^{q/2}, \quad \text{if} \quad s = 2.$$

In the first case the direct summands of $G(F)$ are generated by $\langle 1\rangle$ and all the elements $\langle 1\rangle - \langle b\rangle$, $1 \neq b \in g(F)$. In the second case the direct summands of $G(F)$ are generated by $\langle 1\rangle$, $\langle 1\rangle - \langle -1\rangle$ and all the elements $\langle 1\rangle - \langle b\rangle$,

where $1 \neq b \in h(F)$, $h(F)$ *being any subgroup of* $g(F)$ *such that* $g(F) = \{1, -1\} \times h(F)$.

Proof. Consider first the case $s = 1$. Write $g(F) = \{1, b_2, \ldots, b_q\}$. We know that $J_0(F)$ is generated by the elements $\langle 1\rangle - \langle b_i\rangle$, $i = 2, \ldots, q$, and it is sufficient to prove that these are independent. Since $s = 1$, we have $2J_0(F) = 0$, and the linear dependence of the generators implies the relation

$$\langle 1\rangle - \langle b_{i_1}\rangle + \ldots + \langle 1\rangle - \langle b_{i_m}\rangle = 0, \quad \text{for} \quad 2 \leqslant i_1 < \ldots < i_m \leqslant q.$$

Hence

$$m\langle 1\rangle = \langle b_{i_1}, \ldots, b_{i_m}\rangle,$$

where the b's are different elements of $g(F)$. However, the rigidity of the field implies that any dyadic change on the right hand side reduces to a permutation of the b's, so that it is impossible to pass from the right to the left by dyadic changes. This contradiction proves the independence of the generators of $J_0(F)$.

Now consider the case $s = 2$. Write $g(F) = \{1, -1\} \times h$. From the identity $\langle 1\rangle - \langle -b\rangle = \langle 1\rangle - \langle -1\rangle - (\langle 1\rangle - \langle b\rangle)$ it follows that $\langle 1\rangle - \langle -1\rangle$ and the elements $\langle 1\rangle - \langle b\rangle$, $b \in h$, generate $J_0(F)$. Now, $\langle 1\rangle - \langle -1\rangle$ is of order 2 and if

$$\langle 1\rangle - \langle -1\rangle = \sum x_i(\langle 1\rangle - \langle b_i\rangle), \quad b_i \in h, \; x_i \in \mathbf{Z},$$

then comparing determinants we get $-1 \in h$, a contradiction. Hence $\langle 1\rangle - \langle -1\rangle$ generates a direct summand of order 2 in $J_0(F)$ and the complementary direct summand is generated by the elements $\langle 1\rangle - \langle b\rangle$, $1 \neq b \in h$. It suffices to show that the latter are independent. First observe that $\langle 1\rangle - \langle b\rangle$, with $1 \neq b \in h$, is an element of order 4. Indeed, $4(\langle 1\rangle - \langle b\rangle) = 0$ is obvious ($s = 2$), and $2(\langle 1\rangle - \langle b\rangle) \neq 0$, since otherwise $(1, 1)$ represents $b \neq \pm 1$, contrary to the assumption that F is rigid. Now assume that

$$\sum x_j(\langle 1\rangle - \langle b_j\rangle) = 0, \quad j = 2, \ldots, q/2, \; 1 \neq b_j \in h, \; x_j = 0, \pm 1, 2.$$

This implies an equality of the form

$$r\langle 1\rangle + \langle e_1, \ldots, e_p\rangle = \langle c_1, \ldots, c_n\rangle + 2\langle d_1, \ldots, d_m\rangle, \tag{2.3.1}$$

where e_i, c_j, d_k are different elements of h.

If $r = 0$, this is impossible since dyadic changes on the left hand side can only permute the diagonal entries. Similarly in the case $r < 0$, after writing (2.3.1) in the form $\langle e_1, \ldots, e_p\rangle = -r\langle 1\rangle + \ldots$

If $r > 0$, there is also no way for obtaining the right hand side by dyadic changes performed on the left hand side, since the only new diagonal entry which can be obtained is -1 (from $(1, 1) \cong (-1, -1)$) and this

does not appear on the right hand side of (2.3.1). Thus the elements $\langle 1\rangle - \langle b_j\rangle$, $j = 2, \ldots, q/2$ are independent, which proves the second statement concerning $G(F)$. The statements concerning $W(F)$ follow from the above and the SDT, which also enables us to find the generators for the direct summands of $W(F)$.

It remains to discuss the rigid fields of type III, that is, super-pythagorean fields.

THEOREM 2.4. *Let F be a super-pythagorean field with square class number $q = 2^n$ and let h be any subgroup of $g(F)$ such that $g(F) = \{1, -1\} \times h$. Then $G(F)$ is the direct sum of $2^{n-1}+1$ infinite cyclic subgroups generated by $\langle 1\rangle$, $\langle 1\rangle - \langle -1\rangle$ and all the elements $\langle 1\rangle - \langle a\rangle$, $1 \neq a \in h$.*

The Witt group $W(F)$ is the direct sum of 2^{n-1} infinite cyclic subgroups generated by the similarity classes of the forms (1) and $(1, -a)$, $1 \neq a \in h$.

Proof. The statement concerning $G(F)$ has been proved in [29], Proposition 1.23. The decomposition of $W(F)$ can be obtained according to the SDT.

Another class of pythagorean fields we want to discuss are pythagorean fields satisfying SAP, the Strong Approximation Property studied by Elman and Lam [5] (see also Elman, Lam and Prestel [7]). If F is any pythagorean field with a finite square class number $q = 2^n$, then the number r of orderings of the field F satisfies $n \leqslant r \leqslant 2^{n-1}$. Now, it is known that $r = n$ characterizes fields satisfying SAP and $r = 2^{n-1}$ the super-pythagorean fields (cf. Elman and Lam [5], 4.5 and 5.7; see also Kula [13]). Thus SAP fields and super-pythagorean fields are two extreme cases of pythagorean fields.

THEOREM 2.5. *Let F be a pythagorean field satisfying SAP and with square class number $q = 2^n$. Then there exists a basis $\{-1, a_2, \ldots, a_n\}$ for $g(F)$ such that $\langle 1\rangle$, $\langle 1\rangle - \langle -1\rangle$, $\langle 1\rangle - \langle a_2\rangle$, $\ldots$, $\langle 1\rangle - \langle a_n\rangle$ form a free basis for $G(F)$ and the similarity classes of the forms $(1), (1, -a_2), \ldots, (1, -a_n)$ form a free basis for $W(F)$.*

Proof. For the case of Witt group this is proved by Elman and Lam ([5], Proposition 5.8). They also show that $(1,1), (1, -a_2), \ldots$ $\ldots, (1, -a_n)$ is a free basis for $I(F)$, the subgroup of all even dimensional elements of $W(F)$. Since the canonical homomorphism $f\colon G(F) \to W(F)$ restricted to $J_0(F)$ is injective and $f(J_0(F)) = I(F)$, we obtain the basis for $J_0(F)$:

$$f^{-1}(1,1) = \langle 1\rangle - \langle -1\rangle, \ldots, f^{-1}(1, -a_n) = \langle 1\rangle - \langle a_n\rangle.$$

By FDT, we obtain the free basis for $G(F)$. ∎

Remark 2.6. Pythagorean fields satisfying SAP can also be characterized by the value sets of binary forms. M. Kula ([13], Theorem 4.1)

proved that a real pythagorean field F with $q = 2^n$ satisfies SAP if and only if there exists a basis $\{a_1, \ldots, a_n\}$ for the group $g(F)$ such that

$$|D(1, -a_i)| = 2^{n-1} \quad \text{for} \quad i = 1, \ldots, n.$$

Now let us consider another class of formally real fields which being non-rigid show some signs of rigidity. The class is characterized in the next theorem. However, it should be pointed out that the existence of such fields has not been proved yet, even in the case $q = 8$ (cf. [29], the case II of Theorem 2.5).

THEOREM 2.7. *Let F be a real field with unique ordering and such that every positive element is the sum of two squares. If for any positive definite binary form φ with $\det\varphi \neq 1$ we have $|D(\varphi)| = 2$, then*

$$G(F) \cong \mathbf{Z} \oplus \mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})^{(I)} \quad \text{and} \quad W(F) \cong \mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})^{(I)},$$

where $I = D(1,1) \setminus \{1\}$ (if $q < \infty$, then $|I| = (q/2) - 1$). The direct summands of $G(F)$ are generated by $\langle 1\rangle$, $\langle 1\rangle - \langle -1\rangle$ and all the elements $\langle 1\rangle - \langle b\rangle$, $1 \neq b \in D(1,1)$.

Proof. We have $g(F) = \{1, -1\} \times D(1,1)$ and by the SDT (iii) it is sufficient to show that the set $\{\langle 1\rangle - \langle b\rangle : 1 \neq b \in D(1,1)\}$ is linearly independent. Since $2(\langle 1\rangle - \langle b\rangle) = 0$ for any $b \in D(1,1)$, any linear dependence relation would imply

$$m\langle 1\rangle = \langle b_1, \ldots, b_m\rangle, \quad b_i \in D(1,1),\ b_i \neq 1, \quad b_i \neq b_j \quad \text{for} \quad i \neq j. \tag{2.7.1}$$

Now use the piecewise equivalence and the assumption $|D(b_i, b_j)| = 2$ to prove the impossibility of (2.7.1). The statement concerning $W(F)$ follows from the above and the SDT. ∎

§ 3. The rank of $G(F)$ and $W(F)$. For a finitely generated abelian group G we consider the rank of G, that is, the number of elements in a maximal linearly independent subset of G containing only the elements of infinite order or of prime power order. This is known to be an isomorphism invariant of the group G (cf. Fuchs [8], Theorem III.16.3). Moreover, if G is decomposed into the direct sum of cyclic subgroups whose orders are infinity or prime powers, then rank G equals to the number of direct summands in the decomposition. We shall give here some estimates for rank $G(F)$ and rank $W(F)$ for any field F with a finite square class number q (if $q = \infty$, the group $G(F)$ is not finitely generated) and we show that the bounds are attained in special cases. Observe that, by the SDT, we have $\operatorname{rank} G(F) = 1 + \operatorname{rank} W(F)$, for all real fields and for non-real fields with $s > 1$, while $\operatorname{rank} G(F) = \operatorname{rank} W(F)$ for fields with $s = 1$. Thus we can restrict the investigation to the case of the Grothendieck group.

THEOREM 3.1. *Let F be any field with square class number $q = 2^n$. Then*

(i) $$n+1 \leqslant \operatorname{rank} G(F) \leqslant 2^n.$$

(ii) *Moreover, if F is real, then*

$$n+1 \leqslant \operatorname{rank} G(F) \leqslant 2^{n-1}+1.$$

(iii) *For any $n \geqslant 0$ there exist non-real fields F_1 and F_2 such that $q(F_1) = q(F_2) = 2^n$ and $\operatorname{rank} G(F_1) = n+1$, $\operatorname{rank} G(F_2) = 2^n$.*

(iv) *For any $n \geqslant 1$ there exist real fields F_3 and F_4 such that $q(F_3) = q(F_4) = 2^n$ and $\operatorname{rank} G(F_3) = n+1$, $\operatorname{rank} G(F_4) = 2^{n-1}+1$.*

Proof. We shall use repeatedly the following fact: if G is generated by t elements whose orders are infinity or prime powers, then $\operatorname{rank} G \leqslant t$. We know that $G(F)$ is generated by $\langle 1\rangle$ and all the elements $\langle 1\rangle - \langle a\rangle$, $1 \neq a \in g(F)$. Since $\langle 1\rangle$ is of infinite order and $\langle 1\rangle - \langle a\rangle$ is either of infinite or of 2-power order, the rank of $G(F)$ is not greater than the number of such generators. Hence $\operatorname{rank} G(F) \leqslant 2^n$. On the other hand,

$$\det\colon J_0(F) \to g(F)$$

is a surjective group homomorphism, hence

$$n+1 = 1+\operatorname{rank} g(F) \leqslant 1+\operatorname{rank} J_0(F) = \operatorname{rank} G(F).$$

Thus (i) is proved. Now assume that F is real. By Lemma 1.10 of [29], $G(F)$ is generated by $2^{n-1}+1$ elements, whose orders are either infinity or 2-powers, whence (ii) follows.

(iii) It is known that for any $n \geqslant 0$ there exists a non-real field F_1 such that $q(F_1) = 2^n$ and every binary form over F_1 is universal (cf. Cordes [2], p. 407; Elman and Lam [6], 3.8; [28], Theorem 2.3). By Theorem 2.1, $\operatorname{rank} G(F_1) = n+1$. For F_2 one can choose any non-real rigid field with $q = 2^n$ and $s = 1$. This follows from Theorem 2.3. An explicit example: $F_2 = \boldsymbol{C}((t_1))\dots((t_n))$, the iterated power series field over the complex field. We have $G(\boldsymbol{C}) \cong \boldsymbol{Z}$ and $W(\boldsymbol{C}) \cong \boldsymbol{Z}/2\boldsymbol{Z}$ and an obvious induction using Theorem 1.3 gives

$$G(F_2) \cong \boldsymbol{Z} \oplus (\boldsymbol{Z}/2\boldsymbol{Z})^{2^n-1}.$$

Hence (iii) is proved.

(iv) A field F satisfying assumptions of Theorem 2.2 and such that $q(F) = 2^n$ can be taken for F_3. The existence of such a field for any $n \geqslant 1$ has been proved in [29], § 4, the case 2.5.I. For F_4 take any super-pythagorean field with $q = 2^n$. Theorem 2.4 shows that $\operatorname{rank} G(F_4) = 2^{n-1}+1$. An explicit example:

$$F_4 = \boldsymbol{R}((t_1))\dots((t_{n-1})).$$

Remark 3.2. Cordes [2], Proposition 7.3, considered a special case of the above theorem. He proved that $W(F)$ is cyclic and finite iff $q = 1$ or $q = 2$ and $s = 2$.

EXAMPLE 3.3. For pythagorean field F with a finite number r of orderings, we have $\operatorname{rank} G(F) = r+1$, since by [29], Proposition 1.19, the group $G(F)$ is torsion free, and so, by Theorem 1.3 we have $G(F) = \boldsymbol{Z}^{r+1}$.

EXAMPLE 3.4. For any field F with a finite number r of orderings,

$$\operatorname{rank} G(F) \geqslant r+1$$

with equality iff F is pythagorean.

EXAMPLE 3.5. For a local field K with residue class field F of characteristic $\neq 2$,

$$\operatorname{rank} G(K) = \operatorname{rank} G(F) + \operatorname{rank} W(F),$$

and

$$\operatorname{rank} W(K) = 2 \cdot \operatorname{rank} W(F),$$

by Theorem 1.3.

Although the bounds given in Theorem 3.1 are attained in special cases, the rank of $G(F)$ does not take on all the values between the bounds when F runs through the class of fields with $q = 2^n$. This is pointed out in the following theorem.

THEOREM 3.6. (i) *If F is a non-real field with $q = 2^n$ and the stufe s is greater than one, then*

$$\operatorname{rank} G(F) \leqslant 2^{n-1}+1.$$

(ii) *If F is a non-real field with $q = 2^n \geqslant 4$, $s = 1$ and such that* $\operatorname{rank} G(F) < 2^n$, *then*

$$\operatorname{rank} G(F) \leqslant 3 \cdot 2^{n-2}.$$

(iii) *The bounds in* (i) *and* (ii) *are attained in special cases.*

Proof. (i) is proved by using the same argument as for real fields in the Theorem 3.1(ii). Since $s > 1$, we have a decomposition $g(F) = \{1, -1\} \times h$, where $|h| = 2^{n-1}$. Now, from $\langle 1, -1\rangle = \langle a, -a\rangle$ one obtains $\langle 1\rangle - \langle -a\rangle = \langle 1\rangle - \langle -1\rangle - (\langle 1\rangle - \langle a\rangle)$, that is, the set of generators $\{\langle 1\rangle, \langle 1\rangle - \langle a\rangle, 1 \neq a \in g(F)\}$ for $G(F)$ can be reduced to $\{\langle 1\rangle, \langle 1\rangle - \langle -1\rangle, \langle 1\rangle - \langle a\rangle, 1 \neq a \in h\}$, consisting of $2^{n-1}+1$ elements. Hence (i).

(ii) If $s = 1$ and $\operatorname{rank} G(F) < 2^n$, then by Theorem 2.3 the field F cannot be rigid, i.e., there exists a binary anisotropic form $(1, a)$ representing more than 2 elements of $g(F)$. Hence $\langle 1, a\rangle = \langle b, c\rangle$, for some $b \neq 1$ and $c \neq 1$ and $bc = a$. (Here $a \neq 1$, since otherwise the form $(1, a)$ is isotropic.) Thus $1, b, c, bc$ form a 4-element subgroup of $g(F)$

and we can write $g(F) = \{1, b, c, bc\} \times h$, for a suitable subgroup h of order 2^{n-2}. Now $\langle 1, bc\rangle = \langle b, c\rangle$ implies

$$\langle 1\rangle - \langle xbc\rangle = \langle 1\rangle - \langle x\rangle + \langle 1\rangle - \langle xb\rangle + \langle 1\rangle - \langle xc\rangle,$$

for any $x \in h$. Thus out of any four generators

$$\langle 1\rangle - \langle x\rangle,\ \langle 1\rangle - \langle xb\rangle,\ \langle 1\rangle - \langle xc\rangle,\ \langle 1\rangle - \langle xbc\rangle, \quad x \in h$$

of $J_0(F)$, one can be omitted. Hence $J_0(F)$ is generated by $3\cdot 2^{n-2}-1$ elements and $G(F)$ by $3\cdot 2^{n-2}$ elements, as required.

(iii) Examples. The bound in 3.6(i) is attained when F is any non-real rigid field with $s > 1$. This follows immediately from Theorem 2.3. An explicit example is the field $\boldsymbol{F}_p((t_1))\ldots((t_{n-1}))$, where $\boldsymbol{F}_p$ is the prime field of characteristic $p \equiv 3 \bmod 4$ (cf. [29], § 4, the case 2.4.VII). The bound in 3.6 (ii) is attained in the case of the field $F_n = k((t_1))\ldots$ $\ldots((t_{n-2}))$, $n \geqslant 2$, where k is any field with $q(k) = 4$, $s = 1$ and such that every binary form over k is universal (see [27], case I at p. 35, for an explicit example). We have

$$q(F_n) = 2^n, \quad s(F_n) = s(k) = 1, \quad G(k) \cong \boldsymbol{Z} \oplus (\boldsymbol{Z}/2\boldsymbol{Z})^2, \quad W(k) \cong (\boldsymbol{Z}/2\boldsymbol{Z})^3$$

cf. [29], Theorem 3.2 (3.1)). Now an easy induction on n shows that

$$G(F_n) \cong \boldsymbol{Z} \oplus (\boldsymbol{Z}/2\boldsymbol{Z})^{3\cdot 2^{n-2}-1} \quad \text{and} \quad W(F_n) \cong (\boldsymbol{Z}/2\boldsymbol{Z})^{3\cdot 2^{n-2}}$$

(use Theorem 1.3). Thus $\operatorname{rank} G(F_n) = 3\cdot 2^{n-2}$, as required.

Corollary 3.7. *If F runs through the class of non-real fields with square class number $q = 2^n$, then the two greatest values of* $\operatorname{rank} G(F)$ *are* 2^n *and* $3\cdot 2^{n-2}$.

One can conjecture that the third value of $\operatorname{rank} G(F)$ is $2^{n-1}+1$.

For real fields one can easily prove the following: If F is real pythagorean and $q(F) = 2^n$ and $\operatorname{rank} G(F) < 2^{n-1}+1$, then $\operatorname{rank} G(F) \leqslant 1+3\cdot 2^{n-3}$ (use Theorem 2.4 and Example 3.3 above and Proposition 1.22 of [29]). Moreover, the value $1+3\cdot 2^{n-3}$ is taken on by $\operatorname{rank} G\left(F((t_1))\ldots((t_{n-3}))\right)$, where F is a pythagorean field satisfying SAP with $q = 8$. The above power series field is also pythagorean and the rank can be computed by induction on using Theorem 1.3. However, we do not know whether or not $1+3\cdot 2^{n-3}$ is the second greatest value taken on by the rank of $G(F)$ when F ranges through all real fields with $q = 2^n$.

Chapter IV

Equivalence of fields with respect to quadratic forms

§ 1. *G*-**equivalences.** In this chapter we shall investigate isomorphisms of Grothendieck groups and rings and classify fields with respect to the isomorphism classes of their Grothendieck groups and rings. One of the difficulties involved is that isomorphisms of Grothendieck rings — and the more of Grothendieck groups — do not, in general, preserve dimensions, forms and hyperbolic planes. Consider the following example.

Let F and K be two real closed fields. Then the Grothendieck groups $G(F)$ and $G(K)$ are isomorphic since both have direct sum decompositions $\boldsymbol{Z}\langle 1\rangle \oplus \boldsymbol{Z}\langle -1\rangle$. Now, the mapping $h\colon G(F)\to G(K)$ defined by $h\langle 1\rangle = \langle 1\rangle$ and $h\langle -1\rangle = -\langle -1\rangle$ is also a group isomorphism, and it is routine to check that h is, in fact, a ring isomorphism. This ring isomorphism sends the 1-dimensional element $\langle -1\rangle$ into the -1-dimensional element $-\langle -1\rangle$ and sends the hyperbolic plane $\langle 1, -1\rangle$ into $\langle 1\rangle - \langle -1\rangle$, that is, it preserves neither dimensions, nor hyperbolic planes, nor quadratic forms.

This motivates the distinction between the cases when the groups — or rings — are just isomorphic and when there is an isomorphism with some special properties. We introduce the following four definitions.

Definition 1.1. Two fields F and K are said to be *G-equivalent* if the Grothendieck groups $G(F)$ and $G(K)$ are isomorphic.

Definition 1.2. Two fields F and K are said to be *strongly G-equivalent* if there exists a group isomorphism $T\colon G(F)\to G(K)$ sending the set $\{\langle a\rangle\colon a\in F^*\}$ of 1-dimensional forms over F onto the set $\{\langle b\rangle\colon b\in K^*\}$ of 1-dimensional forms over K (T will be called a *strong G-isomorphism*).

Definition 1.3. Two fields F and K are said to be *GR-equivalent* if the Grothendieck rings $G(F)$ and $G(K)$ are isomorphic.

Definition 1.4. Two fields F and K are said to be *strongly GR-equivalent* if there exists a ring isomorphism $T\colon G(F)\to G(K)$ sending the set of 1-dimensional forms over F onto the set of 1-dimensional forms over K (T will be called the *strong GR-isomorphism*).

First recall that G-equivalence has been discussed in [27]. However, in the Corrigendum to that paper it was pointed out that the proofs assumed more than stated in the definition of the G-equivalence; in fact, the proofs assumed the existence of a strong G-isomorphism T satisfying $T\langle 1\rangle = \langle 1\rangle$, that is, a bit more than the strong G-equivalence. Nevertheless, we shall prove that the invariants discovered in [27] are also strong G-invariants (see Proposition 1.7 below).

We proceed to give some characterizations of the strong equivalences.

THEOREM 1.5. *For any two fields F and K the following conditions are equivalent.*

(i) *F and K are strongly G-equivalent.*

(ii) *There exists a bijective mapping t: $g(F)\to g(K)$ such that*

$$\langle a_1, a_2\rangle = \langle b_1, b_2\rangle \text{ over } F \Leftrightarrow \langle t(a_1), t(a_2)\rangle = \langle t(b_1), t(b_2)\rangle \text{ over } K.$$

(iii) *There exists a bijective mapping t: $g(F)\to g(K)$ such that, for any $n \geqslant 1$,*

$$\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle \text{ over } F \Leftrightarrow \langle t(a_1), \ldots, t(a_n)\rangle = \langle t(b_1), \ldots, t(b_n)\rangle \text{ over } K.$$

Proof. (i) $\Rightarrow$ (ii). Let T: $G(F)\to G(K)$ be a strong G-isomorphism. The set of 1-dimensional forms in $G(F)$ corresponds bijectively to the group $g(F)$, and similarly over the field K, hence we obtain a bijective mapping t: $g(F)\to g(K)$ whose action can be described explicitly as follows: $t(a) = \det T\langle a\rangle$. In other words, $T\langle a\rangle = \langle t(a)\rangle$. Hence

$$\langle a_1, a_2\rangle = \langle b_1, b_2\rangle \text{ over } F \Leftrightarrow T\langle a_1, a_2\rangle = T\langle b_1, b_2\rangle \Leftrightarrow \langle t(a_1), t(a_2)\rangle = \langle t(b_1), t(b_2)\rangle \text{ over } K.$$

(ii) $\Rightarrow$ (iii). This follows from Witt's theorem on piecewise equivalence (Witt [31], Satz 7) by using induction on n.

(iii) $\Rightarrow$ (i). Let $M(F)$ and $M(K)$ be the semigroups of equivalence classes of quadratic forms over F and K, respectively. Define T_0: $M(F)\to M(K)$ by putting

$$T_0\langle a_1, \ldots, a_n\rangle = \langle t(a_1), \ldots, t(a_n)\rangle.$$

Now (iii) assures the well-definedness of T_0 and its bijectivity. Obviously, T_0 is a semigroup isomorphism. By the universal property of the Grothendieck group, T_0 extends uniquely to a group isomorphism T: $G(F)\to G(K)$, which turns out to be a strong G-isomorphism. ∎

It is interesting to note the following characterization of the strong GR-equivalence and to compare it with Theorem 1.5.

THEOREM 1.6. *For any two fields F and K the following conditions are equivalent.*

(i) *F and K are strongly GR-equivalent.*

(ii) *There exists a group isomorphism $t\colon g(F)\to g(K)$ such that*

$$\langle a_1, a_2\rangle = \langle b_1, b_2\rangle \text{ over } F \Leftrightarrow \langle t(a_1), t(a_2)\rangle = \langle t(b_1), t(b_2)\rangle \text{ over } K.$$

(iii) *There exists a group isomorphism $t\colon g(F)\to g(K)$ such that for any $n\geqslant 1$,*

$$\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle \text{ over } F \Leftrightarrow \langle t(a_1), \ldots, t(a_n)\rangle = \langle t(b_1), \ldots, t(b_n)\rangle \text{ over } K.$$

Proof. (i)$\Rightarrow$(ii). Define t as in the proof of Theorem 1.5. Then by the above theorem it suffices to prove that t preserves multiplication. Take any a, b in $g(F)$ and assume that $T\langle a\rangle = \langle a'\rangle$ and $T\langle b\rangle = \langle b'\rangle$. Then

$$t(ab) = \det T\langle ab\rangle = \det(T\langle a\rangle \cdot T\langle b\rangle) = a'\cdot b' = t(a)\cdot t(b),$$

as required.

(ii)$\Rightarrow$(iii) is proved as in Theorem 1.5.

(iii)$\Rightarrow$(i). Define T as in the proof of Theorem 1.5. It remains to prove that T preserves multiplication, and this follows easily from

$$T(\langle a\rangle\cdot\langle b\rangle) = T\langle ab\rangle = \langle t(ab)\rangle = \langle t(a)\cdot t(b)\rangle = T\langle a\rangle\cdot T\langle b\rangle$$

and from the fact that 1-dimensional forms generate additively the Grothendieck ring. ∎

Now we want to discuss some invariants of G- and GR-equivalences.

Proposition 1.7. *The following field invariants are preserved by the strong G-equivalence:*

(i) *q, the cardinality of the group of square classes.*

(ii) *q_n, the cardinality of the set of square classes represented by the form $n\times\langle 1\rangle$.*

(iii) *u_n, the cardinality of the set of equivalence classes of n-dimensional universal quadratic forms.*

(iv) *r, the number of orderings of the field in the case when it is finite (r being zero if the field is non-real). Moreover, if r is finite, it is invariant under G-equivalence.*

(v) *u, the maximal dimension of an anisotropic form over the field.*

We need a lemma.

Lemma 1.8. *Suppose the fields F and K are strongly G-equivalent and let T and t be the corresponding strong G-isomorphism and the bijective mapping satisfying* 1.5 (iii), *respectively. Then for any quadratic form φ over F we have*

$$t\big(D(\langle\varphi\rangle)\big) = D(T\langle\varphi\rangle);$$

in particular, $D(\langle\varphi\rangle)$ and $D(T\langle\varphi\rangle)$ have the same cardinality and $\langle\varphi\rangle$ is universal if and only if $T\langle\varphi\rangle$ is universal.

Proof. This is an easy consequence of the Theorem 1.5 (iii).

Proof of Proposition 1.7. (i) follows from Theorem 1.5.

(ii) Suppose T and t are the two maps of the lemma. If $T\langle 1\rangle = \langle a\rangle$, then $T(n\langle 1\rangle) = n\langle a\rangle$ and, by the lemma,

$$q_n(F) = |D_{g(F)}(n\langle 1\rangle)| = |D_{g(K)}(n\langle a\rangle)| = |D_{g(K)}(n\langle 1\rangle)| = q_n(K).$$

(iii) T preserves dimension and, by the lemma, sends universal forms into universal forms.

(iv) It suffices to prove that r is invariant under G-equivalence, since every G-invariant is automatically a strong G-invariant. If F is non real and $G(F) \cong G(K)$ (group isomorphism), then $G(F)$ has torsion free rank 1, and so $G(K)$ has also torsion free rank 1 and, by Theorem III.1.4, K cannot be real, since then the torsion free rank of $G(K)$ would be at least two. If F is real with a finite number of orderings and if $G(F) \cong G(K)$, then the torsion free ranks of $G(F)$ and $G(K)$ coincide and by Theorem III.1.4, we have $r(F) = r(K)$, as required.

(v) Since a strong G-isomorphism preserves dimension and universality of quadratic forms, it preserves the minimal dimension u with the property that every u-dimensional form is universal. ∎

Proposition 1.7 can be used to show that G-equivalence does not coincide with strong G-equivalence and that this non-coincidence takes place for fields with any finite square class number $q \geqslant 4$.

Proposition 1.9. *For any natural number $n \geqslant 2$ ($n \geqslant 3$) there exist non-real (real) fields F and K such that*

(i) $q(F) = 2^n$, $q(F) < q(K)$, *and*

(ii) *the groups $G(F)$ and $G(K)$ are isomorphic.*

Thus F and K are G-equivalent but they are not strongly G-equivalent.

Proof. Assume $n \geqslant 2$ and consider any rigid field F with square class number $q = 2^n$ and $s = 1$ (cf. Chapter III.2). By Theorem III.2.3,

$$G(F) \cong \mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})^m, \quad \text{where} \quad m = 2^n - 1.$$

On the other hand, pick up any field K with square class number $q(K) = 2^m$ and such that every binary form over K is universal. By Theorem III.2.1, we have $G(K) \cong \mathbf{Z} \oplus (\mathbf{Z}/2\mathbf{Z})^m$. Hence the fields are G-equivalent and because of $n \geqslant 2$, we have

$$q(F) = 2^n < 2^m = q(K),$$

and the fields are not strongly G-equivalent in view of Proposition 1.7 (i).

To show two real fields satisfying (i) and (ii) we take any super-

pythagorean field F with $q = 2^n$, for example

$$F = \boldsymbol{R}((t_1)) \dots ((t_{n-1})),$$

and pick up a pythagorean field K satisfying SAP with $q(K) = 2^{2^{n-1}}$ (the existence of SAP pythagorean fields with any finite square class number $\geqslant 2$ has been proved by Elman and Lam [5], p. 1187). Theorems III.2.4 and III.2.5 show that the groups $G(F)$ and $G(K)$ are isomorphic and, because of $n \geqslant 3$, we have $q(F) < q(K)$. This finishes the proof.

Remark 1.10. The stufe of the field and the Witt group are not — in general — preserved by G-equivalence nor by strong G-equivalence. A counter-example has been given in [27] for fields with $q = 2$ and 4. Such counter-examples do exist for any q. First, take two fields F and K with given q and with the property that every binary form over them is universal. One can choose F and K to satisfy additionaly $s(F) = 1$ and $s(K) = 2$ (cf. Cordes [2], p. 407; [28], p. 56). By Proposition 1.7 of [29], the fields are strongly G-equivalent but they have non-isomorphic Witt groups (by Theorem III.2.1), and also $s(F) \neq s(K)$.

Another example is provided by the proof of Proposition 1.9 above. For, pick up F and K as in the first part of the proof and take K with $s = 2$. Then the fields are G-equivalent and have different square class numbers and also $s(F) \neq s(K)$. Also the Witt groups are not isomorphic, by Theorem III.2.1 and III.2.3.

We now introduce other field invariants which are preserved by strong GR-equivalence. For any $n \geqslant 1$ and for any field F, we denote by $p_n = p_n(F)$ the cardinality of the set of equivalence classes of n-fold Pfister forms over F. For any field F we have $p_1 = q$, since 1-fold Pfister forms are classified by the determinant. The second p-invariant is also easily identified, namely, we have $p_2 = Q$, the number of isomorphism classes of quaternion algebras over the field. This is the consequence of the fact that the equivalence classes of 2-fold Pfister forms are in natural one-to-one correspondence with the isomorphism classes of quaternion algebras over the field (cf. O'Meara [22], 57 : 8, p. 146).

By the Main Theorem of Elman and Lam [4], $p_n(F)$ equals to the number of distinct generators $l(a_1) \dots l(a_n)$ in the Milnor's algebraic K-group $k_n F$.

Proposition 1.11. *The following field invariants are preserved by the strong GR-equivalence*:

(i) *all the strong G-invariants, and*

(ii) p_n, *the cardinality of the set of equivalence classes of n-fold Pfister forms, for any* $n \geqslant 1$.

Proof. (i) is clear. To prove (ii) we observe that for any strong

GR-isomorphism T: $G(F)\to G(K)$ we have

$$T\langle\langle a_1, \ldots, a_n\rangle\rangle = \langle\langle t(a_1), \ldots, t(a_n)\rangle\rangle,$$

where t is the corresponding group isomorphism of Theorem 1.6 (here we have used the fact that t preserves multiplication). Thus T maps bijectively the set of equivalence classes of n-fold Pfister forms over F onto the corresponding set of classes over K. ∎

§ 2. W-equivalences. In this section we discuss briefly the equivalence of fields with respect to the group or ring structure of the Witt ring $W(F)$.

DEFINITION 2.1. Two fields F and K are said to be *W-equivalent* if the Witt groups $W(F)$ and $W(K)$ are isomorphic.

DEFINITION 2.2. Two fields F and K are said to be *strongly W-equivalent* if there exists a group isomorphism T: $W(F)\to W(K)$ sending the set of 1-dimensional forms over F onto the set of 1-dimensional forms over K (a *strong W-isomorphism*).

DEFINITION 2.3. Two fields F and K are said to be *WR-equivalent* if the Witt rings $W(F)$ and $W(K)$ are isomorphic.

DEFINITION 2.4. Two fields F and K are said to be *strongly WR-equivalent* if there exists a ring isomorphism T: $W(F)\to W(K)$ sending the set of 1-dimensional forms over F onto the set of 1-dimensional forms over K (a *strong WR-isomorphism*).

First we state some characterizations of strong equivalences analogous to the Theorems 1.5 and 1.6.

THEOREM 2.5. *For two fields F and K the following statements are equivalent:*

(i) *F and K are strongly W-equivalent.*

(ii) *There exists a bijective mapping t: $g(F)\to g(K)$ such that*

(2.5.1) $\langle a_1, a_2\rangle = \langle b_1, b_2\rangle$ *over* $F \Leftrightarrow \langle t(a_1), t(a_2)\rangle = \langle t(b_1), t(b_2)\rangle$ *over* K,

and

(2.5.2) *there exists* $a\in g(F)$ *such that* $t(-a) = -t(a)$.

(iii) *There exists a bijective mapping t: $g(F)\to g(K)$ such that, for any* $n \geqslant 1$,

(2.5.3) $\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle$ *over* F

$$\Leftrightarrow \langle t(a_1), \ldots, t(a_n)\rangle = \langle t(b_1), \ldots, t(b_n)\rangle \text{ over } K,$$

and

(2.5.4) *there exists* $a\in g(F)$ *such that* $t(-a) = -t(a)$.

Proof. (i) $\Rightarrow$ (ii). Suppose T is a strong W-isomorphism. Then for any $a \in g(F)$ there exists a unique $t(a) \in g(K)$ such that $T\langle a\rangle = \langle t(a)\rangle$. This defines $t\colon g(F) \to g(K)$; t is bijective, since equivalence classes of 1-dimensional forms are in one-to-one correspondence with square classes. Now, $T\langle a_1, a_2\rangle = T\langle a_1\rangle + T\langle a_2\rangle = \langle t(a_1), t(a_2)\rangle$ and (2.5.1) follows from the well-definedness and injectivity of T. Moreover, for every $a \in g(F)$ we have $0 = T\langle a, -a\rangle = \langle t(a), t(-a)\rangle$ in $W(K)$, and so $t(-a) = -t(a)$, hence (2.5.2).

(ii) $\Rightarrow$ (iii). Use induction on n and piecewise equivalence.

(iii) $\Rightarrow$ (i). Define $T\colon W(F) \to W(K)$ by putting

$$T\langle a_1, \ldots, a_n\rangle = \langle t(a_1), \ldots, t(a_n)\rangle. \tag{2.5.5}$$

First we must prove that T is well defined on similarity classes. If two forms φ and ψ are similar and have equal dimensions, then they are equivalent, and by (2.5.3) and (2.5.5), we have $T(\varphi) = T(\psi)$ in $W(K)$. If $\dim\varphi > \dim\psi$, say, then

$$\varphi \cong \psi \perp m \times (1, -1) \cong \psi \perp m \times (a, -a),$$

where a satisfies (2.5.4) and m is a positive integer. If $\varphi = (a_1, \ldots . a_n)$ and $\psi = (b_1, \ldots, b_{n-2m})$, then by (2.5.3) and (2.5.4),

$$\begin{aligned}\langle t(a_1), \ldots, t(a_n)\rangle &= \langle t(b_1), \ldots, t(b_{n-2m}), t(a), -t(a), \ldots, t(a), -t(a)\rangle \\ &= \langle t(b_1), \ldots, t(b_{n-2m}), 1, -1, \ldots, 1, -1\rangle.\end{aligned}$$

Thus $T(\varphi) = T(\psi)$ in $W(K)$. Reversing the arguments we obtain the proof of injectivity of T, and now (iii) and (2.5.5) imply that T is bijective. Clearly, T preserves addition and sends 1-dimensional forms onto 1-dimensional forms, i.e., T is a strong W-isomorphism, as required. ∎

THEOREM 2.6. *For two fields F and K the following statements are equivalent:*

(i) *F and K are strongly WR-equivalent.*

(ii) *There exists a group isomorphism $t\colon g(F) \to g(K)$ satisfying* (2.5.1) *and* (2.5.2).

(iii) *There exists a group isomorphism $t\colon g(F) \to g(K)$ satisfying* (2.5.3) *and* (2.5.4).

Proof. (i) $\Rightarrow$ (ii). As in the proof of Theorem 2.5 we define t to satisfy $T\langle a\rangle = \langle t(a)\rangle$. It remains to show that t preserves multiplication: $\langle t(ab)\rangle = T\langle ab\rangle = T\langle a\rangle \cdot T\langle b\rangle = \langle t(a)t(b)\rangle$, whence $t(ab) = t(a)t(b)$, as required.

(ii) $\Rightarrow$ (iii) is proved as in the proof of Theorem 2.5.

(iii) $\Rightarrow$ (i). T defined by (2.5.5) is a well-defined group isomorphism. Because of $T(\langle a\rangle\langle b\rangle) = T\langle ab\rangle = \langle t(ab)\rangle = \langle t(a)\rangle\langle t(b)\rangle = T\langle a\rangle \cdot T\langle b\rangle$

and the fact that $W(F)$ is additively generated by 1-dimensional forms, we conclude that T is a strong WR-isomorphism. Thus (i) is proved. ∎

Remarks. (2.7.1) From Theorems 2.5 and 2.6 it is obvious that the square class number q is invariant under both strong W- and strong WR-equivalences. But q is not invariant under W-equivalence, the simplest counter-example being the field Q_p of p-adic numbers with $p \equiv 1 \bmod 4$ and the field with $q = 8, s = 1$ and all binary forms universal. Both fields have Witt group isomorphic to the direct sum of 4 two-element groups (cf. [29], Theorem 3.2, the cases (3.3) and (4.1)) and have different square class numbers, since $q(Q_p) = 4$. Such examples can be constructed for any finite q. This shows that W-equivalence does not coincide with strong W-equivalence.

(2.7.2) Harrison ([9], which is not accessible to me) and Cordes [2] investigated WR-equivalence. They established that two fields are WR-equivalent if and only if there exists a group isomorphism $t: g(F) \to g(K)$ satisfying $t(-1) = -1$ and

$$t\big(D(a_1, \ldots, a_n)\big) = D\big(t(a_1), \ldots, t(a_n)\big)$$

(cf. Cordes [2], Theorem 2.3). These conditions are easily seen to be equivalent to 2.6 (iii) above. Thus WR-equivalence coincides with strong WR-equivalence.

(2.7.3) Cordes ([2], Theorem 7.1) has shown that for fields with Witt ring having at most 32 elements, the WR-equivalence coincides with W-equivalence plus one extra condition, namely, the equality of square class numbers. Thus, in that class of fields, strong W-equivalence coincides with WR-equivalence.

(2.7.4) The stufe of the field is an obvious W-invariant while it is not a G-invariant. If F and K are W-equivalent and F is non-real, then $W(F)$ is a torsion bounded group, hence so is $W(K)$, hence K is non-real. Now the maximal order of an element in the Witt group equals twice the stufe (cf. Theorem III.1.2 (ii)), hence $s(F) = s(K)$. If F is real, so is K and $s(F) = s(K) = \infty$.

§ 3. Comparisons. The theorems proved in the preceding two sections characterize the strong equivalences of fields by means of conditions of the same type and so these equivalences can be easily compared and understood. Here we want first to compare the G- and W-equivalences, and then the GR- and WR-equivalences. The results are contained in the following two theorems.

THEOREM 3.1. *For any two fields F and K the following statements are equivalent.*

(i) *There exists a group isomorphism $T: G(F) \to G(K)$ satisfying*

$$T\langle -1\rangle = \langle -1\rangle \quad \text{and} \quad T\langle 1\rangle = \langle 1\rangle.$$

(ii) *F and K are G-equivalent and $s(F) = s(K)$.*

(iii) *F and K are W-equivalent.*

THEOREM 3.2. *For two fields F and K the following statements are equivalent:*

(i) *There exists a ring isomorphism $T\colon G(F)\to G(K)$ such that $T\langle -1\rangle = \langle -1\rangle$.*

(ii) *F and K are WR-equivalent.*

(iii) *F and K are strongly WR-equivalent.*

(iv) *F and K are strongly GR-equivalent and $T\langle -1\rangle = \langle -1\rangle$ for a strong GR-isomorphism T.*

Proof of Theorem 3.1. (i) $\Rightarrow$ (ii). We must prove that $s(F) = s(K)$. Assuming (i), we have $T(\langle 1\rangle - \langle -1\rangle) = \langle 1\rangle - \langle -1\rangle$, hence

$$s(F) = \operatorname{ord}(\langle 1\rangle - \langle -1\rangle) = \operatorname{ord} T(\langle 1\rangle - \langle -1\rangle) = s(K).$$

(ii) $\Rightarrow$ (iii). This is a consequence of the Second Decomposition Theorem III.1.2. For suppose first that F is non-real and write $s = s(F) = s(K)$. By the SDT (ii), we have

$$\boldsymbol{Z}\oplus \boldsymbol{Z}/s\boldsymbol{Z}\oplus U_0(F) \cong G(F) \cong G(K) \cong \boldsymbol{Z}\oplus \boldsymbol{Z}/s\boldsymbol{Z}\oplus U_0(K)$$

hence $U_0(F) \cong U_0(K)$, and by the SDT, we have

$$W(F) \cong \boldsymbol{Z}/2s\boldsymbol{Z}\oplus U_0(F) \cong \boldsymbol{Z}/2s\boldsymbol{Z}\oplus U_0(K) \cong W(K).$$

If F is real, $s = \infty$ and we argue as above using SDT (iii) instead of SDT (ii).

(iii) $\Rightarrow$ (i). This is proved similarly. For non-real F, $W(F) \cong W(K)$ implies $s(F) = s(K)$ and $U_0(F) \cong U_0(K)$. Now we extend this isomorphism to the groups

$$G(F) = \boldsymbol{Z}\langle 1\rangle \oplus \boldsymbol{Z}/s\boldsymbol{Z}(\langle 1\rangle - \langle -1\rangle)\oplus U_0(F)$$

and

$$G(K) = \boldsymbol{Z}\langle 1\rangle \oplus \boldsymbol{Z}/s\boldsymbol{Z}(\langle 1\rangle - \langle -1\rangle)\oplus U_0(K)$$

by sending $\langle 1\rangle$ into $\langle 1\rangle$ and $\langle 1\rangle - \langle -1\rangle$ into $\langle 1\rangle - \langle -1\rangle$. Thus we get a group isomorphism satisfying (i). For a real field F we proceed analogously. ■

Proof of Theorem 3.2. (i) $\Rightarrow$ (ii). The given isomorphism T sends the hyperbolic plane $\langle 1, -1\rangle$ in $G(F)$ onto the hyperbolic plane $\langle 1, -1\rangle$ in $G(K)$, so it induces the ring isomorphism $W(F) \cong W(K)$. (ii) implies (iii) according to Harrison and Cordes ([9], [2]; cf. Remark (2.7.2) above).

(iii) $\Rightarrow$ (iv). By Theorem 2.6, there exists a group isomorphism $t\colon g(F)\to g(K)$ satisfying (2.5.3) and (2.5.4); hence we can define a ring isomorphism $T\colon G(F)\to G(K)$ satisfying $T\langle a_1, \ldots, a_n\rangle = \langle t(a_1), \ldots, t(a_n)\rangle$ (as in the proof of (iii) $\Rightarrow$ (i) of Theorem 1.6). Now, $t(-a) = -t(a)$ for an

$a \in g(F)$ and $t(-a) = t(-1)t(a)$, hence $t(-1) = -1$ and $T\langle -1\rangle = \langle t(-1)\rangle = \langle -1\rangle$, as required.

(iv) $\Rightarrow$ (i) is trivial. ■

EXAMPLE 3.3. Let K_1 and K_2 be two local fields with residue class fields F_1 and F_2, resp., and assume that $\operatorname{char} F_i \neq 2$, $i = 1, 2$. If F_1 and F_2 are W-equivalent, then by Springer's theorem (cf. III.1.3), K_1 and K_2 are W-equivalent and also G-equivalent (by Theorem 3.1 and III.1.3). On the other hand, if F_1 and F_2 are G-equivalent, then K_1 and K_2 need not be G-equivalent. For example, take F_1 and F_2 to be fields with the same finite square class number and with the property that every binary form over each of them is universal. We know that the fields can be chosen to satisfy $s(F_1) = 1$ and $s(F_2) = 2$ and that they are strongly G-equivalent while not W-equivalent (cf. Remark 1.10). By Theorem III.1.3, we have

$$G(K_1) \cong G(F_1) \oplus W(F_1) \quad \text{and} \quad G(K_2) \cong G(F_2) \oplus W(F_2).$$

Now $G(F_1)$ and $G(F_2)$ are finitely generated isomorphic abelian groups, hence if $G(K_1) \cong G(K_2)$, we can cancel the isomorphic summands and obtain $W(F_1) \cong W(F_2)$, which is not the case. Hence K_1 and K_2 are not G-equivalent in spite of the strong G-equivalence of their residue class fields.

Chapter V

A Galois correspondence in the quadratic form theory

§ 1. The binary case. Let $B = B(F)$ be the set of equivalence classes of all binary quadratic forms over F which represent 1 over F. The set B can be made into an abelian group of exponent 2 by introducing the following law of composition:

$$\langle 1, a\rangle \times \langle 1, b\rangle = \langle 1, -ab\rangle. \tag{1.0.1}$$

The unit element in B is the hyperbolic plane $\langle 1, -1\rangle$. Observe that for φ and ψ in B we have

$$D(\varphi \times \psi) \supset D(\varphi) \cap D(\psi). \tag{1.0.2}$$

Indeed, if $c \in D(1, a) \cap D(1, b)$, then $(1, a) \approx c$ and $(1, b) \approx c$, hence $(1, -c) \approx -a$ and $-b$, hence $(1, -c) \approx (-a)(-b) = ab$. Thus $(1, -ab) \approx c$, i.e., $c \in D\big((1, a) \times (1, b)\big)$, as required.

For an n-dimensional quadratic form φ we denote by $d(\varphi)$ the discriminant of φ, that is

$$d(\varphi) = (-1)^{n(n-1)/2} \det \varphi \in g(F).$$

For a binary form $\varphi = (1, a)$ we have $d(\varphi) = -a$, and we easily check that $d\colon B(F) \to g(F)$ is a group isomorphism.

The set $U_2(F)$ of all universal forms in $B(F)$ is a subgroup of $B(F)$ (use (1.0.2) to prove that $U_2(F)$ is closed under $\times$). The law of composition (1.0.1) has been introduced in [28], where also some properties of $U_2(F)$ have been proved.

Consider the image of $U_2(F)$ under the discriminant isomorphism d. We have

$$\begin{aligned} d\big(U_2(F)\big) &= \{a \in g(F)\colon \langle 1, -a\rangle \in U_2(F)\} \\ &= \{a \in g(F)\colon \langle a, b\rangle \approx 1 \text{ for every } b \in g(F)\} \\ &= \left\{a \in g(F)\colon \left(\frac{a, b}{F}\right) \text{ splits for every } b \in g(F)\right\} \\ &= \operatorname{Rad} F, \end{aligned} \tag{1.0.3}$$

where Rad$F$ denotes Kaplansky's radical of the field F (cf. Kaplansky [11]). From this we obtain the following group isomorphism

$$B(F)/U_2(F) \cong g(F)/\mathrm{Rad}F. \tag{1.0.4}$$

Now consider the lattice $L(B)$ of all subgroups of $B = B(F)$ and the lattice $L(g)$ of all subgroups of $g = g(F)$. For any φ in B, the set $D(\varphi)$ is a subgroup of g, so for any subgroup H of B the set

$$V(H) = \bigcap_{\varphi \in H} D(\varphi) \tag{1.0.5}$$

is also a subgroup of g. We call $V(H)$ the value group of H. We have defined the mapping

$$V\colon L(B) \to L(g),$$

which has the following property: for any $H_1, H_2 \in L(B)$,

$$H_1 \subset H_2 \Rightarrow V(H_2) \subset V(H_1). \tag{1.0.6}$$

On the other hand, we can define

$$U\colon L(g) \to L(B)$$

by putting

$$U(h) = \{\varphi \in B\colon h \subset D(\varphi)\}. \tag{1.0.7}$$

Thus $U(h)$ is the set of forms which are universal on the subgroup h, i.e., the set of forms which represent every element of h. If φ and ψ belong to $U(h)$, then $h \subset D(\varphi) \cap D(\psi)$, and by (1.0.2) we have $h \subset D(\varphi \times \psi)$, i.e., $\varphi \times \psi \in U(h)$. Thus $U(h)$ is a subgroup of B. We observe that for any $h_1, h_2 \in L(g)$,

$$h_1 \subset h_2 \Rightarrow U(h_2) \subset U(h_1). \tag{1.0.8}$$

It is also clear that for any $H \in L(B)$ and $h \in L(g)$,

$$H \subset UV(H) \quad \text{and} \quad h \subset VU(h). \tag{1.0.9}$$

Now (1.0.6), (1.0.8) and (1.0.9) give the following result.

THEOREM 1.1. *For any field F, the mappings U and V define a Galois correspondence between the lattices $L(B(F))$ and $L(g(F))$.*

Let us try out the U and V maps on the four extreme elements of $L(g)$ and $L(B)$. For the least elements we have

$$U(\{1\}) = B \quad \text{and} \quad V(\langle 1, -1\rangle) = g \tag{1.1.1}$$

and for the greatest,

$$U(g) = U_2(F) \quad \text{and} \quad V(B) = \mathrm{Rad}F. \tag{1.1.2}$$

Of these, only the last one is not quite trivial. We have

$$\begin{aligned} V(B) &= \{a \in g\colon \langle 1, b\rangle \approx a \text{ for every } b \in g\} \\ &= \{a \in g\colon \langle 1, -a\rangle \in U_2(F)\} \\ &= \mathrm{Rad}F, \end{aligned}$$

by (1.0.3).

A natural consequence of the existence of a Galois correspondence between two lattices is the possibility of introducing the closure operation in these lattices.

DEFINITION 1.2. The subgroup $VU(h)$ of g is called the *closure of* h and is denoted $\mathrm{Cl}(h)$. A subgroup h of g is said to be *closed* if $h = \mathrm{Cl}(h)$. Similarly, for a subgroup H of B, $UV(H)$ is called the *closure of* H and denoted $\mathrm{Cl}(H)$, and H is said to be *closed* if $H = \mathrm{Cl}(H)$.

From (1.0.6), (1.0.8) and (1.0.9) we obtain immediately: For any $h, k \in L(g)$,

(1.2.1) $\quad h \subset \mathrm{Cl}(h); \quad h \subset k \Rightarrow \mathrm{Cl}(h) \subset \mathrm{Cl}(k); \quad \mathrm{Cl}\big(\mathrm{Cl}(h)\big) = \mathrm{Cl}(h).$

For any $H, K \in L(B)$,

(1.2.2) $\quad H \subset \mathrm{Cl}(H); \quad H \subset K \Rightarrow \mathrm{Cl}(H) \subset \mathrm{Cl}(K); \quad \mathrm{Cl}\big(\mathrm{Cl}(H)\big) = \mathrm{Cl}(H).$

THEOREM 1.3. *The mapping U restricted to the subset of closed subgroups of g becomes injective and maps closed subgroups of g onto closed subgroups of B. Similarly, V restricted to the subset of closed subgroups of B becomes injective and maps closed subgroups of B onto closed subgroups of g. Moreover, $U \circ V$ and $V \circ U$ are identities on the sets of closed subgroups of B and g, respectively.*

Proof. All the statements follow from Theorem 1.1 and from the general theory of Galois correspondences (cf. Kurosh [14], VI.11.1).

EXAMPLES. (1.3.1) A subgroup h of g is closed iff $h = V(H)$ for some H in $L(B)$. A subgroup H of B is closed iff $H = U(h)$ for some h in $L(g)$.

(1.3.2) The groups $g, B, \mathrm{Rad}F$ and $U_2(F)$ are always closed (use (1.1.1), (1.1.2) and (1.3.1)).

(1.3.3) For any φ in B we denote by H_φ the subgroup of B generated by φ. Thus $H_\varphi = \{1_B\}$ if φ is the hyperbolic plane and $H_\varphi = \{1_B, \varphi\}$ otherwise. The value group $D(\varphi)$ is always closed since $D(\varphi) = V(H_\varphi)$. We shall show later on that these are basic closed subgroups of g (Theorem 1.6).

(1.3.4) For any a in g we consider the subgroup $U(\{1, a\})$ of B, which is closed by (1.3.1). We have

$$\begin{aligned} U(\{1, a\}) &= \{\langle 1, b\rangle \in B\colon \langle 1, b\rangle \approx a\} \\ &= \{\langle 1, b\rangle \in B\colon -b \in D(1, -a)\} = d^{-1}\big(D(1, -a)\big), \end{aligned}$$

where $d\colon B \to g$ is the discriminant isomorphism.

(1.3.5) The binary form φ is said to be closed if the subgroup H_φ of B is closed, i.e., if $U(D(\varphi)) = H_\varphi$. If φ is universal, then $U(D(\varphi)) = U(g) = U_2(F)$, so that φ is closed iff $U_2(F) = H_\varphi$. Hence the hyperbolic plane is closed iff it is the unique universal binary form over F, and an anisotropic universal binary form is closed iff it is the unique anisotropic universal binary form over F (i.e., iff $u_2 = |U_2(F)| = 2$).

(1.3.6) $\mathrm{Rad}F$ and $U_2(F)$ are the smallest closed subgroups of g and B, respectively. Indeed, let h be any closed subgroup of g; then we have

$$\{1_g\} \subset h \Rightarrow U(1_g) \supset U(h) \Rightarrow \mathrm{Rad}F = VU(1_g) \subset VU(h) = h.$$

The second statement can be proved similarly.

(1.3.7) *For a field F the following statements are equivalent:*

(i) *Every binary form over F is universal.*

(ii) *B is the unique closed subgroup of B.*

(iii) *g is the unique closed subgroup of g.*

Proof. (i) implies that $U_2(F) = B$ and since $U_2(F)$ is the smallest closed subgroup of B, we obtain (ii). If (ii) holds, then by Theorem 1.3, g contains exactly one closed subgroup and by (1.3.2) it has to be g, i.e., we get (iii). Now (iii) and (1.3.2) imply that $g = \mathrm{Rad}F = V(B)$, hence we have (i).

For a family $\{H_i\}_{i\in I}$ of subgroups of B we denote by $\bigcup_{i\in I} H_i$ the subgroup of B generated by the union of sets H_i, $i\in I$, and the same notation is used for subgroups of g.

Proposition 1.4. (i) *For any family $\{H_i\}_{i\in I}$ of subgroups of B,*

$$V\Big(\bigcup_{i\in I} H_i\Big) = \bigcap_{i\in I} V(H_i).$$

(ii) *For any family $\{h_i\}_{i\in I}$ of subgroups of g,*

$$U\Big(\bigcup_{i\in I} h_i\Big) = \bigcap_{i\in I} U(h_i).$$

Proof. (i) We have $H_i \subset \bigcup_{i\in I} H_i$, hence $V(H_i) \supset V\big(\bigcup_{i\in I} H_i\big)$, for all $i\in I$, so that

$$\bigcap_{i\in I} V(H_i) \supset V\Big(\bigcup_{i\in I} H_i\Big). \tag{1.4.1}$$

Conversely, if $a \in \bigcap_{i\in I} V(H_i)$, then for every $i\in I$ and every $\varphi_i \in H_i$, we have $a\in D(\varphi_i)$. If $\varphi \in \bigcup_{i\in I} H_i$, then $\varphi = \varphi_{i_1} \times \ldots \times \varphi_{i_n}$, for some $i_1, \ldots, i_n \in I$, $n\in N$, $\varphi_{i_j} \in H_{i_j}$, $j = 1, \ldots, n$. Since $a\in D(\varphi_{i_j})$, $j = 1, \ldots, n$, we obtain, on using (1.0.2), $a\in D(\varphi)$. Thus $a\in V\big(\bigcup_{i\in I} H_i\big)$, which put together with (1.4.1) gives (i).

(ii) From $h_i \subset \bigcup_{i\in I} h_i$ it follows that $U(h_i) \supset U\big(\bigcup_{i\in I} h_i\big)$ for all $i\in I$, hence $\bigcap_{i\in I} U(h_i) \supset U\big(\bigcup_{i\in I} h_i\big)$. Assume now that $\varphi \in \bigcap_{i\in I} U(h_i)$; then $\varphi \in U(h_i)$ for all $i\in I$, and so $D(\varphi) \supset h_i$, for $i\in I$. From this we conclude that $D(\varphi) \supset \bigcup_{i\in I} h_i$ and so $\varphi \in U\big(\bigcup_{i\in I} h_i\big)$. Thus we have proved (ii).

COROLLARY 1.5. *The intersection of any family of closed subgroups of B (or g) is a closed subgroup of B (or g, respectively).*

Proof. If the subgroups H_i, $i\in I$, of B are closed, then there exist subgroups h_i, $i\in I$, of g such that $H_i = U(h_i)$, $i\in I$. Now $\bigcap_{i\in I} H_i = \bigcap_{i\in I} U(h_i) = U\big(\bigcup_{i\in I} h_i\big)$, and the intersection is closed by (1.3.1). The same argument applies for subgroups of g.

Remark. If H_1 and H_2 are subgroups of B and h_1 and h_2 are subgroups of g, then Proposition 1.4 asserts that

$$V(H_1 \cup H_2) = V(H_1) \cap V(H_2) \quad \text{and} \quad U(h_1 \cup h_2) = U(h_1) \cap U(h_2).$$

It can be easily checked that we have also

$$V(H_1 \cap H_2) \supset V(H_1) \cup V(H_2) \quad \text{and} \quad U(h_1 \cap h_2) \supset U(h_1) \cup U(h_2).$$

However, in general one cannot expect the equality here. Using the characterization of super-pythagorean fields by the behaviour of binary forms (given in Proposition 1.22 of [29]), it is easy to produce counter-examples for superpythagorean fields. Thus V and U are not, in general, lattice anti-homomorphisms. One can also ask under what circumstances, there exists, for any H_1 and H_2, an H such that $V(H_1) \cup V(H_2) = V(H)$. This question will be answered completely at the end of this section (cf. Propositions 1.9 and 1.10).

Now we give a characterization of closed subgroups of g and B.

THEOREM 1.6. (i) *A subgroup h of g is closed if and only if*

$$h = \bigcap_{i\in I} D(1, a_i), \quad \text{for some } a_i \in g,\ i\in I. \tag{1.6.1}$$

(ii) *A subgroup H of B is closed if and only if*

$$H = d^{-1}\Big(\bigcap_{i\in I} D(1, b_i)\Big), \quad \text{for some } b_i \in g,\ i\in I \tag{1.6.2}$$

(here d is the discriminant group isomorphism $d\colon B \to g$).

(iii) *Let H be a subgroup of B and $h = d(H)$. Then H is closed if and only if h is closed.*

Proof. (i) Suppose h is closed. Then $h = V(H)$ for a subgroup H of B. We can choose a basis $\{\varphi_i\}_{i\in I}$ for H and then we have $H = \bigcup_{i\in I} H_{\varphi_i}$. On using Proposition 1.4 (i) we get

$$h = V(H) = \bigcap_{i\in I} V(H_{\varphi_i}) = \bigcap_{i\in I} D(\varphi_i),$$

as required. Conversely, if h satisfies (1.6.1), then h is closed by (1.3.3) and Corollary 1.5.

(ii) Suppose H is closed. Then $H = U(h)$ for a subgroup h of g. Let $\{a_i\}_{i\in I}$ be a basis for the group h, so that $h = \bigcup_{i\in I} \{1, a_i\}$. We use Proposition 1.4 (ii) and Example (1.3.4) to obtain

$$H = U(h) = \bigcap_{i\in I} U\{1, a_i\} = \bigcap_{i\in I} d^{-1}\big(D(1, -a_i)\big) = d^{-1}\Big(\bigcap_{i\in I} D(1, -a_i)\Big),$$

which is (1.6.2). On the other hand, if (1.6.2) is satisfied, then as above $H = \bigcap_{i\in I} U\{1, -b_i\}$ and H is closed by (1.3.1) and Corollary 1.5.

(iii) follows immediately from (i) and (ii). ∎

In the case of pythagorean fields with finite square class number it is possible to show that the closed subgroups of g coincide with the value groups of some Pfister forms. This will follow from Theorem 1.6 (i) and the following lemma.

LEMMA 1.7. *Let F be a pythagorean field and let $a_1, \ldots, a_n$ be elements of F^* such that the group $h = D(1, a_1) \cap \ldots \cap D(1, a_n)$ is finite. Then there exists a Pfister form φ such that $h = D(\varphi)$.*

Proof. Pick up any basis $\{b_1, \ldots, b_m\}$ for h and put

$$\varphi = ((b_1, \ldots, b_m)).$$

Then the diagonal entries of φ coincide with all the elements of h, so that $h \subset D(\varphi)$. On the other hand, if $c \in D_F(\varphi)$, then c is the sum of elements of the form xy^2, where $x \in h$ and $y \in F^*$, and each of them is represented by all the forms $(1, a_i)$. Now the sets $D_F(1, a_i)$ are closed under addition since the field is pythagorean, hence $c \in h$. Thus $D(\varphi) \subset h$, which proves the lemma.

THEOREM 1.8. *Let F be a pythagorean field with a finite number of square classes.*

(i) *For every closed subgroup h of $g(F)$ there exists a Pfister form φ such that $h = D(\varphi)$.*

(ii) *For every closed subgroup H of $B(F)$ there exists a Pfister form φ such that $H = d^{-1}\big(D(\varphi)\big)$.*

Proof. (i) If h is closed, then by 1.6 (i), h is the intersection of a finite number of subgroups $D(1, a_i)$. By Lemma 1.7, h is the value group of a Pfister form.

(ii) The statement follows immediately from 1.8 (i) and Theorem 1.6.

Remark. The result 1.8 (ii) is due to A. Sładek who found a proof independent of Theorem 1.6.

We end this section with some remarks concerning the possibility of introducing a topology in the group g with the property that closed

subsets in the topology of g coincide with closed subgroups of g in the sense of Galois correspondence. Let us agree that the empty subset of g will also be counted as closed. Then the family C of subsets of g consisting of the empty set and of all closed subgroups of g has the following properties:

(1.8.1) The empty set and the whole set g belong to C.

(1.8.2) The intersection of any family of subsets belonging to C also belongs to C.

Here (1.8.1) follows from (1.3.2) and (1.8.2) from Corollary 1.5. In order that the family C defined a topology in g with the property that all closed subsets of g coincide with those of C, it is necessary and sufficient that the following condition be satisfied:

(1.8.3) The union of any two subsets of g belonging to C also belongs to C.

But it is well known that the union of two subgroups is a subgroup iff one of the two contains the other. Hence, (1.8.3) is satisfied if and only if the family C is totally ordered, that is, if for any closed subgroups h_1 and h_2 of g, we have either $h_1 \subset h_2$ or $h_2 \subset h_1$.

We shall show that this happens only in some special cases.

PROPOSITION 1.9. *For a non-real field F, the family of closed subgroups of $g = g(F)$ is totally ordered if and only if every binary quadratic form over F is universal (iff g is the unique closed subgroup of g, by Example* (1.3.7)).

Proof. The sufficiency is obvious, so we prove only the necessity. If the closed subgroups of g are totally ordered, then

(1.9.1) for any $a, b \in g$, either $D(1, a) \subset D(1, b)$ or $D(1, b) \subset D(1, a)$,

since $D(1, a)$ is always closed, by (1.3.3).

First observe that (1.9.1) is impossible if the stufe $s = s(F)$ is at least 4. For then we have $-1 = a + b$, where $a, b \in D_F\big((s/2)\langle 1\rangle\big)$, and we shall prove that $a \notin D_F(1, b)$ and $b \notin D_F(1, a)$.

Indeed, if $a = x^2 + by^2$, then

$$-1 = a + b = x^2 + b(y^2+1) \in D_F\big((\tfrac{1}{2}s+1)\langle 1\rangle\big),$$

so that $s \leqslant \frac{1}{2}s + 1$, which contradicts $s \geqslant 4$. Hence $D(1, a)$ is not contained in $D(1, b)$ and similarly $D(1, b)$ is not contained in $D(1, a)$.

Now consider the two remaining values of s.

Suppose $s = 1$. Take any a and b in g and assume that $D(1, a) \subset D(1, b)$. Then $(1, b) \approx a$, and since $s = 1$, we get $(a, b) \approx 1$. Similarly, $D(1, b) \subset D(1, a)$ implies that $(a, b) \approx 1$. Thus every binary form represents 1 and this is equivalent to saying that every binary form is universal.

Now assume $s = 2$. We first show that the form $(1, 1)$ is universal. If not, pick up an a which is not in $D(1, 1)$. Then also $D(1, a)$ is not contained in $D(1, 1)$. On the other hand, if (1.9.1) holds, then we must have $D(1, 1) \subset D(1, a)$, and then $(1, a) \approx -1$, hence $(1, 1) \approx -a$, hence $(1, 1) \approx (-1)(-a) = a$, contrary to the choice of a. Thus $(1, 1)$ is universal. Now take any a, b in g and assume that $D(1, a) \subset D(1, b)$. Then we have

$$(1, b) \cong (a, ab),$$

and by the universality of $(1, 1)$ also

$$(1, b) \cong (-1, -b).$$

Using these equivalences we obtain

$$(1, a, b, ab) \cong (1, b, -1, -b) \cong (1, -1, 1, -1).$$

Thus every 2-fold Pfister form is hyperbolic and this implies that every binary form is universal. ■

Now we settle the case of real fields satisfying (1.8.3).

PROPOSITION 1.10. *For a real field F, the family of closed subgroups of $g = g(F)$ is totally ordered if and only if the following four conditions are satisfied:*

(i) *F has just one ordering,*

(ii) *every positive element of F is a sum of two squares,*

(iii) *every indefinite binary form is universal,*

(iv) *every positive definite binary form represents all positive elements of the field.*

Proof. Suppose at first that the set of closed subgroups of g is totally ordered. Then (1.8.4) holds. Take any $a \in F^*$. If $D(1, a) \subset D(1, -a)$, then $(1, -a) \approx a$ and consequently $a \in D_F(1, 1)$. If $D(1, -a) \subset D(1, a)$, then $(1, a) \approx -a$ and we obtain $-a \in D_F(1, 1)$. Thus $D_F(1, 1)$ is a subgroup of index 2 in F^*. If P is any ordering of F, then $D_F(1, 1) \subset P$, and since P is also a subgroup of index 2 of F^*, we must have $P = D_F(1, 1)$. So we have proved (i) and (ii).

To prove (iii), take any indefinite binary form $(a, -b)$, say, where a and b are positive. If $D(1, a) \subset D(1, b)$, then $(1, b) \approx a$ and so $(1, b) \cong (a, ab)$, whence $(a, -b) \approx 1$. If $D(1, b) \subset D(1, a)$, then analogously $(-a, b) \approx 1$. But we shall prove in a moment that

(1.10.1) for any $a, b \in D(1, 1)$, we have $(a, -b) \cong (-a, b)$

and from this and $(-a, b) \approx 1$ it follows that $(a, -b) \approx 1$. Thus in any case every indefinite binary form represents 1, whence every such form is universal.

To complete the proof of (iii) it remains to prove (1.10.1). Take $a, b \in D(1,1)$ and assume $D(1,-a) \subset D(1,-b)$. Then

$$D(1,-a) = D(1,-a) \cap D(1,-b) \subset D(1,-ab),$$

by (1.0.2), and so $(1,-ab) \approx -a$, hence $(1,-ab) \cong (-a,b)$. On the other hand $ab \in D(1,1)$ so that $(1,-ab) \approx -1$ and $(1,-ab) \cong (-1,ab)$. These two equivalences prove (1.10.1).

Now, (iv) follows from (iii). Indeed, it is sufficient to prove that the forms $(1,a)$, where $a \in D(1,1)$, represent every element of $D(1,1)$. So take $b \in D(1,1)$. Then $(1,-b)$ is universal by (iii), hence $(1,-b) \approx -a$, whence $(1,a) \approx b$, as required.

Now assume that a real field F satisfies the conditions (i) through (iv). If φ is any form in B, then $D(\varphi) = D(1,1)$ for definite φ and $D(\varphi) = g$ for indefinite φ. Any closed subgroup of g is the intersection of some $D(\varphi)$ (Theorem 1.6), so there are just two closed subgroups: $D(1,1)$ and g, and the assertion follows trivially. ∎

COROLLARY 1.11. *For a field F, the family of closed subgroups of $g = g(F)$ is totally ordered if and only if there are at most two closed subgroups of g.*

Proof. For a non-real field this has been observed in Proposition 1.9. If the field is real and the closed subgroups are totally ordered, then by Proposition 1.10 (iii) and (iv), there are only two different value sets for all binary forms in $B(F)$, namely g and $D(1,1)$. Hence these are the only closed subgroups of g (by Theorem 1.6).

Examples of fields with the property of Proposition 1.9 are well known: see Cordes [2], p. 407; Elman and Lam [6], (3.8); and [28], Theorem 2.3, for examples of such fields with any given finite square class number and Pfister [23], Satz 20, for an example of a field with the property of Proposition 1.9 and infinite square class number. Real fields with any given finite square class number and the properties stated in Proposition 1.10 have been constructed in [29], § 4, Example 2.5.I.

§ 2. A generalization. In this section we shall show that the basic facts of § 1 carry over to the more general case of linked n-fold Pfister forms. Recall that two n-fold Pfister forms φ and ψ are said to be linked if there exist an $(n-1)$-fold Pfister form σ and two 1-fold Pfister forms τ_1 and τ_2 such that $\varphi \cong \sigma \otimes \tau_1$ and $\psi \cong \sigma \otimes \tau_2$. Thus φ and ψ are linked iff there exist $a_1, \ldots, a_{n-1}, a, b$ in F^* such that $\varphi \cong ((a_1, \ldots, a_{n-1}, a))$ and $\psi \cong ((a_1, \ldots, a_{n-1}, b))$. A necessary and sufficient condition for φ and ψ to be linked is that the Witt index of the form $\varphi \perp -\psi$ be 2^{n-1} (cf. Elman and Lam [4], Proposition 4.4). The Pfister forms τ_1 and τ_2 above are by no means unique. In fact, for a Pfister form σ,

$$\sigma \otimes (1,a) \cong \sigma \otimes (1,b) \Leftrightarrow ab \in D(\sigma). \tag{2.0.1}$$

For an $(n-1)$-fold Pfister form σ we denote by $B(\sigma; F)$ or $B(\sigma)$ the set of equivalence classes of n-fold Pfister forms φ which can be written as $\varphi = \sigma \otimes \tau$, where τ is a 1-fold Pfister form. Thus $B(\sigma)$ is the set of equivalence classes of all pairwise linked n-fold Pfister forms having the same linkage form σ. We have $B(\langle 1\rangle; F) = B(F)$, the group of binary equivalence classes introduced in § 1, and for any Pfister form σ we can also write

$$B(\sigma; F) = \langle \sigma \rangle \cdot B(F).$$

For two forms $\varphi = \sigma \otimes (1, a)$ and $\psi = \sigma \otimes (1, b)$ we define their product by

$$\varphi \times \psi = \sigma \otimes (1, -ab). \tag{2.0.2}$$

First let us observe that $\varphi \times \psi$ does not depend on the choice of a and b. Indeed, if $\varphi \cong \sigma \otimes (1, a) \cong \sigma \otimes (1, a')$ and $\psi \cong \sigma \otimes (1, b) \cong \sigma \otimes (1, b')$, then, by (2.0.1), we have $aa' \in D(\sigma)$ and $bb' \in D(\sigma)$, hence $(-ab)(-a'b') \in D(\sigma)$, hence $\sigma \otimes (1, -ab) \cong \sigma \otimes (1, -a'b')$.

More generally, if φ has two diagonalizations $((a_1, \ldots, a_{n-1}, a))$ and $((a'_1, \ldots, a'_{n-1}, a'))$ and ψ has diagonalizations $((a_1, \ldots, a_{n-1}, b))$ and $((a'_1, \ldots, a'_{n-1}, b'))$, then

$$((a_1, \ldots, a_{n-1}, -ab)) \cong ((a'_1, \ldots, a'_{n-1}, -a'b')). \tag{2.0.3}$$

Indeed, by the Main Theorem of Elman and Lam [4] (Theorem 3.2), we have

$$l(-a_1) \ldots l(-a_{n-1}) l(-a) = l(-a'_1) \ldots l(-a'_{n-1}) l(-a') \quad \text{in} \quad k_n F$$

and

$$l(-a_1) \ldots l(-a_{n-1}) l(-b) = l(-a'_1) \ldots l(-a'_{n-1}) l(-b') \quad \text{in} \quad k_n F,$$

where $k_n F$ is Milnor's $K_n F$ group modulo $2K_n F$ (for details see Milnor [20] and Elman and Lam [4]). Now, adding the two equalities gives

$$l(-a_1) \ldots l(-a_{n-1}) \big(l(-a) + l(-b)\big) = l(-a'_1) \ldots l(-a'_{n-1}) \big(l(-a') + l(-b')\big)$$

in $k_n F$, hence

$$l(-a_1) \ldots l(-a_{n-1}) l(ab) = l(-a'_1) \ldots l(-a'_{n-1}) l(a'b') \quad \text{in} \quad k_n F.$$

Using the Main Theorem again we obtain (2.0.3).

Thus the multiplication (2.0.2) is well defined on equivalence classes and makes $B(\sigma)$ into an abelian group of exponent two. The identity element of this group is the hyperbolic class $\langle \sigma \otimes (1, -1)\rangle$. The group $B(\sigma)$ turns out to be a homomorphic image of the group $g = g(F)$. Indeed, the mapping $g(F) \to B(\sigma; F)$ defined by $a \mapsto \langle \sigma \otimes (1, -a)\rangle$ is a surjective group homomorphism, and by (2.0.1), its kernel coincides with $D(\sigma)$.

Thus we have the following group isomorphism

$$B(\sigma; F) = g(F)/D(\sigma). \tag{2.0.4}$$

An immediate consequence of this is that $B(\sigma; F)$ is trivial iff σ is universal.

In the case when σ is a 1-fold Pfister form there is a natural interpretation for the group $B(\sigma; F)$ in terms of the Brauer group $\mathrm{Br}(F)$ of the field F. For the quaternion algebra $(a, b/F)$ denote by $[a, b]$ the corresponding element of $\mathrm{Br}(F)$. Let us introduce the following notation: for any $c \in g(F)$,

$$Q(c) = \{[c, x] \in \mathrm{Br}(F) : x \in g\}.$$

Obviously, $Q(c)$ is a subgroup of $\mathrm{Br}(F)$. Now, the mapping $B(\langle 1, -c\rangle; F) \to Q(c)$ defined by $\langle 1, -c, -a, ac\rangle \mapsto [c, a]$ is a group isomorphism. Indeed, its bijectivity is well known (cf. O'Meara [22], 57 : 8, p. 146) and one verifies immediately that it preserves the multiplication, too.

Now let us turn to the main subject of this section. In order to start the theory of § 1 we have to check the crucial property (1.0.2) of the law of composition. We shall prove that for any two linked Pfister form φ and ψ we have

$$D(\varphi \times \psi) \supset D(\varphi) \cap D(\psi). \tag{2.0.5}$$

Assume $c \in D(\varphi) \cap D(\psi)$. Then the forms $\varphi \otimes (1, -c)$ and $\psi \otimes (1, -c)$ are isotropic and it is sufficient to prove that $(\varphi \times \psi) \otimes (1, -c)$ is isotropic.

We have $\varphi = \sigma \otimes (1, a)$, $\psi = \sigma \otimes (1, b)$ for a Pfister form σ and we put $\eta = \sigma \otimes (1, -c)$.

Since $\varphi \otimes (1, -c)$ and $\psi \otimes (1, -c)$ are isotropic, there exist non-zero vectors u, v, x and y such that

$$\eta(u) + a\eta(v) = 0 \quad \text{and} \quad \eta(x) + b\eta(y) = 0.$$

We may assume that $\eta(u) \neq 0$ and $\eta(x) \neq 0$ (if $\eta(u) = 0$, then η is isotropic, hence it represents everything and we can choose v to be any anisotropic vector and pick up u to satisfy $\eta(u) = -a\eta(v)$).

Hence $\eta(u) = -a\eta(v)$ and $\eta(u)\big(\eta(x) + b\eta(y)\big) = 0$, so that

$$\eta(u)\eta(x) - ab\eta(v)\eta(y) = 0.$$

Now η is a Pfister form, hence there exist vectors t and z such that $\eta(u)\eta(x) = \eta(z)$ and $\eta(v)\eta(y) = \eta(t)$ and we obtain

$$\eta(z) - ab\eta(t) = 0 \quad \text{and} \quad \eta(z) \neq 0.$$

This shows that $\eta \otimes (1, -ab) = (\varphi \times \psi) \otimes (1, -c)$ is isotropic as we wanted. Thus we have proved the assertion (2.0.5).

Now we can define the mappings V and U by using the formulas (1.0.5) and (1.0.7) and show that they define a Galois correspondence between the subgroups of $B(\sigma)$ and g.

Chapter VI

Field constructions

In the classification of Grothendieck groups for fields with $q \leqslant 8$ given in [29] there are two cases where the existence of fields is not known. The two cases are characterized by the following values of field invariants:

(A) $q = 8, s < \infty, q_2 = 8, 2 \leqslant u_2 < 8$ (the type 2.4.II of [29]),

(B) $q = 8, s = \infty, q_2 = 4, u_2 = 1$ (the type 2.5.II of [29]).

Here $q_2 = |D(1,1)|$ and u_2 is the number of equivalence classes of universal binary forms over the field.

In this chapter we want to prove that the existence of a field satisfying (B) would imply the existence of a field satisfying (A); in fact, a suitable quadratic extension of a field of the second type satisfies (A).

THEOREM 1. *Let F be a field satisfying* (B) *and let $a \in F$ be a non-square which is the sum of two squares in F. Then the field $K = F(\sqrt{-a})$ satisfies* (A).

Proof. Suppose F satisfies (B). Then F is a real field and $D_F(1,1)$ is a subgroup of index 2 of F^*, hence $D_F(1,1)$ constitutes the unique ordering of the field F. We can write

$$g(F) = \{1, -1\} \times \{1, a\} \times \{1, b\}, \quad \text{where} \quad a, b \in D(1,1).$$

The norm-form of the extension K/F is $(1, a)$ and we have $D(1, a) = \{1, a\}$. Indeed, $(1, a)$ represents only positive elements of F and if $(1, a)$ represented b, then the form $(1, -b)$ would be universal, contrary to $u_2(F) = 1$. By Lemma 4.3 of [29] we obtain

$$g(K) = \{1, -1\} \times \{1, b\} \times \{1, a\}, \quad \text{where} \quad a^2 = -a. \tag{1.1}$$

Thus $q(K) = 8$ and $1 < s < \infty$; in fact, $s = 2$, since from $a = x^2 + y^2$ we obtain

$$-1 = (x/a)^2 + (y/a)^2. \tag{1.2}$$

To prove K satisfies (A) it remains to establish $q_2 = 8$ and $u_2 < 8$, since $u_2 \geqslant 2$ is a consequence of $q_2 = 8$ and $s = 2$ (these imply that $(1, 1)$ and $(1, -1)$ are two non-equivalent universal forms). We first prove $u_2(K) < 8$. It suffices to show that $(1, b)$ is not universal over K. The

form $(1, b)$ does not represent $a = N_{K/F}(\alpha)$ over F (since otherwise, $(1, -a)$ would be a second universal form over F, contrary to (B)), and since

$$N_{K/F}\big(D_K(1, b)\big) \subset D_F(1, b)$$

by Corollary 2.2.7 of Scharlau [24] (cf. also Lorenz [17], 10.6), it cannot represent α over K. Thus $(1, b)$ is not universal over K and $u_2(K) < 8$.

We offer also a direct argument which proves the non-universality of $(1, b)$. This works as follows. If $(1, b)$ represented α, then we would have

$$(x + y\alpha)^2 + b(z + t\alpha)^2 = \alpha,$$

for appropriate x, y, z, t (not all zero) from F. This implies

$$x^2 - ay^2 + bz^2 - abt^2 = 0,$$

that is, the Pfister form $(1, -a, b, -ab)$ is isotropic over F, hence $(1, -ab) \cong (a, -b)$. Now $(1, -ab)$ represents -1, since ab is the sum of two squares, so that $(1, -ab)$ represents all the basis elements of $g(F)$, hence it is universal, contrary to $u_2(F) = 1$. In order to prove $q_2(K) = 8$ we need a lemma.

LEMMA 2. *Let F be any field and d a non-zero element of F. If $D_F(1, d) \cup \cup -D_F(1, d) = F^*$, then for $a \in F^*$ and $\alpha^2 = -a$ we have:*

$$a \in D_F(1, d) \Rightarrow a \in D_{F(\alpha)}(1, d).$$

Let us first deduce $q_2(K) = 8$ from the lemma. Put $d = 1$, then clearly

$$F^* = D_F(1, 1) \cup -D_F(1, 1);$$

hence by the lemma, $a \in D_K(1, 1)$. Now $b \in D_F(1, 1) \subset D_K(1, 1)$ and $-1 \in D_K(1, 1)$ by (1.2); hence from (1.1) we see that the form $(1, 1)$ represents all the basis elements of $g(K)$, hence it is universal, and $q_2(K) = 8$.

Proof of Lemma 2. Assume $a = c^2 + de^2$ and consider first the case where $c \neq 0$. By the hypothesis, either $2c \in D_F(1, d)$ or $-2c \in D_F(1, d)$ and we choose c so that $2c \in D_F(1, d)$. Thus

$$2c = y^2 + dt^2, \quad y, t \in F,$$

and

$$a(y^2 + dt^2) = (c^2 + de^2)(y^2 + dt^2) = x^2 + dz^2, \tag{2.1}$$

where $x = cy + det$, $z = ct - ey$.

Now observe that

$$2xy + 2dzt = 2cy^2 + 2cdt^2 = 4c^2. \tag{2.2}$$

Put $X = x/2c$, $Y = y/2c$, $Z = z/2c$, $T = t/2c$; then by (2.1) we have

$$X^2 - aY^2 + dZ^2 - adT^2 = 0,$$

and by (2.2),

$$2XYa + 2dZTa = a.$$

On adding we obtain

$$(X + Ya)^2 + d(Z + Ta)^2 = a,$$

as required.

Now consider the case where $c = 0$, i.e., $a = de^2$. Then $(1, d) \cong (1, a)$ and it suffices to show that $a \in D_{F(a)}(1, a)$. This follows immediately from the identity

$$\big(a + (1/4a)\,a\big)^2 + a\big((1/4a) + a\big)^2 = a.$$

This finishes the proof of Lemma 2 and of Theorem 1.

Chapter VII

Open problems

We collect here ten problems which are strictly connected with the contents of the preceding chapters. We begin with questions concerning the group structure of $G(F)$ and $W(F)$. From the results of Knebusch–Rosenberg–Ware ([12], Proposition 3.19) it follows that, for any field F, $W(F) = V \oplus W^t(F)$, where V is free. This suggests the following two questions.

PROBLEM 1. Is the Witt group $W(F)$ (or equivalently $G(F)$, or $W^t(F)$, or $G^t(F)$) always a direct sum of cyclic groups?

PROBLEM 2. Characterize the fields F with the property that rank $V = |X|$, where X is the set of orderings of the field F.

The first question can be answered in the affirmative for: (i) any non-real field F, (ii) any field F with the property that the group $G^t(F)$ is countable, and (iii) for any field with finite t-invariant (the minimal number of terms needed for representing any totally positive element as the sum of squares).

According to Theorem III.1.4, fields with finite number of orderings have the property stated in the second question. But the field $F = Q(\sqrt{2}, \sqrt{3}, \ldots, \sqrt{p}, \ldots)$, where p runs through all the prime numbers, fails to have the above property. Indeed, X is uncountable in this case, while $W(F)$, and the more V, is countable.

PROBLEM 3. What are the values actually taken on by the rank of $G(F)$ for fields with given square class number q? And the same for torsion free rank of $G(F)$.

The first question is motivated by Theorem III.3.5. As to the second question, by Theorem III.1.4, the torsion free rank of $G(F)$ equals to the number r of orderings of F plus one. Thus the problem is to determine the values of $r = r(F)$, where F runs through real fields with given square class number q. For the estimates for r see [29], Proposition 1.12 and Proposition 1.22.

PROBLEM 4. How many classes of G-equivalent fields with given

square class number are there? The same for the other equivalences. Give estimates if not exact numbers.

For fields with $q = 1, 2, 4$ the corresponding numbers are 1, 2, 5 and for $q = 8$ we have at least 11 and at most 13 classes of G-equivalent fields (cf. [29], Theorems 2.1 through 2.5 and § 4).

PROBLEM 5. Investigate the interrelations between GR-equivalence of fields and strong G- and strong GR-equivalences. In particular, does GR-equivalence imply strong G-equivalence? Does GR-equivalence coincide with strong GR-equivalence? Do the two strong equivalences coincide?

PROBLEM 6. Investigate the behaviour of the various types of field equivalences under some field extensions. For instance, if F and K are strongly G-equivalent, $t\colon g(F)\to g(K)$ is the corresponding bijection (cf. Theorem IV.1.5) and a is a non-square in F, are the quadratic extensions $F(\sqrt{a})$ and $K\left(\sqrt{t(a)}\right)$ strongly G-equivalent?

PROBLEM 7. Is it possible to introduce a law of composition on the set of equivalence classes of n-fold Pfister forms to make it into a group with the property that $D(\varphi \times \psi) \supset D(\varphi) \cap D(\psi)$?

For $n = 1$ and for n-fold linked Pfister forms this has been done in Chapter V.

PROBLEM 8. Investigate the properties of the number of closed subgroups of $g(F)$ (in the meaning of Chapter V). Describe the connections with other field invariants.

PROBLEM 9. Do there exist the two fields characterized by conditions (A) and (B) of Chapter VI?

PROBLEM 10. Given any power of two 2^n, does there exist a field with finite square class number q and $u_2 = 2^n$? (u_2 is the number of equivalence classes of universal binary forms over the field).

In this context we recall that changing in the above u_2 into s, the stufe, we obtain another unsolved problem (cf. Lam [15], p. 333).

References

[1] J. K. Arason und A. Pfister, *Beweis des Krullschen Durchschnittsatzes für den Wittring*, Invent. Math. 12 (1971), pp. 173–176.

[2] C. M. Cordes, *The Witt group and the equivalence of fields with respect to quadratic forms*, J. Algebra 26 (1973), pp. 400–421.

[3] R. Elman, *Round forms over real algebraic function fields in one variable*, Proc. Amer. Math. Soc. 41 (1973), pp. 431–436.

[4] R. Elman and T. Y. Lam, *Pfister forms and K-theory of fields*, J. Algebra 23 (1972), pp. 181–213.

[5] — — *Quadratic forms over formally real fields and pythagorean fields*, Amer. J. Math. 94 (1972), pp. 1155–1194.

[6] — — *Quadratic forms and the u-invariant, II*, Invent. Math. 21 (1973), pp. 125–137.

[7] R. Elman, T. Y. Lam and A. Prestel, *On some Hasse principles over formally real fields*, Math. Zeitschr. 134 (1973), pp. 291–301.

[8] L. Fuchs, *Infinite Abelian Groups*, vol. I, Academic Press, New York and London 1970.

[9] D. K. Harrison, *Witt Rings*, University of Kentucky Notes, Lexington 1970.

[10] J. S. Hsia and R. P. Johnson, *Round and group quadratic forms over global fields*, J. Number Theory 5 (1973), pp. 356–366.

[11] I. Kaplansky, *Fröhlich's local quadratic forms*, J. Reine Angew. Math. 239/240 (1969), pp. 74–77.

[12] M. Knebusch, A. Rosenberg, and R. Ware, *Structure of Witt rings and quotients of abelian group rings*, Amer. J. Math. 94 (1972), pp. 119–155.

[13] M. Kula, *Ordered fields and quadratic forms over pythagorean fields*, Uniw. Śląski w Katowicach Prace Naukowe — Prace Mat. 7 (1977), pp. 13–21.

[14] A. G. Kurosh, *Lectures on General Algebra*, Chelsea, New York 1963.

[15] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, Benjamin, Reading 1973.

[16] S. Lang, *Algebra*, 3rd ed., Addison–Wesley, Reading 1971.

[17] F. Lorenz, *Quadratische Formen über Körpern*, Lecture Notes in Mathematics No. 130, Springer, Berlin 1970.

[18] F. Lorenz und J. Leicht, *Die Primideale des Wittschen Ringes*, Invent. Math. 10 (1970), pp. 82–88.

[19] M. Marshall, *Round quadratic forms*, Math. Zeitschr. 140 (1974), pp. 255–262.

[20] J. Milnor, *Algebraic K-theory and quadratic forms*, Invent. Math. 9 (1970), pp. 318–344.

[21] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Springer, Berlin–Heidelberg–New York 1973.

[22] O. T. O'Meara, *Introduction to Quadratic Forms*, 2nd ed., Springer, Berlin–Heidelberg–New York 1971.

[23] A. Pfister, *Quadratische Formen in beliebigen Körpern*, Invent. Math. 1 (1966), pp. 116–132.

[24] W. Scharlau, *Quadratic Forms*, Queen's Papers on Pure and Applied Mathematics No. 22, Kingston, Ont., 1969.

[25] A. Sładek, *Grothendieck groups of quadratic forms over formally real fields*, Uniw. Śląski w Katowicach Prace Naukowe — Prace Mat. 5 (1974), pp. 41–47.

[26] T. A. Springer, *Quadratic forms over fields with a discrete valuation, I*, Indag. Math. 17 (1955), pp. 352–362.

[27] K. Szymiczek, *Grothendieck groups of quadratic forms and G-equivalence of fields*, Proc. Cambridge Philos. Soc. 73 (1973), pp. 29–36. Corrigendum, ibid. 74 (1973), p. 199.

[28] — *Universal binary quadratic forms*, Uniw. Śląski w Katowicach Prace Naukowe — Prace Mat. 5 (1974), pp. 49–57.

[29] — *Quadratic forms over fields with finite square class number*, Acta Arith. 28 (1975), pp. 195–221.

[30] — *A structure theorem for Grothendieck group of quadratic forms over a field*, Colloquia Mathematica Societatis János Bolyai, Vol. 13, Topics in Number Theory, Debrecen (Hungary), 1974, North-Holland Publ. Co., Amsterdam–Oxford–New York 1976, pp. 389–397.

[31] E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. 176 (1937), pp. 31–44.