Multirings and The Chamber of Secrets: relationships between abstract theories of quadratic forms

Kaique Matias de Andrade Roberto

Dissertação apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do título
de
Mestre em Ciências

Área de Concentração: Matemática

Orientador: Prof. Dr. Hugo Luiz Mariano

Data da defesa: 20 de fevereiro de 2019

Multirings
and The Chamber of Secrets:
relationships between
abstract theories of quadratic forms

Esta versão da dissertação contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa da versão original do trabalho, realizada em 20/02/2019. Uma cópia da versão original está disponível no Instituto de Matemática e Estatística da Universidade de São Paulo.

Comissão Julgadora:

- Prof. Dr. Hugo Luiz Mariano (orientador) - IME-USP
- Prof. Dr. Maximo Alejandro Dickmann - UP
- Prof. Dr. Francisco Miraglia Neto - IME-USP
- Prof. Dr. Peter Arndt - UO (Suplente)
- Prof. Dr. Luan Alberto Ferreira - IFSP (Suplente)
- Prof. Dr. Daniel Levcovitz - ICMC-USP (Suplente)

Agradecimentos

Após essa longa jornada, com um acúmulo de várias noites sem dormir e litros incontáveis de café, não poderia deixar de fazer vários agradecimentos (claro, com a minha dose característica de drama).

Primeiro de tudo, a inspiração e motivação para este trabalho veio dos três homens da minha vida: meu pai, José Roberto, e meus dois irmãos, Nicolas (Bill) e Lucas. E se a inspiração veio destes três gigantes, não poderia deixar de agradecer a mais estas duas pessoas: Tio Edilson e Tia Helena, que cuidaram de mim com grande carinho durante muitos anos cruciais da minha vida. Uma pena que o tio Edilson faleceu... embora certamente ele esteja me acompanhando de seu lugarzinho lá no céu, tenho certeza que me diria orgulhosamente "eu sabia que você ia chegar lá! Tu é doido mas eu sempre acreditei em você!".

E falando daqueles que sempre acreditaram em mim, agradeço com um carinho especial aos meus grandes amigos Daniel de Brito Reis, Marcos Rafael Nogueira Cavalcante (Monsenhor), Ricardo Murça (Amém!), Alexandre Ribeiro e Luciana Bonatto e aos cruspianos Rafael, Robson GR e Stephany Somekawa. É um prazer inenarrável poder fazer minha jornada ao lado de vocês! Obrigado pela ajuda, apoio e paciência com este Mumuzinho durante todos estes anos!

Também agradeço ao meu amigo e orientador, Hugo Luiz Mariano, que além de ser um matemático excepcional, é uma pessoa extraordinária e um orientador inspirador. Tenho aprendido muito durante os nossos anos de trabalho na iniciação científica e no mestrado. Quando crescer, quero ser um matemático que nem você!

Falando de inspiração, agradeço aqueles que me inspiraram a ser matemático: os professores Osmar Antônio de Lima e Régis Silva e a todos os professores da Escola Estadual Dr. Mário Toledo de Moraes. Se hoje eu falo de formas quadráticas com paixão, é porque o precedente veio da paixão que vocês me inspiraram em suas aulas.

Agradeço também ao pessoal do Instituto do Câncer do Estado de São Paulo, Icesp, pelo simples fato de que é por causa do trabalho de vocês que eu ainda estou vivo (um grande abraço para a Fernanda Bonani e para o Paulo Antônio). E falando em sobrevivência, não poderia deixar de agradecer à CAPES e OBMEP, pelo financiamento e suporte ao longo destes últimos 11 anos. Deixo também um grande abraço para todos os funcionários e terceirizados do IME-USP. A matemática desse instituto só existe por conta do trabalho diário e muitas vezes silencioso de vocês.

Agora deixo vocês com a leitura deste trabalho porque minhas lágrimas de gratidão já estão molhando meu teclado...

Resumo

ROBERTO, K. M. A. **Multianeis e a Câmara Secreta: relações funtoriais entre teorias abstratas de formas quadraticas**. 2019. 285 f. Dissertação (Mestrado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2019.

O principal objetivo deste trabalho é estabelecer precisamente quais são as conexões funtoriais entre as teorias abstratas de formas quadráticas, criando uma via introdutória entre a teoria clássica e as abstratas durante este processo. Há uma gama de literatura desenvolvida tanto na teoria clássica quanto nas abstratas, mas nenhuma intercalando-as "geograficamente". Nesta perspectiva, discutiremos os aspectos fundamentais da teoria clássica e reduzida de formas quadráticas, encapsulando as teorias das Estruturas Quaterniônicas, Esquemas de Cordes, Anéis de Witt Abstratos, Espaços de Ordens Abstratos, Grupos Especiais, Espectro Real Abstratos e Semigrupos Reais em um quadro funtorial, inserindo os novos elementos envolvendo a teoria recente dos Multianéis e Multi-corpos.

Palavras-chave: Multi-anéis, grupo especial, semigrupo real, quadro funtorial.

Abstract

ROBERTO, K. M. A. **Multirings and The Chamber of Secrets: relationships between abstract theories of quadratic forms**. 2019. 285 f. Dissertação (Mestrado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2019.

The aim of this work is to establish precisely what are the functorial connections between the abstract theories of quadratic forms, as well as, to create a short and introductory path from the classic theory to the abstract ones. There is a large amount of literature developed about classic and abstract theories but does note relate them "geographically". In this perspective, we discuss the fundamental aspects of the classic and reduced theory of quadratic forms, and sum up the theories of Quaternionic Structures, Cordes Schemes, Abstract Witt Rings, Abstract Ordering Spaces, Special Groups, Abstract Real Spectra and Real Semigroups in a functorial picture, inserting the new aspects involve the recent theory of Multirings and Multifields.

Keywords: multirings, special group, real semigroup, functorial picture.

Contents

Abbreviation List

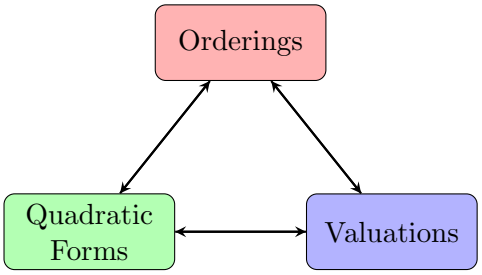
AOR	Abstract Ordering Space
ARS	Abstract Real Spectra
BA	Boolean Algebra
CS	Cordes Scheme
MF	Multifield
MR	Multiring
PRS	Pre-realsemigroup
PSG	Pre-special Group
QS	Quaternionic Structure
RS	Realsemigroup
RSG	Reduced Special Group
SG	Special Group
TS	Ternary Semigroup

Introduction

The aim of this present work is establish precisely what are the functorial connections between the abstract theories of quadratic forms as soon as to create a short and introductory path from the classic theory to the abstract ones. This is an important contribution, since there are an amount of good literature developed in classic and abstract theories but no one interchanging them "geographically".

Chapter 1 is a "crash course" in algebraic theory of quadratic forms, in the sense to provide a good introduction to quadratic forms for the readers that are not familiar with this subject (and it is crucial since we will work with abstract versions of quadratic forms).

In chapter 2 we talk about the very first "abstract theory" of quadratic forms, the reduced theory. It is nothing more than a theory of quadratic forms "in the point of view" of a fixed preordering. Almost all of the results in chapter 1 is immediated translated in this new context. Beside this, a new phenomena appears (we call it the "Lam's triangle"), that is the interchanging of information between quadratic forms, orderings and valuations:



In chapter 3 we treat about the first generation of abstract theories. The first abstract theories appears in 70's, by the hands of M. Marshall and C. M. Cordes. These theories appears for a reason: they are interested in the existence (or not) of fields with prescribed properties relating to quadratic forms.

In chapter 4, we discuss the second generation of abstract theories. The first one appears in the decade of 80's, the Marshall's Abstract Space of Orderings (AOS). They are important because generalize both theory of orderings on fields and the reduced theory of quadratic forms. Since the abstract theories of chapter 3 does not have field-theoretic methods to deal with the reduced case, the AOS solves this issue. But only in the decade of 90's that arise a (finitary) first-order theory that generalize the reduced and non-reduced theory of quadratic forms simultaneously. This theory is the Special Groups of F. Miraglia and M. Dickmann. It takes as primitive the binary isometry, is a first-order theory and treat the reduced and non-reduced case in a very elegant way. This simplicity brings new methods and tools to the algebraic theory of quadratic forms, culminating in a proof of Marshall's and Lam conjecture.

In chapter 5 the paradigm changes drastically. We start with a third generation of abstract theories, that appears in a first atempt to develop a theory of quadratic forms over (general) coefficients on rings. As we will see, the ring-theoretic case is much more difficult that the field

one, the isometry is not well behaved and an algebraic counterpart of the ARS's appears just in years 2000, with the realsemigroups (RS) of Dickmann and Petrovich. The RS appears in an atempt to creat a duality $\mathcal{RS} \simeq \mathcal{ARS}^{op}$ likewise $\mathcal{SG} \simeq \mathcal{AOS}^{op}$. They are successful in explore the analogies with the $\mathcal{SG}$ case (e.g, the Duality $\mathcal{RS} \simeq \mathcal{ARS}^{op}$), but this is not pay off in deep theorems yet, since the theory still is in development.

In chapter 6 the Chamber of The Secrets is opening: here we connect the new theory of multirings and multifields with the most significant theories of quadratic forms. This is (in some way) a new picture: despites of the Marshall's and Miraglia's observation about these connections, it is the first time that this is made explicit. So, because this, the implications of the multirings and multifieds theory in the abstract theory of quadratic forms are a road to discover.

Chapter 1

Quadratic Forms over Fields

At a first moment, we gather the principal results from the "classic" algebraic theory of quadratic forms. These are the Witt ring and its properties, Pfister's Local-Global Principle, Pfister forms and Hauptsatz, first connections between quadratic forms and orderings and so on. In this intent, we made a compiled of the chapters 1, 2, 8 and 10 of Lam's book [Lam05].

Our aim here, is to provide a good introduction to quadratic forms for the readers that are not familiar with this subject (and it is crucial since we will work with abstract versions of quadratic forms). Unfortunately, because this, we do not present many beauty applications as the field invariants, connections with Milnor's K-theory, quaternion algebras and more deep results on function fields. We will make some remarks on this direction in section 1.12, but for the readers interested on these applications, we strongly recomend the already cited book [Lam05], that covers all these aspects.

1.1 Foundations

Here, we will estabilish the "Rules of the Game", i.e, the list of the basic definitions and results from algebraic quadratic forms theory.

Definition 1.1.1. *An (n-ary) quadratic form over an field*[1] F *is a polynomial* f *in* n *variables over* F *that is homogeneous of degree* 2[2]*. It has the general form*

$$f(X_1, ..., X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j \in F[X_1, ..., X_n] = F[X].$$

To render the coefficients symmetric, it is customary to rewrite f as

$$f(X) = \sum_{i,j=1}^{n} \frac{1}{2}(a_{ij} + a_{ji}) X_i X_j = \sum_{i,j=1}^{n} b_{ij} X_i X_j,$$

where $b_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$. In this way, f determines uniquely a *symmetric matrix* (b_{ij}) (denoted by

[1] All fields consider in this present work have characteristic different from 2.

[2] An homogeneous polynomial $f \in F[X_1, ..., X_n]$ is a polynomial whose nonzero monomials all have the same total degree.

M_f) such that:

$$f(X) = (X_1, ..., X_n)^t \cdot M_f \cdot \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix}$$

where t is the transposition and X is viewed as a column vector. Quadratic forms arise naturally in many contexts of mathematics. There are some examples:

- The real inner product $\langle x, y\rangle = x_1y_1 + ... + x_ny_n$;
- The discrete variance of a random variable $X = \{x_1, ..., x_n\}$:

$$\mathrm{Var}(X) = \sum_{i=1}^{n} p_i(x_i - \overline{x})^2$$

  where $\overline{x}$ is the mean of X and p_i is the probability associated to x_i.

Indeed, it is a valuable analogy consider a quadratic form as a "generalized inner products". Now, as "good mathematicians", we will study the behavior of such "generalized inner products". The very first thing to do, is "collapse" quadratic forms that "describes the same phenomena":

Definition 1.1.2. *Let f and g be n-ary quadratic forms. We say that f is equivalent to g, notation $f \cong g$, if there exists an invertible matrix $C \in GL_n(F)$ such that $f(X) = g(C \cdot X)$.*

This means that there exists a nonsingular, homogeneous linear substitution of the variables $X_1, ..., X_n$ that takes the form g to the form f. Since

$$g(C \cdot X) = (C \cdot X)^t \cdot M_g \cdot (C \cdot X) = X^t \cdot (C^t \cdot M_g \cdot C) \cdot X,$$

the equivalence condition $f(X) = g(C \cdot X)$ stipulated above amounts to a matrix equation

$$M_f = C^t \cdot M_g \cdot C.$$

Thus, equivalence of forms amounts to congruence of the associated symmetric matrices (once that $C^t \cdot M_g \cdot C$ remains a symmetric matrix).

Example 1.1.3. *Let $f(X_1, X_2) = X_1X_2$. We have that f is equivalent to the form $g(X_1, X_2) = X_1^2 - X_2^2$ by the computation*

$$\begin{aligned} g\left(\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix} \cdot \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}\right) &= g(X_1/2 + X_2/2, X_1/2 - X_2/2) = \\ &= (X_1/2 + X_2/2)^2 - (X_1/2 - X_2/2)^2 = \\ &= X_1^2/4 + X_1X_2/2 + X_2^2/4 - X_1^2/4 + X_1X_2/2 - X_2^2/4 \\ &= X_1X_2 = f(X_1, X_2), \end{aligned}$$

or in matricial terms,

$$\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix} = \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}.$$

Remember that char$(F) \neq 2$.

Our point of view here is axiomatic, so is worthy to point out that we have another categorical equivalent axiomatizations for quadratic forms. We will discuss briefly the quadratic spaces and more information can be found in the chapter 1 of [San15].

Definition 1.1.4. *A quadratic space (V, B) consist of a finite-dimensional F-vector space V and a symmetric bilinear pairing $B : V \times V \to F$ on V. The map $q_B : V \to F$ given by $q_B(x) = B(x, x)$ for all $x \in V$ will called quadratic map associated to the quadratic space (V, B). Sometimes we will denote (V, B) by (V, q_B).*

Definition 1.1.5. *If (V, B) and (W, C) are quadratic spaces, we say that they are isometric, notation $V \cong W$ if there exists a linear isomorphism $\tau : V \to W$ such that*

$$C(\tau(x), \tau(y)) = B(x, y)$$

for all $x, y \in V$.

Naturally, we want to get something like this:

Proposition 1.1.6. *Let F be a field. Then there is a one-one correspondence between the equivalence classes of n-ary quadratic forms $\mathcal{Q}_F$ and the isometry classes of n-dimensional quadratic spaces $Quad_F$.*

Proof. Given a quadratic form f, define $Q_f : F^n \to F$ by $Q_f(x) = x^t \cdot M_f \cdot x$. In the sequel, define $B_f : F^n \times F^n \to F$ by

$$B_f(x, y) = \frac{1}{2}(Q_f(x + y) - Q_f(x) - Q_f(y)).$$

Let $f \cong g$ be isometric forms, where $M_f = C^t \cdot M_g \cdot C$ with $C \in \mathrm{GL}_n(F)$.

$$\begin{aligned} 2B_f(x, y) &= Q_f(x + y) - Q_f(x) - Q_f(y) \\ &= (x + y)^t \cdot M_f \cdot (x + y) - x^t \cdot M_f \cdot x - y^t \cdot M_f \cdot y \\ &= (x + y)^t \cdot (C^t \cdot M_g \cdot C) \cdot (x + y) - x^t \cdot (C^t \cdot M_g \cdot C) \cdot x - y^t \cdot (C^t \cdot M_g \cdot C) \cdot y \\ &= (C \cdot (x + y))^t \cdot M_g \cdot (C \cdot (x + y)) - (C \cdot x)^t \cdot M_g \cdot (C \cdot x) - (C \cdot y)^t \cdot M_g \cdot (C \cdot y) \\ &= 2B_g(C(x), C(y)). \end{aligned}$$

Then we have a (well-defined) map

$$\begin{aligned} \Phi \colon \mathcal{Q}_f &\to \mathrm{Quad}_F \\ [f] &\mapsto [(F^n, B_f)] \end{aligned}$$

On the other hand, given a quadratic space (V, B), for a choice of a base $\{e_1, ..., e_n\}$ of V, we can define a quadratic form

$$f_B(X_1, ..., X_n) = \sum_{i,j} B(e_i, e_j) X_i X_j$$

with $M_f = (B(e_i, e_j))$. If we choose another base $\{f_1, ..., f_n\}$, the quadratic form f' resulting from

the new choice of basis will be equivalent to f. In fact, if $f_i = \sum_{k=1}^{n} c_{ki}e_k$, then

$$\begin{aligned}(M'_f)_{ij} &= B(f_i, f_j) \\ &= B\left(\sum_{k=1}^{n} c_{ki}e_k, \sum_{l=1}^{n} c_{lj}e_j\right) \\ &= \sum_{k=1}^{n}\sum_{l=1}^{n} c_{ki} \cdot B(e_k, e_l) \cdot c_{lj} \\ &= (C^t \cdot M_f \cdot C)_{ij}\end{aligned}$$

where $C = (c_{kl})$. Therefore, this form is invariant under change of base, and since every n-dimensional F-vector space is isomorphic (and so on, isometric as quadratic space) to F^n, we have a map

$$\begin{aligned}\Psi \colon \mathrm{Quad}_F &\to \mathcal{Q}_f \\ [(V, B)] &\mapsto [f_B]\end{aligned}$$

Finally, we have $\Phi \circ \Psi = \mathrm{Id}$ (because $M_{f_B} = (B(e_i, e_j))_{ij}$) and $\Psi \circ \Phi = \mathrm{Id}$ by construction, finising the proof. □

Then quadratic forms and quadratic spaces describes the same thing, so we will switch between these notions according the convenience.

Our next step, is answer the question:

What class of quadratic forms matters? What properties they have?

So we need to classify them, by introducing new definitions and operations. In this sense, we start with the following lemma: let (V, B) be a quadratic space and M be a symmetric matrix associated to one of the forms in the equivalence class of f_B.

Lemma 1.1.7. *The following statements are equivalent:*

a - M is a nonsingular matrix.

b - $x \mapsto B(\,, x)$ defines an isomorphism $V \to V^*$, where V^* denotes the vector space dual of V.

c - For $x \in V$, $B(x, y) = 0$ for all $y \in V$ implies that $x = 0$.

Proof. The equivalence $(b) \Leftrightarrow (c)$ is just the fact that isomorphism are injective functions and $\dim(V) = \dim(V^*)$, so if $B(x, y) = 0$ for all $y \in V$, then x is in the kernel of the morphism $x \mapsto B(\,, x)$. And $(a) \Leftrightarrow (b)$ is consequence of the fact that M (by the appropriate choice of basis) is the matrix associated to the morphism $x \mapsto B(\,, x)$. □

Definition 1.1.8. *Let (V, B) be a quadratic space. (V, B) is a regular (or nonsingular) quadratic space if one (and hence all) of the equivalent statements of the lemma 1.1.7 holds.*

Keeping in mind the "generalized inner product" analogy, we equip our theory with some terminology provenient from linear algebra:

Definition 1.1.9. *Let (V, B) be a quadratic space, and S be a subspace of V. Then $(S, B|_{S\times S})$ is a quadratic space in its own right. The orthogonal complement of S is defined by*

$$S^{\perp} = \{x \in V : B(x, y) = 0, \forall y \in S\}.$$

The orthogonal complement of V itself is called the radical of (V, B), denoted by $V^{\perp} = rad(V)$.

Lemma 1.1.10. *Let (V, B) be a regular quadratic space and S be a subspace of V. Then:*

a - $\dim S + \dim S^{\perp} = \dim V$;

b - $(S^{\perp})^{\perp} = S$.

Proof. Let $\varphi : V \to V^*$ be the linear isomorphism defined in the item (b) of 1.1.7. Then $S^{\perp}$ is precisely the subspace of V annihilated by the functionals in $\varphi(S)$. By the usual duality theory in linear algebra, we have

$$\begin{aligned}\dim S^{\perp} &= \dim V^* - \dim \varphi(S)\\ &= \dim V - \dim S,\end{aligned}$$

since φ is an isomorphism. This estabilishes (a). Applying (a) twice, we get

$$\dim(S^{\perp})^{\perp} = \dim V - (\dim V - \dim S) = \dim S.$$

Since $(S^{\perp})^{\perp} \supseteq S$, we get (b). □

Definition 1.1.11. *If $(V_1, B_1), (V_2, B_2)$ are quadratic spaces, we may form the orthogonal sum (V, B) of $(V_1, B_1), (V_2, B_2)$, notation $(V, B) = (V_1, B_1) \perp (V_2, B_2)$ in this way: $V = V_1 \oplus V_2$ and $B : V \times V \to F$ is given by*

$$B((x_1, y_1), (x_2, y_2)) = B_1(x_1, y_1) + B_2(x_2, y_2).$$

And hence, $q_B = q_{B_1} + q_{B_2}$.

Example 1.1.12. *If q_1 is the ternary form $XY - 3Z^2$ and q_2 is the binary form $X^2 - Y^2$, $q_1 \perp q_2$ is the form $XY - 3Z^2 + V^2 - W^2$ in the five variables V, W, X, Y, Z.*

Lemma 1.1.13. *Let $(V_1, B_1), (V_2, B_2)$ be quadratic spaces. Then $(V_1, B_1) \oplus (V_2, B_2)$ is regular if and only if (V_1, B_1) and (V_2, B_2) are regular.*

Proof. Is direct consequence of

$$M_{f_{B_1}\perp f_{B_2}} = \begin{pmatrix} M_{f_{B_1}} & 0 \\ 0 & M_{f_{B_2}} \end{pmatrix},$$

where f_{B_1}, f_{B_2} are the unique form up to isometry determined by B_1 and B_2 respectively and $M_{f_{B_1}}, M_{f_{B_2}}$ are the symmetric matrix associated to one of the forms in the equivalence class of f_{B_1} and f_{B_2} respectively. □

Now, we advance another step in our purpose of classify quadratic forms. The next definition is crucial:

Definition 1.1.14. *Let F be a quadratic form over F and $d \in \dot{F} := F \setminus \{0\}$. We shall say that f represents d if there exists $x_1, x_2, ..., x_n \in F$ such that $f(x_1, ..., x_n) = d$.*

Note that $(x_1, ..., x_n)$ is a nonzero vector. We shall write $D_F(f) = D(f)$ to denote the set of values in $\dot{F}$ represented by f. This set depends only on the equivalence class of f. Beside this, $d \in D(f)$ if and only if $da^2 \in D(f)$ for all $a \in \dot{F}$.

For $d \in F$, we shall write $\langle d \rangle$ to denote the isometry class of the 1-dimensional space corresponding to the quadratic form dX^2. Follow by definition 1.1.8 that $\langle d \rangle$ is regular if and only if $d \in \dot{F}$.

Proposition 1.1.15. *Let (V, B) be a quadratic space and $d \in \dot{F}$. Then $d \in D(V)$ if and only if there exists another quadratic space (V', B') such that $V \cong \langle d \rangle \perp V'$.*

Proof. If we have $V \cong \langle d \rangle \perp V'$, then $d \in D(\langle d \rangle \perp V') = D(V)$. Conversely, suppose $d \in D(V)$, so there exists $v \in V$ with $q(v) = d$ (where $q = q_B$). We first make a reduction to the case where V is regular. Take any subspace W such that $V = (\text{rad}V) \oplus W = (\text{rad}V) \perp W$. We have $D(V) = D(W)$ be definition of orthogonal sum, and W is regular (by construction). Hence, we may assume without loss of generality that V is regular.

The quadratic subspace $F \cdot v$ is isometric to $\langle d \rangle$, and $(F \cdot v) \cap (F \cdot v)^{\perp} = 0$. Since

$$\dim(F \cdot v) + \dim(F \cdot v)^{\perp} = \dim V$$

by lemma 1.1.10, we conclude that $V \cong \langle d \rangle \perp (F \cdot v)^{\perp}$. □

Corollary 1.1.16. *If (V, B) is any quadratic space over F, then there exist scalars $d_1, ..., d_n \in F$ (an "orthogonal basis") such that $V \cong \langle d_1 \rangle \perp \langle d_2 \rangle \perp ... \perp \langle d_n \rangle$. In other words, any n-ary quadratic form is equivalent to some diagonal form, $d_1X_1^2 + ... + d_nX_n^2$.*

Proof. If $D(V)$ is empty, then $B \cong 0$ and V is isometric to an orthogonal sum of $\langle 0 \rangle$'s. If there exists some $d \in D(V)$, then $V \cong \langle d \rangle \perp V'$ for some (V', B'), and the proof proceeds by induction on $\dim V$. □

We shall abbreviate the diagonal form $\langle d_1 \rangle \perp \langle d_2 \rangle \perp ... \perp \langle d_n \rangle$ by $\langle d_1, d_2, ..., d_n \rangle$. The n-ary diagonal form $\langle d, ..., d \rangle$ will be abbreviated as $n\langle d \rangle$. For example, $2\langle a \rangle \perp 3\langle b \rangle$ means the 5-ary form $\langle a, a, b, b, b \rangle$. Another corollary follows:

Corollary 1.1.17. *Let f be an n-dimensional quadratic form over F. Then $b \in D(f) \Leftrightarrow$ there exist $b_2, ..., b_n \in \dot{F}$ such that $f \cong \langle b, b_2, ..., b_n \rangle$. Moreover, if f is regular then we can choose $b_2, ..., b_n \in \dot{F}$.*

Proof. ($\Leftarrow$) is a natural consequence of the definitions of isometry and representation. For ($\Rightarrow$), consider the quadratic space (V, B_f)associated to f. We have $V \cong \langle b \rangle \perp V'$ by proposition 1.1.15. Hence, the result follows diagonalizing V'. □

Proposition 1.1.15 and corollaries 1.1.16, 1.1.17 are a powerful tools in deal with quadratic forms. These reduces the study of quadratic forms to diagonal forms, i.e, instead of deal with matrices, polynomials and vector spaces we only need to worry with n-tuple of elements in $\dot{F}$. Of course, we will use (and abuse) of this method from now to the end of the dissertation.

However, we do not forget the intuition and geometric appeal that linear algebra and matrices got to us! In face of this, we still work with spacial notions in this and next section.

Corollary 1.1.18. *If (V, B) is a quadratic space and S is a regular subspace, then:*

a - $V = S \perp S^{\perp}$.

b - If T is a subspace of V such that $V = S \perp T$, then $T = S^{\perp}$.

Proof. a - Since $S \cap S^\perp = \text{rad}S = 0$, it is suffices to show that V is spanned by S and $S^\perp$. By corollary 1.1.16, S has an orthogonal basis $x_1, ..., x_p$, and the regularity of S implies that $B(x_i, x_i) \neq 0$ for all i. Given $z \in V$, consider the vector

$$y = z - \sum_{i=1}^{p} \frac{B(z, x_i)}{B(x_i, x_i)} x_i.$$

We have

$$\begin{aligned} B(y, x_j) &= B(z, x_j) - \sum_{i=1}^{p} \frac{B(z, x_i)}{B(x_i, x_i)} B(x_i, x_j) \\ &= B(z, x_j) - \frac{B(z, x_j)}{B(x_j, x_j)} B(x_j, x_j) = 0. \end{aligned}$$

Thus $y \in S^\perp$, and

$$z = y + \sum_{i=1}^{p} \frac{B(z, x_i)}{B(x_i, x_i)} x_i \in S \perp S^\perp.$$

b - If $V = S \perp T$, then $T \subseteq S^\perp$. But

$$\dim T = \dim V - \dim S = \dim S^\perp$$

and $\dim T, \dim S^\perp \leq \dim V \in \mathbb{N}$. So, we must have $T = S^\perp$.

□

Corollary 1.1.19. *Let (V, B) be a regular quadratic space. Then a subspace S is regular if and only if there exists $T \subseteq V$ such that $V = S \perp T$.*

Proof. ($\Rightarrow$) Take $T = S^\perp$ and apply the item (a) of the corollary 1.1.18.

($\Leftarrow$) If $V = S \perp T$, then $\text{rad}S \subseteq \text{rad}V = 0$, so S is regular and $T = S^\perp$, by item (b) of corollary 1.1.18. □

Definition 1.1.20. *Let f be a nonsingular quadratic form. The discriminant of f is defined to be $d(f) = \det(M_f) \cdot \dot{F}^2$ (an element of $\dot{F}/\dot{F}^2$), where M_f is the symmetric matrix associated with f.*

Note that if $f \cong g$, then $M_f = C^t M_g C$ for some nonsingular matrix C, and hence

$$d(f) = \det(M_f) \cdot \dot{F}^2 = \det(M_g) \cdot (\det C)^2 \cdot \dot{F}^2 = d(g).$$

This shows that $d(f)$ is an *invariant* of the equivalence class of f.

Let (V, B) be a (regular) quadratic space that corresponde to the equivalence class of f. If $V \cong \langle d_1, ..., d_n \rangle$ is a "diagonalization" of V, then $d(f) = d_1 ... d_n \cdot \dot{F}^2$. It is sometimes convenient to call this quantity the discriminant of V, written $d(V)$.

We had seen some cool results about regular quadratic forms, so you could be thinking

Our job is done! Regular forms classify quadratic forms!

But it is not enough. For example, let the binary form $q = \langle 1, -1 \rangle$ (say in $\mathbb{R}$). q is a regular form, but $q(x, x) = 0$ for all $x \in \mathbb{R}$, so from the "q-point of view", all vectors in the line $y = x$ have "length" zero. In an ideal world, non-zero vectors must be "positive length"! So regular forms do not "see" these "strange" vectors.

Definition 1.1.21. *Let v be a nonzero vector in a quadratic space (V, B). We say that v is an isotropic vector if $B(v, v) = 0$ and say that v is anisotropic otherwise. The quadratic space (V, B) is isotropic if it contains a (nonzero) isotropic vector and is said to be anisotropic otherwise. Finally, we shall say that (V, B) is totally isotropic if all nonzero vectors in V are isotropic (that is, if $B \equiv 0$).*

Theorem 1.1.22. *Let (V, q) be a 2-dimensional quadratic space. The following four statements are equivalent:*

a - V is regular and isotropic.

b - V is regular, with $d(V) = -1 \cdot \dot{F}^2$.

c - V is isometric to $\langle 1, -1 \rangle$.

d - V corresponds to the equivalence class of the binary form X_1X_2.

The isometry class of a 2-dimensional quadratic space satisfying these conditions is called hyperbolic plane and will be denoted by $\mathbb{H}$.

Proof. We already seen that $(c) \Leftrightarrow (d)$ in example 1.1.3, and $(d) \Rightarrow (a)$ is immediate.

$(a) \Rightarrow (b)$: Let x_1, x_2 be an orthogonal basis for V. Regularity of V implies that $q(x_i) = d_i \neq 0$ $(i = 1, 2)$. Let $ax_1 + bx_2$ be an isotropic vector with $a \neq 0$ (without loss of generality). Then

$$0 = q(ax_1 + bx_2) = a^2d_1 + b^2d_2 \Rightarrow d_1 = -(ba^{-1})^2 \cdot d_2$$
$$\Rightarrow d(V) = d_1d_2 \cdot \dot{F}^2 = -1 \cdot \dot{F}^2.$$

$(b) \Rightarrow (c)$: Under the hypothesis of (b), we have a diagonalization $V \cong \langle a, -a \rangle$ for some $a \in \dot{F}$. By the argument in example 1.1.3, we know that $aX^2 - aY^2$ is equivalent to aXY. The latter represents all elements in $\dot{F}$. In particular, (V, q) itself represents 1. By the proposition 1.1.15, we conclude that $V \cong \langle 1, -1 \rangle$. □

An orthogonal sum of hyperbolic planes will be called a *hyperbolic space*. The corresponding quadratic form may be taken either as $(X_1^2 - X_2^2) + ... (X_{2m-1}^2 - X_{2m}^2)$ or as $X_1X_2 + ... + X_{2m-1}X_{2m}$.

Definition 1.1.23. *A quadratic form (or quadratic space) is called universal if it represents all the nonzero elements of F.*

Theorem 1.1.24. *Let (V, B) be a regular quadratic space. Then:*

a - Every totally isotropic subspace $U \subseteq V$ of positive dimension r is contained in a hyperbolic subspace $T \subseteq V$ of dimension $2r$.

b - V is isotropic if and only if V contains a hyperbolic plane.

c - If V is isotropic, then V is universal.

Proof. a - We shall prove by induction on r. Take any basis $x_1, ..., x_r$ in U, and let S be the span of $x_2, ..., x_r$. Of course, $U^\perp \subseteq S^\perp$. Since V is regular, we may apply the proposition 1.1.15 to get

$$\dim S^\perp = \dim V - \dim S > \dim V - \dim U = \dim U^\perp.$$

This means that there exists a vector $y_1 \in S^\perp$ that is orthogonal to $x_2, ..., x_r$, but not orthogonal to x_1. In particular, x_1, y_1 are linearly independent vectors (since x_1 is isotropic). The subspace $H_1 = Fx_1 + Fy_1$ has discriminant

$$d(H_1) = \det \begin{pmatrix} 0 & B(x_1, y_1) \\ B(x_1, y_1) & B(y_1, y_1) \end{pmatrix} \cdot \dot{F}^2 = -1 \cdot \dot{F}^2,$$

so $H_1 \cong \mathbb{H}$ by the theorem 1.1.22. We have thus a splitting $V = H_1 \perp V'$, where $V' = H_1^\perp$ contains $x_2, ..., x_r$ (corollary 1.1.18). Since V' is regular (corollary 1.1.19), the proof proceeds by induction.

b - Follow by (a) putting $r = 1$.

c - Is imediatly consequence of the fact that $\mathbb{H}$ is universal.

□

Theorem 1.1.25. *Let f, g be arbitrary quadratic forms over a field F, $a_1, ..., a_n, b_1, ..., b_n \in \dot{F}$ and $\pi \in S_n$[3]. Then:*

a - $f \cong g \Rightarrow \dim(f) = \dim(g)$ *and* $d(f) = d(g)$.

b - $f \cong g \Rightarrow af \cong ag$ *for all* $a \in \dot{F}$.

c - $\langle a_1 b_1^2, ..., a_n b_n^2 \rangle \cong \langle a_1, ..., a_n \rangle$.

d - $\langle a_{\pi(1)}, ..., a_{\pi(n)} \rangle \cong \langle a_1, ..., a_n \rangle$.

e - *If* $\langle a_1, ..., a_k \rangle \cong \langle b_1, ..., b_k \rangle$ *and* $\langle a_{k+1}, ..., a_n \rangle \cong \langle b_{k+1}, ..., b_n \rangle$ *then* $\langle a_1, ..., a_n \rangle \cong \langle b_1, ..., b_n \rangle$.

Proof.

a - Isometry is already defined on forms of the same dimension. Now, suppose that $M_f = C^t M_g C$. Then

$$\det(M_f) = \det(C^t M_g C) = \det(M_g) \det(C)^2 \Rightarrow d(f) \quad = \det(M_f) \cdot \dot{F}^2 = \det(M_g) \cdot \dot{F}^2 = d(g).$$

b - If $g(X) = f(C \cdot X)$ for some $C \in \mathrm{GL}_n(F)$, then the same matrix C gives $ag(X) = af(C \cdot X)$.

c - Is just the fact that the symmetric matrix

$$B = \begin{pmatrix} b_1 & 0 & ... & 0 \\ 0 & b_2 & ... & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & ... & b_n \end{pmatrix}$$

transform $\langle a_1, ..., a_n \rangle$ to $\langle a_1 b_1^2, ..., a_n b_n^2 \rangle$.

d - Consider the matrix $A = (a_{ij})$ where $a_{i\pi(i)} = 1$ and the other entries are 0. We have that $A \in \mathrm{GL}_n(F)$ and A transform $\langle a_1, ..., a_n \rangle$ to $\langle a_{\pi(1)}, ..., a_{\pi(n)} \rangle$.

[3]The group of bijections $\pi : \{1, 2, ..., n\} \to \{1, 2, ..., n\}$.

e - If B transform $\langle a_1, ..., a_k\rangle$ into $\langle b_1, ..., b_k\rangle$ and C transform $\langle a_{k+1}, ..., a_n\rangle$ into $\langle b_{k+1}, ..., b_n\rangle$ then

$$D = \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix}$$

transform $\langle a_1, ..., a_n\rangle$ into $\langle b_1, ..., b_n\rangle$.

□

Corollary 1.1.26. *Let $a, b, c, d \in \dot{F}$. Then:*

a - $\langle a\rangle \cong \langle b\rangle \Leftrightarrow a \equiv b \,(mod\ \dot{F}^2)$.

b - $\langle a, b\rangle \cong \langle c, d\rangle \Leftrightarrow ab \equiv cd \,(mod\ \dot{F}^2)$ *and there exist* $x, y \in F$ *such that* $c = ax^2 + by^2$.

Proof.

a - Is just the items (a) and (c) of corollary 1.1.25.

b - ($\Rightarrow$) $ab \equiv cd \,(\text{mod}\ \dot{F}^2)$ comparing discriminants and by theorem 1.1.17(e), we have $c \in D(a, b)$. Then there exist $x, y \in F$ such that $c = ax^2 + by^2$.

($\Leftarrow$) As $c = ax^2 + by^2$ for some $x, y \in F$, we have $c \in D(a, b)$. Hence by corollary 1.1.17 $\langle c, e\rangle \cong \langle a, b\rangle$ for some $e \in \dot{F}$. Thus $ce \cdot \dot{F}^2 = ab \cdot \dot{F}^2 = cd \cdot \dot{F}^2$ so $e \cdot \dot{F}^2 = d \cdot \dot{F}^2$. By item (a) $\langle e\rangle \cong \langle d\rangle$ and by corollary 1.1.25 $\langle c, e\rangle \cong \langle c, d\rangle$. Then by transitivity of isometry $\langle a, b\rangle \cong \langle c, d\rangle$.

□

Corollary 1.1.27. $\langle a, -a\rangle \cong \langle 1, -1\rangle$ *holds for all* $a \in \dot{F}$.

Proof. $a(-a) \cdot \dot{F}^2 = 1(-1) \cdot \dot{F}^2$ and

$$a = \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2.$$

Thus by item (b) of corollary 1.1.26 we have $\langle a, -a\rangle \cong \langle 1, -1\rangle$. □

Corollary 1.1.28. *Let f be a regular quadratic form over F of dimension n. Then f is isotropic if and only if there exist $b_3, ..., b_n \in \dot{F}$ with $f \cong \langle 1, -1, b_3, ..., b_n\rangle$. In particular, this implies $n \geq 2$.*

Proof. If $f \cong \langle 1, -1, b_3, ..., b_n\rangle$, then $1^2 - 1^2 + b_3(0)^2 + ... + b_n(0)^2 = 0$ and f is isotropic (for the vector $v = (1, 1, 0, 0, ..., 0)$, we have $f(v) = 0$ and $v \neq 0$). Now suppose that $f \cong \langle a_1, ..., a_n\rangle$ is isotropic. Then for some $x_1, ..., x_n \in F$ not all zero, we have $a_1x_1^2 + ... + a_nx_n^2 = 0$. By 1.1.25(d) we may assume $x_1 \neq 0$. Take $a = a_1x_1^2$. Then $-a = a_2x_2^2 + ... + a_nx_n^2 \in D(a_2, ..., a_n)$ so bycorollary 1.1.17, there exist $b_3, ..., b_n \in \dot{F}$ such that $\langle a_2, ..., a_n\rangle \cong \langle -a, b_3, ..., b_n\rangle$. Also $\langle a_1\rangle \cong \langle a\rangle$ by corollary 1.1.26(a) so by 1.1.25(e) and corollary 1.1.27

$$f \cong \langle a_1, ..., a_n\rangle \cong \langle a, -a, b_3, ..., b_n\rangle \cong \langle 1, -1, b_3, ..., b_n\rangle.$$

□

Proposition 1.1.29. *Leq $q = \langle a, b\rangle$, $q' = \langle c, d\rangle$ be regular binary forms. Then $q \cong q'$ if and only if $d(q) = d(q')$ and q, q' represents a common element $e \in \dot{F}$.*

Proof. We just need to prove ($\Leftarrow$). Assume that $d(q) = d(q') \in \dot{F}/\dot{F}^2$ and let $e \in D(q) \cap D(q')$. By proposition 1.1.15, we know that $q \cong \langle e, e' \rangle$ for some $e' \in \dot{F}$. Taking discriminant, we have $ab\dot{F}^2 = cd\dot{F}^2$, so $q \cong \langle e, abe \rangle$. Similarly, $q' \cong \langle e, cde \rangle$. But $ab\dot{F}^2 = cd\dot{F}^2$, so $q \cong q'$. □

Now we know what we need to do: it is necessary to look for some criteria to decompose general diagonal forms to *anisotropic* diagonal forms. But before this, let is get more familiarity operating quadratic forms. Our classification task will return in the future.

So, we already know how to "sum" quadratic forms. A natural question is:

Is it possible "multiply" forms?

Of course is, and this is the subject of the next definition:

Definition 1.1.30. *Let $(V_1, B_1, q_1), (V_2, B_2, q_2)$ be two quadratic spaces over F, of dimension m and n. We define a new vector space $V = V_1 \otimes V_2$ ($\otimes = \otimes_F$), and let $B : V \times V \to F$ be the unique simmetric bilinear pairing satisfying*

$$B(v_1 \otimes v_2, v_1' \otimes v_2') = B_1(v_1, v_1')B_2(v_2, v_2'),\ v_1, v_2 \in V_1,\ v_1', v_2' \in V_2.$$

and therefore, $q_B(v_1 \otimes v_2) = q_1(v_1)q_2(v_2)$. The pair (V, B) is a new quadratic space over F with dimension mn, called the Kronecker product (or tensor product) of V_1 and V_2.

Let $\{e_1, ..., e_m\}$ and $\{f_1, ..., f_n\}$ be basis of V_1 and V_2 respectively. Taking $a_{ij} = B_1(e_i, e_j)$ and $b_{lk} = B_2(f_l, f_k)$, we have that $M = (a_{ij})$ and $N = (b_{lk})$ are the symmetric matrices associated with q_1 and q_2 in the given choice of base (respectively). Now, consider the basis of $V = V_1 \otimes V_2$ given by $\{e_1 \otimes f_1, e_1 \otimes f_2, ..., e_1 \otimes f_n, ..., e_m \otimes f_1, ..., e_m \otimes f_n\}$. With respect to this choice of basis, the form q gives rise to the symmetric matrix

$$\left(\begin{array}{ccc|ccc|c} a_{11}b_{11} & a_{11}b_{12} & \cdots & a_{12}b_{11} & a_{12}b_{12} & \cdots & \cdots \\ a_{11}b_{21} & a_{11}b_{22} & \cdots & a_{12}b_{21} & a_{12}b_{22} & \cdots & \cdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \cdots \\ \hline a_{21}b_{11} & a_{21}b_{12} & \cdots & \cdots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{array}\right) = \begin{pmatrix} a_{11}N & a_{12}N & \cdots & a_{1m}N \\ a_{21}N & a_{22}N & \cdots & a_{2m}N \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}N & a_{m2}N & \cdots & a_{mm}N \end{pmatrix}$$

which is precisely the ordinary Kronecker product of the two matrices M, N. In particular, $\langle a \rangle \otimes \langle b \rangle \cong \langle ab \rangle$ for all $a, b \in F$.

As consequence of this matricial property, we have the following lemma:

Lemma 1.1.31. *The Kronecker product operation for quadratic forms satisfies the following properties:*

a - $q_1 \otimes q_2 \cong q_2 \otimes q_1$.

b - $(q_1 \otimes q_2) \otimes q_3 \cong q_1 \otimes (q_2 \otimes q_3)$.

c - *The "distributive law"* $q \otimes (q_1 \perp q_2) \cong (q \perp q_1) \otimes (q \perp q_2)$.

Using the distributive law, we obtain the following rule:

$$\langle a_1, ..., a_m \rangle \otimes \langle b_1, ..., b_n \rangle \cong \langle a_1b_1, ...a_1b_m, a_2b_1, ..., a_2b_m, ..., a_nb_1, ..., a_mb_n \rangle.$$

If r is a nonnegative integer and f is a form, $r \cdot f$ (or sometimes rf) denotes the orthogonal sum of r copies of f.

Corollary 1.1.32. *If q is any regular quadratic form, then $q \otimes \mathbb{H} \cong (\dim q) \cdot \mathbb{H}$.*

Proof. By induction on $\dim q$, we reduce to the case where $q = \langle a \rangle$, $a \neq 0$. But then, $\langle a \rangle \otimes \mathbb{H} = \langle a, \rangle \otimes \langle 1, -1 \rangle \cong \langle a, -a \rangle \cong \mathbb{H}$, by the theorem 1.1.22. □

1.2 Witt's theorems and its consequences

We are aware equipped with basic facts about isometry, sum and product of forms, so we are prepared to deal with our classification task. We will get the desired decomposition in this section, as consequence of some classical theorems due to Ernest Witt.

To proof the first one, the Cancellation Theorem, we need the notion of a *hyperplane refletion*. Let (V, B, q) be any quadratic space. We shall write $O_q(V) = O(V)$ to denote the group of isometries of (V, q). This so-called *orthogonal group* is the symmetry group which underlies the geometry of our quadratic spaces. The following construction associates an element $\tau_y \in O(V)$ to every anisotropic vector $y \in V$. As a map from V to itself, τ_y is defined by

$$\tau_y(x) = x - \frac{2B(x,y)}{q(y)}y$$

for every $x \in V$. Below, are some properties of τ_y:

a - τ_y is a linear endomorphism.

b - τ_y is the identity map on $(F \cdot y)^\perp$. In fact, in the above formula, if $B(x, y) = 0$, then $\tau_y(x) = x$. Furthermore, if we apply τ_y to y itself, we get

$$\tau_y(y) = y - \frac{2B(y,y)}{q(y)}y = y - 2y = -y.$$

In particular, τ_y is an involution ($\tau_y^2 = id$): it leaves the hyperplane $(F \cdot y)^\perp$ pointwise fixed, and reflects the vector λy across $(F \cdot y)^\perp$ to $-\lambda y$.

c - $\tau_y \in O(V)$ by the calculation:

$$\begin{aligned} B(\tau_y(x), \tau_y(x')) &= B\left(x - \frac{2B(x,y)}{q(y)}y, x' - \frac{2B(x',y)}{q(y)}y\right) \\ &= B(x,x') - \frac{4B(x,y)B(x',y)}{q(y)^2}B(y,y) - \frac{4B(x,y)B(x',y)}{q(y)} \\ &= B(x,x') \,(\text{since } B(y,y) = q(y)). \end{aligned}$$

d - As a linear automorphism, τ_y has discriminant -1.

e - The set of hyperplane refletions $\{\tau_y : q(y) \neq 0\}$ is closed under conjugation in the orthogonal group $O(V)$. In fact, if $\sigma \in O(V)$, then one has $\sigma\tau_y\sigma^{-1} = \tau_{\sigma y}$:

$$\begin{aligned} \sigma\tau_y\sigma^{-1}(x) &= \sigma[\tau_y\sigma^{-1}x] \\ &= \sigma\left[\sigma^{-1}x - \frac{2B(\sigma^{-1}x, y)}{q(y)}y\right] \\ &= x - \frac{2B(x,\sigma y)}{q(\sigma y)}\sigma y = \tau_{\sigma y}(x) \end{aligned}$$

for every $x \in V$.

Proposition 1.2.1. *Let (V, q) be a quadratic space, and let x, y be vectors in V such that $q(x) = q(y) \neq 0$. Then there exists on element $\tau \in O(V)$ such that $\tau(x) = y$.*

Proof. Geometrically, if we consider the reflection with respect to the hyperplane $(F \cdot (x-y))^{\perp}$, then x should be taken to y. But, is $x - y$ necessarily anisotropic? We derive first the law of parallelogram:

$$\begin{aligned} q(x+y) + q(x-y) &= B(x+y, x+y) + B(x-y, x-y) \\ &= 2B(x,x) + 2B(y,y) = 4q(x) \neq 0. \end{aligned}$$

This implies that $q(x+y), q(x-y)$ cannot be both zero. Replacing y by $-y$ if necessary, we may assume that $q(x-y) \neq 0$ (because if we can find $\tau \in O(V)$ such that $\tau(x) = -y$, then $q(-y) = q(y) \neq 0$, so $\tau_{-y}(\tau(x)) = \tau_{-y}(-y) = y$). Applying the reflection τ_{x-y} to x, we obtain

$$\tau_{x-y}(x) = x - \frac{2B(x, x-y)}{q(x-y)}(x-y).$$

But

$$\begin{aligned} q(x-y) &= B(x-y, x-y) \\ &= B(x,x) + B(y,y) - 2B(x,y) \\ &= 2(B(x,x) - B(x,y)) = 2B(x, x-y). \end{aligned}$$

Thus, $\tau_{x-y}(x) = x - (x-y) = y$, finishing the proof. □

We are in position to prove

Theorem 1.2.2 (Witt's Cancellation)**.** *If q, q_1, q_2 are arbitrary quadratic forms, then*

$$q \perp q_1 \cong q \perp q_2 \Rightarrow q_1 \cong q_2.$$

Proof. Suppose it is given that $q \perp q_1 \cong q \perp q_2$.

Case 1: q is totally isotropic and q_1 is regular. Let M_1, M_2 be the symmetric matrices associated with q_1 and q_2. The hypothesis implies that $\begin{pmatrix} 0 & 0 \\ 0 & M_1 \end{pmatrix}$ is congruent to $\begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix}$, so there exists an invertible matrix $E = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, $\dim(A) = \dim(q)$, $\dim(D) = \dim(q_1) = \dim(q_2)$, such that

$$\begin{aligned} \begin{pmatrix} 0 & 0 \\ 0 & M_1 \end{pmatrix} &= E^t \begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix} E \\ &= \begin{pmatrix} A^t & B^t \\ C^t & D^t \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \\ &= \begin{pmatrix} A^t & B^t \\ C^t & D^t \end{pmatrix} \begin{pmatrix} 0 & 0 \\ M_2 C & M_2 D \end{pmatrix} \\ &= \begin{pmatrix} C^t M_2 C & C^t M_2 D \\ D^t M_2 C & D^t M_2 D \end{pmatrix} \end{aligned}$$

In particular $M_1 = D^t M_2 D$. Since M_1 is nonsingular, so is D, and hence M_1, M_2 are congruent. This gives $q_1 \cong q_2$.

Case 2: q is totally isotropic. To see this, diagonalize q_1, q_2 and assume that q_1 has exactly r zeros coefficients in the diagonalization, while q_2 has exactly r zeros or more. Rewriting the hypothesis, we have

$$q \perp r\langle 0\rangle \perp q_1' \cong q \perp r\langle 0\rangle \perp q_2'.$$

Since q_1' is regular, the case 1 implies that $q_1' \cong q_2'$. By tagging on r terms of $\langle 0\rangle$, we conclude that $q_1 \cong q_2$.

Case 3: general case. Let $\langle a_1, ..., a_n\rangle$ be a diagonalization of q. Inducting on n, we are reduced to the case $n = 1$. The case $a_1 = 0$ has been handled in case 2, so we may assume that $q = \langle a_1\rangle$, $a_1 \neq 0$. The hypothesis now reads: $\langle a_1\rangle \perp q_1 \cong \langle a_1\rangle \perp q_2$. Let $p_1 = \langle a_1\rangle \perp q_1$ and $p_2 = \langle a_1\rangle \perp q_2$. Since $a_1 \neq 0$, there exists $x_1, y_1, x_2, y_2 \in V$ (eventually $x_1 = y_1$ and $x_2 = y_2$) such that $p_1(x_1) = p_1(y_1) \neq 0$ and $p_2(x_2) = p_2(y_2) \neq 0$.

By proposition 1.2.1, there exists $\tau_1, \tau_2 \in O(V)$ isometries such that $\tau_1(x_1) = \tau_1(y_1)$ and $\tau_2(x_2) = \tau_2(y_2)$. Since $\tau_1 \restriction_{(F\cdot x_1)^\perp} : (F\cdot x_1)^\perp \to (F\cdot y_1)^\perp$ and $\tau_2 \restriction_{(F\cdot x_2)^\perp} : (F\cdot x_2)^\perp \to (F\cdot y_2)^\perp$ are isometries and $q_1 = (V,q) \restriction_{(F\cdot x_1)^\perp}$, $q_2 = (V,q) \restriction_{(F\cdot x_2)^\perp}$; $\tau_2^{-1} \restriction_{(F\cdot y_2)^\perp} \circ \tau_1 \restriction_{(F\cdot x_1)^\perp}$ is the isometry that witness $q_1 \cong q_2$.

□

Finally, we get our desired decomposition theorem:

Theorem 1.2.3 (Witt's Decomposition)**.** *Any quadratic space (V,q) splits into an orthogonal sum*

$$(V_t, q_t) \perp (V_h, q_h) \perp (V_a, q_a),$$

where V_t is totally isotropic, V_h is hyperbolic (or zero), and V_a is anisotropic (or zero). Furthermore, the isometry types of V_t, V_h, V_a are all uniquely determined.

Proof. For the existence, take any subspace V_0 such that $V = (\mathrm{rad}V) \oplus V_0 = (\mathrm{rad}V) \perp V_0$. Then $V_t = \mathrm{rad}V$ is totally isotropic, and V_0 is regular. If V_0 is isotropic, we may write $V_0 = H_1 \perp V_1$ (by theorem 1.1.24), where $H_1 \cong \mathbb{H}$. If V_1 is again isotropic, we may further write $V_1 = H_2 \perp V_2$, where $H_2 \cong \mathbb{H}$. After a finite number of steps, we achieve a decomposition

$$V_0 = (H_1 \perp ... \perp H_r) \perp V_a, \ (r \geq 0),$$

where $H_1 \perp ... \perp H_r = V_h$ is hyperbolic (or zero), and V_a is anisotropic. This proves the existence part.

To estabilish the uniqueness part, suppose V has another Witt decomposition $V = V_t' \perp V_h' \perp V_a'$. Since V_t' is totally isotropic and $V_h' \perp V_a'$ is regular, we have

$$\mathrm{rad}V = (\mathrm{rad}V_t') \perp \mathrm{rad}(V_h' \perp V_a') = V_t',$$

so $V_t \cong V_t'$. By the Cancellation Theorem 1.2.2, we have now $V_h \perp V_a \cong V_h' \perp V_a'$. Write $V_h \cong m\cdot\mathbb{H}$ and $V_h' \cong m'\cdot\mathbb{H}$. By cancelling $\mathbb{H}$ one at time, we conclude that $m = m'$ since V_a, V_a' are both anisotropic. After all m hyperbolic planes have been cancelled, we arrive at $V_a \cong V_a'$, completing the proof. □

So with Witt's decomposition theorem, we can happily say

Just anisotropic forms matters!

and consider our classification task done. But *the devil is in the details!* In a pratical situation, taking a general (diagonal) anisotropic form of dimension n could lead us to some trouble with the "length" of n. In other words, we do not want to make heavy calculation with forms of higher dimension. So would be desirable reduce this "length" as much as possible. This is the content of the next two theorems.

Then, our ultimate slogan is

Just binary anisotropic forms matters!

If you casually underestimate the power of binary forms, we have a final argument for you: the Chain Equivalence Theorem. First, we define simply and chain equivalence:

Definition 1.2.4. *Let $q = \langle a_1, ..., a_n\rangle$ and $q' = \langle b_1, ..., b_n\rangle$. We shall say that q and q' are simply-equivalent, if there exist indices $i, j \leq n$, such that*

a - $\langle a_i, a_j\rangle \cong \langle b_i, b_j\rangle$,

b - $a_k = b_k$ *whenever k is different from i and j.*

Note that, if $i = j$, the expression $\langle a_i, a_j\rangle$ is understood to be just $\langle a_i\rangle$.

More generally, we say that two diagonal forms f and g are chain-equivalent, if there exists a sequence of diagonal forms $f_0, f_1, ..., f_m$ such that $f_0 = f$, $f_m = g$, and each f_i is simply-equivalent f_{i+1} ($0 \leq i \leq m-1$).

Chain equivalence is an equivalence relation on all diagonal forms (of a fixed dimension), and it will be denoted by the symbol $\approx$. Of course, $f \approx g$ implies $f \cong g$. It turns out that the converse is also true, and this is the content of the following celebrated result of Witt:

Theorem 1.2.5 (Witt's Chain Equivalence)**.** *If f and g are arbitrary diagonal forms (of the same dimension), then $f \cong g \Rightarrow f \approx g$.*

Proof. Say $f = \langle a_1, ..., a_n\rangle$ and $g = \langle b_1, ..., b_n\rangle$. Note that if σ is a permutation of the indices $\{1, 2, ..., n\}$, and $f^\sigma = \langle a_{\sigma(1)}, a_{\sigma(2)}, ..., a_{\sigma(n)}\rangle$, then $f \approx f^\sigma$. This follows from the observation that the full symmetric group on $\{1, ..., n\}$ is generated by the transpositions. Since $f \cong g$, the two forms, f and g, have the same number of zero terms in their diagonalizations. It is, therefore, sufficient to show that the regular parts of f and g are chain-equivalent. By Witt's Decomposition Theorem 1.2.3, the number of zeros in f is equal of the number of zeros in g, so we may assume that f and g are both regular, that is, a_i, b_j are all nonzero. The argument is by induction on n. There is nothing to prove if $n = 1, 2$, so we consider $n \geq 3$ in the following.

Among all diagonal forms that are chain-equivalent to f, choose an $f' = \langle c_1, ..., c_n\rangle$ such that some $\langle c_1, ..., c_p\rangle$ represents b_1 and p is smallest possible (the existence of f' follows from the Well-Ordering Principle). We claim that $p = 1$. In fact, suppose the contrary. Write $b_1 = c_1e_1^2 + ... + c_pe_p^2$ ($p \geq 2$). By the minimality of p, no subsum in this summation can be equal to zero. In particular, $d = c_1e_1^2 + c_2e_2^2 \neq 0$. By proposition 1.1.15, $\langle c_1, c_2\rangle \cong \langle d, c_1c_2d\rangle$. Thus

$$\begin{aligned} f \approx f' &= \langle c_1, c_2, ..., c_n\rangle \\ &\approx \langle d, c_1c_2d, c_3, ..., c_p, ..., c_n\rangle \\ &\approx \langle d, c_3, ..., c_p, ..., c_n, c_1c_2d\rangle, \end{aligned}$$

and $b_1 = d + c_3e_3^2 + ... + c_pe_p^2$ is already represented by $\langle d, c_3, ..., c_p\rangle$, which has dimension $p-1$, contradicting the choice of p. We have thus shown that $p = 1$. Hence $\langle c_1\rangle \cong \langle b_1\rangle$, and so $f \approx \langle b_1, c_2, ..., c_n\rangle$. By Witt's Cancellation Theorem,

$$\langle b_1, c_2, ..., c_n\rangle \cong \langle b_1, b_2, ..., b_n\rangle \Rightarrow \langle c_2, ..., c_n\rangle \cong \langle b_2, ..., b_n\rangle.$$

By the inductive hypothesis, this implies that $\langle c_2, ..., c_n\rangle \approx \langle b_2, ..., b_n\rangle$. So finally,

$$f \approx \langle b_1, c_2, ..., c_n\rangle \approx \langle b_1, b_2, ..., b_n\rangle = g.$$

□

1.3 The Witt Ring

Okay, you define quadratic forms and classify them. In the process, some operations (orthogonal sum and Kronecker product) appears, and you prove that with these operations, the "quadratic forms are almost a ring". What we get if we pursuit these ideas?

If you thought something like that, do not worry, we do not forget about our operations. Let $M(F)$ be the set of all isometry classes of nonsingular quadratic forms over F. The binary operations $\perp$ and $\otimes$ already define the structure of a commutative semiring on $M(F)$. By Witt's Cancellation Theorem (1.2.2), the additive structure ($\perp$) actually makes $M(F)$ into a cancellation monoid, although no nonzero element in $M(F)$ has an additive inverse. The procedure required to remedy this is the so-called Grothendieck construction. In fact, this construction is essentially the same of the construction of $\mathbb{Z}$ from $\mathbb{N}$.

In general, let M be any commutative cancelative monoid under addition. We define a relation $\sim$ on $M \times M$ by

$$(x, y) \sim (x', y') \Leftrightarrow x + y' = x' + y.$$

The cancellation law in M implies that $\sim$ is an equivalence relation on $M \times M$. We define the *Grothendieck group* of M to be $\text{Groth}(M) = (M \times M)/\sim$ (the set of equivalence classes) with the addition induced by

$$(x, y) + (x', y') = (x + x', y + y').$$

This is a well-defined addition on $\text{Groth}(M)$, and that in $\text{Groth}(M)$, the two classes $(x, y), (y, x)$ are additive inverses of each other. So, indeed, $\text{Groth}(M)$ is a group. The map $i : M \to \text{Groth}(M)$ defined by $i(x) = (x, 0)$ is an injective monoid homomorphism of M into $\text{Groth}(M)$, which may be viewed as an inclusion $M \subseteq \text{Groth}(M)$. Note that $(x, y) = i(x) - i(y) = x - y$, so in particular, $\text{Groth}(M)$ is the additive group generated by M. Any monoid homomorphism f of M into an abelian group G extends uniquely to a group homomorphism $f : \text{Groth}(M) \to G$ by the rule $f(x - y) = f(x) - f(y) \in G$. This is the universal property of $\text{Groth}(M)$. Lastly, if M has a (commutative) multiplication which makes it into a semiring, i.e, that distributes over the sum in M, then

$$(x, y)(x', y') = (xx' + yy', yx' + xy')$$

induces a (commutative) multiplication on $\text{Groth}(M)$ that makes it into a (commutative) ring.

We may now apply the above machinery to the commutative semiring $M = M(F)$.

Definition 1.3.1. *$\hat{W}(F) = \text{Groth}(M(F))$ is called the Witt-Grothendieck ring of quadratic forms over the field F.*

Every element of $\hat{W}(F)$ has the formal expression $q_1 - q_2$, where q_1, q_2 are nonsingular quadratic forms, or rather, isometry classes of such forms. Since $M(F) \subseteq \hat{W}(F)$, the two statements $q_1 = q_2 \in \hat{W}(F)$ and $q_1 \cong q_2$ are synonymous.

Now, consider the dimension map $\dim : M(F) \to \mathbb{Z}$, which is a semiring morphism on $M(F)$. This extends uniquely (via the universal property) to a surjective ring morphism $\dim : \hat{W}(F) \to \mathbb{Z}$, by $\dim(q_1 - q_2) = \dim q_1 - \dim q_2$.

Definition 1.3.2. *The kernel of the morphism* $\dim : \hat{W}(F) \to \mathbb{Z}$, *denoted by* $\hat{I}F$ *is called the fundamental ideal of* $\hat{W}(F)$.

Proposition 1.3.3. $\hat{I}F$ *is additively generated by the expressions* $\langle a\rangle - \langle 1\rangle$, $0 \neq a \in F$.

Proof. If $z \in \hat{I}F$, then $z = q_1 - q_2$, where q_1 and q_2 have the same dimension. Say, $q_1 = \langle a_1, ..., a_n\rangle$, $q_2 = \langle b_1, ..., b_n\rangle$. Then

$$z = \sum_i (\langle a_i\rangle - \langle b_i\rangle) = \sum_i (\langle a_i\rangle - \langle 1\rangle) - \sum_i (\langle b_i\rangle - \langle 1\rangle).$$

□

By the homomorphism theorem, we have $\hat{W}(F)/\hat{I}F \cong \mathbb{Z}$.

It is important to observe that the Witt-Grothendieck ring has the same problem of regular forms: hyperbolicity scapes of them. To solve this situation in our ring theoretic point of view, we consider another important ideal of $\hat{W}(F)$, the ideal of all hyperbolic spaces and their "additive inverses", denoted by $\mathbb{Z} \cdot \mathbb{H}$ (this is an ideal by corollary 1.1.32.

Definition 1.3.4. *The factor ring* $W(F) = \hat{W}(F)/\mathbb{Z} \cdot \mathbb{H}$ *is called the Witt Ring of* F.

Now, some consequences of this definition:

Proposition 1.3.5.

a - The elements of $W(F)$ *are in one-to-one correspondence with the isometry classes of all anisotropic forms.*

b - Two nonsingular forms q, q' *represent the same element in* $W(F)$ *if and only if* $q_a \cong q'_a$ *i.e, if the anisotropic part (conform 1.2.3) of* q *and* q' *are isometric. In this case,* q *and* q' *are said to be Witt-similar.*

c - If $\dim q = \dim q'$, *then* q *and* q' *represent the same element in* $W(F)$ *if and only if* $q \cong q'$.

Proof. For the item (a), since the form $\mathbb{H}$ represents the element 0 in $W(F)$ and $\mathbb{H} \cong \langle a, -a\rangle$, we have $-\langle a\rangle = \langle -a\rangle \in W(F)$ for all $a \in \dot{F}$. In particular, every element of $W(F)$ is represented by a form q. If we write down the Witt decomposition of q, say $q = q_h \perp q_a$, then q and q_a represent the same element in $W(F)$ (since $q_h = 0$ in $W(F)$). Therefore, each element of $W(F)$ is represented by a suitable anisotropic form. For the proof of item (a), it remains only to show that, if q and q' are anisotropic forms, then $q = q' \in W(F) \Rightarrow q \cong q'$. But $q = q' \in W(F)$ implies that $q = q' + m\mathbb{H} \in \hat{W}(F)$ for some integer m. Without loss of generality, we may assume that $m \geq 0$. Then we have an isometry $q \cong q' \perp m\mathbb{H}$, which implies that $m = 0$ (since q is anisotropic). Thus, indeed, $q \cong q'$. Items (b) and (c) are direct consequence of item (a). □

Moreover, the Witt ring construction behaves functorially:

Proposition 1.3.6. *$\hat{W}$ and W are both functors from fields of characteristic not 2 to commutative rings.*

Proof. We just to worry about morphisms. Let $f : K \to L$ be a morphism of fields (of characteristic not 2) and (V, B) be a K-quadratic space. We can built a L-quadratic space (V^L, B^L) as follow: $V^L := L \otimes_K V$ and B^L is defined by the rule $B^L(x \otimes u, y \otimes v) = xy \cdot f(B(u, v))$. By the universal property of tensor product, we have that B^L is in fact, a bilinear symmetric form. Then, we have a semiring morphism $\tilde{f} : M(K) \to M(L)$, given by $[(V, B)] \mapsto [(V^L, B^L)]$. Note that $f \mapsto \tilde{f}$ is a functor (preserves *id* and 0). Finally, the functoriality of $\hat{W}$ is consequence of the universal property of Grothendieck construction, and the functoriality of W is consequence of the homomorphism theorem. □

Definition 1.3.7. *The image of the ideal $\hat{I}F$ under the natural projection $\hat{W}(F) \to W(F)$ will be denoted by IF. This is called the fundamental ideal of $W(F)$.*

Proposition 1.3.8. *A form q represents an element in $IF \subseteq W(F)$ if and only if $\dim q$ is even.*

Proof. ($\Rightarrow$) if q represents an element in IF, then there exists an equation $q = q_1 - q_2 + m\mathbb{H} \in \hat{W}(F)$, where $m \in \mathbb{Z}$ and $\dim q_1 = \dim q_2 = k$. Applying the map dim, we see that $\dim q = 2m + 2k$.

($\Leftarrow$) We can assume without loss of generality that q is a binary form $q = \langle a, b\rangle$. Then q is the image of $\langle a\rangle - \langle -b\rangle \in \hat{I}F$ under the natural projection $\hat{W}(F) \to W(F)$. By definition, this says that $q \in IF \subseteq W(F)$. □

The ring epimorphism $\dim : \hat{W}(F) \to \mathbb{Z}$ induces another epimorphism

$$\hat{W}(F)/\mathbb{Z} \cdot \mathbb{H} = W(F) \to \mathbb{Z}/2\mathbb{Z},$$

which we shall denote by $\dim_0$. By the above proposition, $\ker(\dim_0) = IF$, so we obtain

Corollary 1.3.9. $\dim_0$ *defines an isomorphism $W(F)/IF \cong \mathbb{Z}/2\mathbb{Z}$.*

Now, we going to search for the relationships connecting $\hat{W}(F)$ to $\dot{F}/\dot{F}^2$ and $W(F)$ to $\dot{F}/\dot{F}^2$. Let us recall the meaning of the discriminant of a form $q \in M(F)$, $d(q) = \det(q) \cdot \dot{F}^2$. We have a monoid morphism $d : M(F) \to \dot{F}/\dot{F}^2$. By

$$d(q_1 - q_2) = d(q_1)d(q_2)^{-1} = d(q_1)d(q_2),$$

this extends to a homomorphism d from the additive group $\hat{W}(F)$ to $\dot{F}/\dot{F}^2$. Since $d(\mathbb{H}) = -1 \cdot \dot{F}^2$, the homomorphism d does not factor through $W(F)$. However, there is a clever way to remedy this.

Let q be a (nonsingular) form of dimension n. We define the "signed discriminant" of q by $d_\pm(q) = (-1)^{n(n-1)/2}d(q) \in \dot{F}/\dot{F}^2$. The obvious advantage of this signed discriminant is that $d_\pm(\mathbb{H}) = 1 \cdot \dot{F}^2$. However, $d_\pm(q \perp q') = d_\pm(q)d_\pm(q')$ fails in general: $d_\pm(\mathbb{H}) = 1 \cdot \dot{F}^2$, $d_\pm(\langle 1, 1\rangle) = -1 \cdot \dot{F}^2$ but $d_\pm(\langle 1, 1\rangle \perp \mathbb{H}) = 1 \cdot \dot{F}^2$. To restore the homomorphism property, we look at $d_\pm$ together with $\dim_0$, and manufacture a bigger group to receive the combined invariant. This new group is an extension of $\dot{F}/\dot{F}^2$ by $\mathbb{Z}/2\mathbb{Z}$. Namely, we define (set theoretically) $Q(F) = \mathbb{Z}/2\mathbb{Z} \times (\dot{F}/\dot{F}^2)$, and introduce on it the binary operation $(e, d) \cdot (e', d') = (e + e', (-1)^{ee'}dd')$ (not the direct product operation!).

Lemma 1.3.10. *$Q(F)$ with the operation defined above is an abelian group.*

Proof. Let $(a,d),(b,e),(c,f) \in Q(F)$.

$$\begin{aligned}[(a,d)\cdot(b,e)]\cdot(c,f) &= (a+b,(-1)^{ab}de)\cdot(c,f)\\ &= (a+b+c,(-1)^{(a+b)c}(-1)^{ab}def)\\ &= (a+b+c,(-1)^{ab+ac+bc}def),\end{aligned}$$

and

$$\begin{aligned}(a,d)\cdot[(b,e)\cdot(c,f)] &= (a,b)\cdot(b+c,(-1)^{bc}ef)\\ &= (a+b+c,(-1)^{a(b+c)}(-1)^{bc}def)\\ &= (a+b+c,(-1)^{ab+ac+bc}def).\end{aligned}$$

Then $\cdot$ is associative. $(a,b)\cdot(0,1) = (a+0,(-1)^{a0}b1) = (a,b)$ and $(0,1)\cdot(a,b) = (0+a,(-1)^{0a}1b) = (a,b)$, hence $(0,1)$ is the identity element. Finally,

$$(e,d)\cdot(e,(-1)^e d) = (e+e,(-1)^{ee}(-1)^e dd) = (0,1).$$

Therefore, $Q(F)$ is a group. Moreover,

$$(a,d)\cdot(b,e) = (a+b,(-1)^{ab}de) = (b+a,(-1)^{ba}ed) = (b,e)\cdot(a,d),$$

so $Q(F)$ is an abelian group. □

Note that the "inclusion" $d \mapsto (0,d)$ identifies $\dot{F}/\dot{F}^2$ with a subgroup of index 2 in $Q(F)$.

Proposition 1.3.11. $(\dim_0, d_\pm)$ *defines a monoid epimorphism from* $M(F)$ *to* $Q(F)$. *This extends to a group epimorphism* $\hat{W} \to Q(F)$. *The latter induces a group isomorphism* $f : W(F)/I^2F \cong Q(F)$.

Proof. The map $M(F) \to Q(F)$ is given by $q \mapsto (\dim_0(q), d_\pm(q)) \in Q(F)$. To check that it is a monoid homomorphism, we calculate as follows (where $\dim(q) = n$, and $\dim(q') = n'$):

$$\begin{aligned}(\dim_0, d_\pm)(q)\cdot(\dim_0, d_\pm)(q') &= (n,(-1)^{n(n-1)/2}d(q))\cdot(n',(-1)^{n'(n'-1)/2}d(q'))\\ &= (n+n',(-1)^{nn'}(-1)^{[n(n-1)+n'(n'-1)]/2}d(q)d(q'))\\ &= (n+n',(-1)^{(n+n')(n+n'-1)/2}d(q\perp q'))\\ &= (\dim_0, d_\pm)(q\perp q') \in Q(F).\end{aligned}$$

Further, $M(F) \to Q(F)$ is clearly an epimorphism, since

$$(\dim_0, d_\pm)(\langle a\rangle) = (1, a\cdot\dot{F}^2) \text{ and } (\dim_0, d_\pm)(\langle 1,-a\rangle) = (0, a\cdot\dot{F}^2).$$

By the universal property of $\hat{W}(F)$, the map $(\dim_0, d_\pm)$ extends uniquely to a group epimorphism from $\hat{W}(F)$ to $Q(F)$. Moreover, since $(\dim_0, d_\pm)(\mathbb{H}) = (0,(-1)d(\mathbb{H})) = (0,1)$ is the identity element of $Q(F)$, we get an induced epimorphism $W(F) \to Q(F)$. We claim that this homomorphism is trivial on I^2F. By proposition 1.3.3, IF is additively generated by binary forms $\langle 1,a\rangle$, so I^2F is additively generated by the four-dimensional forms $\langle 1,a\rangle \otimes \langle 1,b\rangle$. But

$$(\dim_0, d_\pm(\langle 1,a,b,ab\rangle) = (0,(-1)^0 a\cdot b\cdot ab\cdot\dot{F}^2) = (0,1),$$

so we obtain an epimorphism $f : W(F)/I^2F \to Q(F)$. We shall show that f is an isomorphism,

by constructing an inverse $g : Q(F) \to W(F)/I^2F$. We simply set $g(0,a) = \langle 1, a\rangle \pmod{I^2F}$, $g(1,a) = \langle a\rangle \pmod{I^2F}$, and carry out the following computation:

$$\begin{aligned} g[(0,a)(0,b)] &= g(0,ab) = \langle 1, -ab\rangle \equiv \langle 1, -a, 1, -b\rangle \\ &\equiv g(0,a) + g(0,b) \pmod{I^2F}, \\ g[(1,a)(1,b)] &= g(0,-ab) = \langle 1, ab\rangle \equiv \langle a, b\rangle \\ &\equiv g(1,a) + g(1,b) \pmod{I^2F} \\ g[(0,a)(1,b)] &= g(1,ab) = \langle ab\rangle \\ &\equiv \langle 1, -a, b\rangle \equiv g(0,a) + g(1,b) \pmod{I^2F}. \end{aligned}$$

Hence, g is a group homomorphism. By construction, $f \circ g = Id_{Q(F)}$, and g splits the surjection f. But, by $g(1,a) \equiv \langle a\rangle (\text{mod } I^2F)$, g is onto. It follows that f and g are inverse isomorphisms of each other. □

Corollary 1.3.12 (Pfister)**.** *I^2F consists of classes of even-dimensional forms q for which $d(q) = (-1)^{n(n-1)/2}$ (where $n = \dim(q)$).*

Proof. This is just restating that $f : W(F)/I^2F \to Q(F)$ is a monomorphism. □

Corollary 1.3.13 (Pfister)**.** *The restriction of f induces an isomorphism from IF/I^2F onto $\dot{F}/\dot{F}^2$.*

Proof. Is just the fact that the image of IF under f is $\{0\} \times \dot{F}/\dot{F}^2$. □

Corollary 1.3.14. *The following are equivalent:*

i - *$\hat{W}(F)$ is a noetherian ring.*

ii - *$W(F)$ is a noetherian ring.*

iii - *$\dot{F}/\dot{F}^2$ is a finite group.*

Proof. (1)⇒(2) Is just the fact of $W(F) = \hat{W}(F)/\mathbb{Z}\mathbb{H}$, and that a quotient ring of any noetherian ring is noetherian.

(2)⇒(3) Since $W(F)$ is assumed noetherian, IF is a finitely generated $W(F)$-module, so IF/I^2F is a finitely generated $W(F)/IF$-module. But $W(F)/IF \cong \mathbb{Z}_2$, so IF/I^2F must be finite. It follows from corollary 1.3.13 that $\dot{F}/\dot{F}^2$ is finite.

(3)⇒(1) By the diagonalization theorem, $\hat{W}(F)$ is additively generated by $\langle a\rangle$. $a \in \dot{F}/\dot{F}^2$. Thus, (3) implies that $\hat{W}(F)$ is a finitely generated abelian group. As a ring, of course, $\hat{W}(F)$ is then noetherian. □

Witt rings are amazing, but where are the examples?

Calm down my dear friends. The examples are hard to compute. However, we do not let you without someone. Let's start with this definition.

Definition 1.3.15. *A field F is said to be quadratically closed if every element of F is a square, i.e, if $F^2 = F$.*

Proposition 1.3.16. *F is a quadratically closed field if and only if $\dim : \hat{W}(F) \to \mathbb{Z}$ is a (ring) isomorphism. In this case, $W(F) \cong \mathbb{Z}_2$ (by $\dim_0$).*

Proof. ($\Rightarrow$) if F is quadratically closed, then $\langle a\rangle \cong \langle 1\rangle$ for all $a \in \dot{F}$ and $q \cong \dim q\langle 1\rangle$ for every regular form q. This implies that dim is an isomorphism.

($\Leftarrow$) if dim is an isomorphism, then $\langle a\rangle \cong \langle 1\rangle$ for every $a \in \dot{F}$, so every $a \in F$ is a square. □

Proposition 1.3.17. *Let $F = \mathbb{R}$ (or any euclidean field)[4]. Then:*

a - There exist exactly two anisotropic forms up to isometry at each (positive) dimension. For dimension $n > 0$, these are $n\langle 1\rangle$) and $n\langle -1\rangle$.

b - $W(F) \cong \mathbb{Z}$.

c - (Sylvester's Law of Inertia) Two (nonsingular) forms over F are equivalent if and only if they have the same dimension and the same signature (the term will be defined in the proof).

d - $\hat{W}(F) \cong \mathbb{Z} \oplus \mathbb{Z}$. As a ring, $\hat{W}(F)$ is isomorphic to the integral group ring $\mathbb{Z}[G]$ of a 2-element group G.

Proof. a - The conclusion follow by that if a form is anisotropic, in its diagonalization we cannot have coefficients of mixed signs.

b - Direct consequence of item a.

c - Let us first define "signature". We claim that, in a diagonalization of a form q, the number of positive coefficients (hence also the number of negative coefficients) is uniquely determined. In fact, let q be a form of dimension n, and suppose that $r\langle 1\rangle \perp (n-r)\langle -1\rangle$, $s\langle 1\rangle \perp (n-s)\langle -1\rangle$ are two diagonalizations of q, where $s \geq r$. Passing to the Witt Ring $W(F)$, we have an equation

$$r\langle 1\rangle - (n-r)\langle 1\rangle = s\langle 1\rangle - (n-s)\langle 1\rangle \in W(F),$$

which implies that $2r\langle 1\rangle = 2s\langle 1\rangle \in W(F)$. By the item b, we have $r = s$. Thus, we may write $n_+ = r$ (number of positive terms) and $n_- = (n-r)$ (number of negative terms). The *signature* of q is defined to be

$$n_+ - n_- = n_+ - (n - n_+) = 2n_+ - n.$$

Thus, two forms are equivalent if and only if they have the same n and the same n_+, i.e, if and only if they have the same dimension and the same signature. This is Sylvester's Law of Inertia.

d - It is suffice to show that $\langle 1\rangle, \langle -1\rangle$ form a free $\mathbb{Z}$-basis for $\hat{W}(F)$. We already know that they span $\hat{W}(F)$. To show that they are independent, let $a\langle 1\rangle + b\langle -1\rangle = 0$ in $\hat{W}(F)$, where $a, b \in \mathbb{Z}$. Passing to $W(F)$, we see that $a = b$. Then $a = b = 0$.

□

Now, we are interested in writing down full sets of generators and relations for $\hat{W}(F)$ in the category of commutative rings, as well as in the category of abelian groups. Once we estabilish such results, then similar results may be derived for $W(F)$, since $W(F) = \hat{W}(F)/\mathbb{Z} \cdot \mathbb{H}$.

We first consider $\hat{W}(F)$ as a commutative ring. The elements $\langle a\rangle$ ($a \in \dot{F}$) generate $\hat{W}(F)$, and satisfy the following properties:

I - $\langle a^2\rangle = 1$ (the identity of the ring);

II - $\langle a\rangle \cdot \langle b\rangle = \langle ab\rangle$, for $a, b \in \dot{F}$;

[4]Euclidean fields will be defined in 1.4.8

III - $\langle a\rangle + \langle b\rangle = \langle a+b\rangle \cdot (1 + \langle ab\rangle)$, where $a, b, a+b \in \dot{F}$.

Our aim is to prove that these are essentially all the relations among the symbols $\langle a\rangle$, $a \in \dot{F}$. The precise meaning of this statements the content of the following:

Theorem 1.3.18. *Let $\mathcal{F}$ be the free commutative ring generated by the symbols $[a]$ $(a \in \dot{F})$. Let $\mathcal{R}$ be the ideal of $\mathcal{F}$ generated by the elements*

R1 - $[1] - 1$*;*

R2 - $[ab] - [a]\cdot[b]$*, $a, b \in \dot{F}$, and*

R3 - $[a] + [b] - [a+b]\cdot(1 + [ab])$*, $a, b, a+b \in \dot{F}$.*

Then, the factor ring $X = \mathcal{F}/\mathcal{R}$ is isomorphic to $\hat{W}(F)$.

Proof. By the universal property of the free commutative ring $\mathcal{F}$, and by I, II and III, we have a ring surjection $f : X \to \hat{W}(F)$. We need only show that there exists an inverse. Thus, we try to define first a monoid homomorphism $\varphi : M(F) \to X$. For a given quadratic form q. take any diagonalization of q, say, $\langle a_1, ..., a_n\rangle$. We propose to set $\varphi(q) = [a_1] + ... + [a_n] \in X$. We must show, however, that $\varphi(q)$ does not depend on the particular diagonalization of q chosen above. This means that if $\langle b_1, ..., b_n\rangle$ is another diagonalization of q, we must show that $\sum[a_i] = \sum[b_i] \in X$. By Witt's Chain Equivalence Theorem (1.2.5), we may suppose that $\langle a_1, ..., a_n\rangle$ is actually simply-equivalent to $\langle b_1, ..., b_n\rangle$. Without loss of generality, we may assume that $a_i = b_i$ for $i \geq 3$, and $\langle a_1, a_2\rangle \cong \langle b_1, b_2\rangle$. Consequently, it is enough to show that

$$\langle a_1, a_2\rangle \cong \langle b_1, b_2\rangle \Rightarrow [a_1] + [a_2] = [b_1] + [b_2] \in X. \qquad (*)$$

Before we proceed, we must deduce some consequences of the relations in (R1),(R2),(R3), in order to know more about X. We claim that, for every $a \in \dot{F}$, $[a^2] = 1 \in X$. To see this, we calculate $[a] + [a]$ in two different ways.

(A) Since $a + a = 2a \neq 0$, (R3) implies $[a] + [a] = [2a]\cdot(1 + [a^2]) \notin X$.

(B) By (R1) and the distributive law, we have

$$\begin{aligned} [a] + [a] &\overset{R1}{=} [a]\cdot([1] + [1]) \\ &\overset{R3}{=} [a]\cdot[2]\cdot(1 + [1]) \\ &\overset{R2}{=} [2a]\cdot(1 + [1]) \in X. \end{aligned}$$

But (R1) implies that each $[b]$ $(b \in \dot{F})$ is a unit in X. Comparison of (A) and (B) then yields the desired information: $[a^2] = 1 \in X$.

Coming back to (*), we write $b_1 = a_1x^2 + a_2y^2$, and $a_1a_2 = b_1b_2c^2$ $(c \in \dot{F})$. We have two cases:

i - $x = 0$ or $y = 0$. Suppose, for instance, $x = 0$ ($y = 0$ is similar). Then $b_1 = a_2y^2 \Rightarrow [b_1] = [a_2y^2] = [a_2] \in X$. On the other hand,

$$[a_1] = \left[b_2 \cdot \frac{b_1}{a_2} \cdot c^2\right] = [b_2y^2c^2] = [b_2] \in X.$$

Hence, (*) follows.

ii - $x \neq 0$, $y \neq 0$. Then, in X, we have

$$\begin{aligned}[a_1] + [a_2] &= [a_1x^2] + [a_2y^2] \\ &= [a_1x^2 + a_2y^2] \cdot (1 + [a_1a_2(xy)^2]) \\ &= [b_1] \cdot (1 + [b_1b_2]) \\ &= [b_1] + [b_2].\end{aligned}$$

Thus $\varphi : M(F) \to X$ is well-defined and is clearly a monoid homomorphism. By the universal property of $\hat{W}(F)$, φ extends to a group homomorphism $\varphi : \hat{W}(F) \to X$, which is evidently an inverse for $f : X \to \hat{W}(F)$. The latter is therefore a ring isomorphism.

□

Theorem 1.3.19. *Let $\mathcal{F}'$ be the free abelian group generated by the symbols $\{a\}$, $a \in \dot{F}$. Let $\mathcal{R}'$ be the subgroup of $\mathcal{F}'$ generated by the elements:*

R'1 - $\{ab^2\} - \{a\}$, $a, b \in \dot{F}$;

R'2 - $\{a\} + \{b\} - \{a + b\} - \{ab(a + b)\}$, $a, b, a + b \in \dot{F}$.

Then, the factor group $X' = \mathcal{F}'/\mathcal{R}'$ is isomorphic to $\hat{W}(F)$.

Proof. Analogous the theorem 1.3.18. □

It is now easy to derive similar results for $W(F)$. In the category of commutative rings, we need only add the relation (R4): $[1] + [-1]$ to (R1),(R2),(R3); and in the category of abelian groups, we need only add the relation (R'3): $\{1\} + \{-1\}$ to (R'1) and (R'2).

1.4 Orderings on Fields

In atempt to apply quadratic forms in field theory we quickly found orderings in the process. So, to avoid further complications, we decide to do a brief introduction to orderings on fields and estabilish some notations.

Definition 1.4.1. *A field F is said to be formally real if -1 is not a sum of squares in F. Otherwise, we say that F is nonreal.*

For an arbitrary field F, let $\sigma(F)$ denote the set of elements of F that can be expressed as a sum of squares in F. We shall also write $\dot{\sigma}(F)$ for $\sigma(F) \setminus \{0\}$.

Proposition 1.4.2.

a - $\dot{\sigma}(F)$ is a subgroup of $\dot{F}$ that is closed inder addition.

b - If F is nonreal and char$(F) \neq 2$, then $\sigma(F) = F$.

c - If F is formally real, then char$(F) = 0$.

Proof. a - $1 = 1^2 \in \sigma(F)$. Now, let $x, y \in \dot{\sigma}(F)$, $x = x_1^2 + ... + x_n^2$ and $y = y_1^2 + ... + y_m^2$. We have

$$xy = (x_1^2 + ... + x_n^2)(y_1^2 + ... + y_m^2) = \sum_{i=1}^{n} \sum_{j=1}^{m} x_i^2 y_j^2$$

and

$$x^{-1} = \frac{x}{x^2} = \left(\frac{x_1}{x}\right)^2 + \left(\frac{x_2}{x}\right)^2 + ... + \left(\frac{x_n}{x}\right)^2.$$

Therefore, $\dot{\sigma}(F)$ is a subgroup of $\dot{F}$.

b - Let $x \in F$. Since the hyperbolic plane $\langle 1, -1\rangle$ is universal (remember that $\text{char}(F) \neq 2$), there exist $y, z \in F$ such that $x = y^2 - z^2$. If $-1 \in \sigma(F)$, we get

$$x = y^2 + (-1)z^2 \in \sigma(F) + \sigma(F) \cdot \sigma(F) \subseteq \sigma(F).$$

Hence, $\sigma(F) = F$.

c - If $\text{char}(F) = p \neq 0$, then $p \cdot 1 = 0$ and $-1 = 1 + ... + 1$ ($(p-1)$-times) is a sum of squares.

□

Definition 1.4.3. *An ordering on a field F is the assignment of a proper subset $P \subseteq F$ (called the positive cone of the ordering) which posseses the following properties:*

P1 - $P + P \subseteq P$;

P2 - $P \cdot P \subseteq P$;

P3 - $P \cup (-P) = F$.

Given such a set P, we shall say briefly that F is ordered by P, or that (F, P) is an ordered field.

Proposition 1.4.4. *Let (F, P) be any ordered field. Then:*

a - $\sigma(F) \subseteq P$.

b - $char(F) \neq 2$.

c - $-1 \notin P$, *and* $P \cap (-P) = \{0\}$.

d - F *is formally real (and so* $char(F) = 0$*).*

e - $\dot{P} := P \setminus \{0\}$ *is a subgroup of index* 2 *in* $\dot{F}$.

f - *If* $P' \subseteq F$ *gives another ordering on* F, *then* $P \subseteq P' \Rightarrow P = P'$.

Proof. a - Since $P + P \subseteq P$, it is suffices to prove that $F^2 \subseteq P$. Let $x \in F$. By P3, we have $x \in P$ or $-x \in P$. If $x \in P$, then $x^2 = x \cdot x \in P \cdot P \subseteq P$. If $-x \in P$, then $x^2 = (-x)(-x) \in P \cdot P \subseteq P$.

b - Otherwise, $-1 = 1 \in P$ by (a), and $P = -P$, contradicting the very definition of an ordering.

c - Assume that $-1 \in P$. For any $a \in F$, we have

$$a = \left(\frac{a+1}{2}\right)^2 + (-1)\left(\frac{a-1}{2}\right)^2 \in P + P \cdot P \subseteq P,$$

contradicting the fact of P be a proper subset of F. Therefore $-1 \notin P$. Next, consider $x \in P \cap (-P)$. If $x \neq 0$, we would have $-1 = (x^{-1})^2 x(-x) \in P$, contradiction. This shows that $P \cap (-P) = \{0\}$.

d - Since $-1 \notin P$ and $\sigma(F) \subseteq P$, we have $-1 \notin \sigma(F)$, so F is formally real.

e - For $x \in \dot{P}$, we have $x^{-1} = (x^{-1})^2 x \in \dot{P}$. Hence $\dot{P}$ is a subgroup of $\dot{F}$. Since $\dot{F} = \dot{P} \cup (-\dot{P})$, we have $[\dot{F} : \dot{P}] = 2$.

f - $1 \in \sigma(F) \subseteq P$ and $P \subseteq P'$. Assume that there exist $x \in P' \cap (-P)$, $x \neq 0$. Then $-1 = (x^{-1})^2 x(-x) \in P'$, contradiction.

□

In view of P3 and (b) in the above proposition, we see that F is the disjoint union of $\{0\}, \dot{P}$ and $-\dot{P}$. This is the "law of trichotomy" in an ordered field (F, P). As usual, we may introduce the notation $x \leq_P y$ to mean that $y - x \in P$. This is a linear ordering compatible with $\cdot$ and $+$.

Let (F, P) be an ordered field. For any subfield F_0 of F, we may order F_0 by taking $P_0 := P \cap F_0$ to be its positive cone. This order is said to be **induced** (on F_0) by the ordering P on F.

The quintessential example of an ordered field is $F = \mathbb{R}$, which has (unique) ordering given by the positive cone $P = \mathbb{R}^2$. By what we said in the last paragraph, any subfield $F_0 \subseteq \mathbb{R}$ inherits and ordering $\mathbb{R}^2 \cap F_0$ from $\mathbb{R}$. Thus, the rational field $\mathbb{Q}$, all real quadratic fields, the field $\mathbb{Q}(\sqrt[3]{2})$, and the field of all real algebraic numbers, etc, are all equipped with natural orderings.

But there is nothing new in the last paragraph. There is another "non trivial" example of ordering?

This is an interesting question. Indeed, is very unintuitive think about "weird" orderings. Seems that our intuition are limited to the reals... so, let do some examples:

Example 1.4.5. *Let $F = \mathbb{Q}(\alpha)$ where $\alpha^2 = 2$. We can define an ordering P on F by using the embedding $\varphi : F \to \mathbb{R}$ with $\varphi(\alpha) = \sqrt{2}$. Similarly, we can define another ordering $P' \neq P$ on F by using the $\mathbb{Q}$-automorphism $\varphi' : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(-\sqrt{2})$ with $\varphi'(\alpha) = -\sqrt{2}$.*

Example 1.4.6. *Let $F = K(x)$, where K is a field given with an ordering P_0. We can extend this ordering on F in several ways. First, we declare a polynomial*

$$f(x) = a_0 + a_1 x + ... + a_n x^n \in K[x],\ a_n \neq 0,$$

positive if $a_n \in \dot{P}_0$. Then we declare a rational function $g(x)/f(x)$ positive if the polynomial $f(x)g(x)$ is positive. The set of positive elements in F defined in this way, together with 0, gives an ordering P_1 on F. Note that in this ordering, we have

$$0 < ... < x^{-2} < x^{-1} < a < x < x^2 < ...$$

for any $a \in \dot{P}_0$, as we can readily check. We can also get a second extension of P_0 as follows. Declare a polynomial

$$f(x) = a_r x^r + a_{r+1} x^{r+1} + ... + a_n x^n \in K[x],\ r \leq n,\ a_n, a_r \neq 0$$

positive if $a_r \in \dot{P}_0$, and extend this positivity notion to $F = K(x)$ as before. This results in a second ordering P_2 extending P_0. With respect to this ordering P_2, we have instead

$$0 < ... < x^2 < x < a < x^{-1} < x^{-2} < ...$$

*for any $a \in \dot{P}_0$. These orderings are examples of **nonarchimedean** orderings on F: these are orderings with respect to which there are elements that are larger than all integers (and hence all rational numbers) in F.*

Example 1.4.7. *Consider P_0 the usual ordering on $\mathbb{R}$. Let C be any subset of $\mathbb{R}$ with the property*

$$\text{For any pair } a < b \in \mathbb{R} : b \in C \Rightarrow a \in C$$

(for example, take C as an open interval $(-\infty, b)$). We can define an ordering P_C on $F = \mathbb{R}(x)$ as follows. For any nonzero polynomial $f(x) \in \mathbb{R}[x]$, write down the factorization of f into irreducible factors

$$f(x) = r(x - a_1)...(x - a_n)q_1(x)...q_m(x),$$

where $r, a_1, ..., a_n \in \mathbb{R}$ and the q_i's are monic irreducible quadratic polynomials. We shall take $f(x) \in \dot{P}_C$ iff $r \in \dot{P}_0$ and the number of $a_i \notin C$ is even, or $r \notin \dot{P}_0$ and the number of $a_i \notin C$ is odd. For nonzero rational functions $g(x)/f(x)$, we take (as before) $g/f \in \dot{P}_C$ iff $gf \in \dot{P}_C$. It can be shown that the P_C obtained in this manner is an ordering on $\mathbb{R}(x)$, and is, in fact, the unique ordering P on $\mathbb{R}(x)$ with respect to which $C = \{b \in \mathbb{R} : b <_P x\}$.

We finalize this section with some definitions and results that will be used throughout the entire chapter.

Definition 1.4.8. *A field F is called euclidean if F is formally real and $|\dot{F}/\dot{F}^2| = 2$ (in such field, $\dot{F} = \dot{F}^2 \cup (-\dot{F}^2)$). A field F is called pythagorean if the sum of two squares in F is always a square. In such field, $\sigma(F) = F^2$.*

Let F be a field and $a, b \in \dot{F}$. How $a^2 + b^2 = a^2(1 + (b/a)^2)$, to prove that F is pythagorean, is suffice to show that $1 + y^2 \in F^2$ for all $y \in F$.

Proposition 1.4.9. *If F is euclidean, then F is pythagorean with a unique ordering.*

Proof. We claim that $P := F^2$ is an ordering. For this P, we already have $P \neq F$, $P \cdot P \subseteq P$ and $P \cup (-P) = F$. Thus, we only need to prove that $P + P \subseteq P$, that is, F is pythagorean.

Consider a sum $1 + y^2$, where $y \in F$. If $1 + y^2 \in -F^2$, then $-1 = -(1 + y^2) + y^2 \in F$, and F is nonreal, absurd since F is euclidean. Hence, $1 + y^2 \in F^2$ and P is an ordering. Follow by proposition 1.4.4(e) that P is the unique ordering on F. □

The next result offers several important characterization of euclidean fields:

Theorem 1.4.10. *For any field F (of any characteristic), the following are equivalent:*

i - F is euclidean.

ii - F is formally real, but every quadratic extension of F is nonreal.

iii - $\sqrt{-1} \notin F$ and $F(\sqrt{-1})$ is quadratically closed (that is, $K^2 = K$).

iv - $char(F) \neq 2$ and there exist a quadratic extension $L \supseteq F$ that is quadratically closed.

Example 1.4.11. *Two immediate examples of euclidean fields are the real field $\mathbb{R}$ and the field A of algebraic numbers. Here $A = \overline{\mathbb{Q}} \cap \mathbb{R}$, where $\mathbb{Q}$ denotes the algebraic closure of $\mathbb{Q}$. Another interesting example: let $\tilde{\mathbb{Q}}$ be the field of constructible numbers, that is, $\tilde{\mathbb{Q}}$. Then $F : \tilde{\mathbb{Q}} \cap \mathbb{R}$ is an euclidean field, with $F(\sqrt{-1} = \tilde{\mathbb{Q}}$.*

Definition 1.4.12. *A field F is called **real-closed** if F is formally real, but no proper algebraic extension of F is formally real.*

An immediate consequence of 1.4.10 is

Corollary 1.4.13. *Let F be a real-closed field. Then F is euclidean (with a unique ordering F^2), and $F(\sqrt{-1})$ is quadratically closed.*

Of course, we need to prove that this definition make sense, i.e, that there is an abundant supply of real-closed fields.

Proposition 1.4.14. *Let F be any formally real field, and $\overline{F}$ be its algebraic closure. Then there exists a real-closed field R between F and $\overline{F}$.*

Proof. Consider the collection $\mathcal{S}$ of all formally real subfields of $\overline{F}$ containing F. If $\{F_\alpha\}$ is a chain (relative to inclusion) of such fields, then $F_0 = \bigcup_\alpha F_\alpha$ belongs to the same family $\mathcal{S}$. By Zorn's Lemma, there exists $R \in \mathcal{S}$ that is a maximal member of $\mathcal{S}$ with respect to inclusion. By maximality, such a field R must be real-closed. □

We note the following property of a formally real field.

Proposition 1.4.15. *If F is formally real, so is every odd-degree extension K of F.*

Corollary 1.4.16. *If F is real-closed, then any odd-degree polynomial $f \in F[x]$ has a root in F.*

Theorem 1.4.17. *For any field F, the following are equivalent:*

i - F is real-closed.

ii - F is euclidean, and every odd-degree polynomial in $F[x]$ has a root in F.

iii - $\sqrt{-1} \notin F$ and $F(\sqrt{-1})$ is algebraically closed.

Corollary 1.4.18. *The real field $\mathbb{R}$ is real-closed, and the complex field $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ is algebraically closed.*

Proof. To begin with, $\mathbb{R}$ is a euclidean field. By the usual continuity argument in calculus, every real polynomial of odd degree has a real root. Therefore, (ii) in the above theorem is satisfied for $F = \mathbb{R}$, and we get the desired conclusions from (i) and (iii). □

We shall introduce the notion of "real-closure", which will be used in the next section.

Definition 1.4.19. *Let F be a field ordered by a positive cone P. An extension field $R \supseteq F$ is called a **real closure** of F (relative to P) if it satisfies the following three conditions:*

i - R is real-closed.

ii - R is algebraic over F.

iii - The given ordering on F is induced by the unique ordering on R (in other words, $P = R^2 \cap F$).

We have the following existence and uniqueness result.

Theorem 1.4.20.

i - Every ordered field (F, P) posseses a real-closure.

ii - If (F_1, P_1), (F_2, P_2) are ordered fields and R_1, R_2 are their real-closures, then any order isomorphism $f : F_1 \to F_2$ (isomorphism such that $f(P_1) = P_2$) extends uniquely to an isomorphism $\tilde{f} : R_1 \to R_2$, which is automatically an order isomorphism.

This theorem means that the possible orderings which can be put on F are in 1-1 correspondence with the F-isomorphism classes of the real-closed algebraic extensions of F.

1.5 Pfister's Local-Global Principle

Now, we will make our first application of theory of ordered fields to theory of quadratic forms. For a field F, let us write X_F (or sometimes $X(F)$ and $\mathrm{Sper}(F)$) for the (possibly empty) set of orderings on F. In order to work with X_F as a set of "points", we shall write α for a typical element in X_F, and write "$\leq_\alpha$" for the total ordering given by α on F. To reconcile this with our earlier notation, we shall write $P_\alpha = \{a \in F : a \geq_\alpha 0\}$ for the positive cone of the ordering α.

For each $\alpha \in X_F$, let us fix a real-closure F_α with respect to α (i.e, a real-closed field containing the ordered field (F, α)). Letting $r_\alpha : F \to F_\alpha$ be the inclusion map, we have a functorial homomorphism $r_\alpha^* : W(F) \to W(F_\alpha)$. Now, just as in 1.3.17, we have a canonical isomorphism $W(F_\alpha) \cong \mathbb{Z}$. The composition of these two maps gives a surjection $\mathrm{sgn}_\alpha : W(F) \to \mathbb{Z}$, which sends an F-quadratic form q to its signature $\mathrm{sgn}_\alpha(q)$ with respect to F_α.[5]

Letting α range over the set of orderings X_F, we get a "total signature" map

$$\mathrm{sgn} : W(F) \to \prod_{\alpha \in X_F} W(F_\alpha) \cong \prod_{\alpha \in X_F} \mathbb{Z},$$

which sends a form q to $(\mathrm{sgn}_\alpha(q))_{\alpha \in X_F}$ on the right hand side. One of the contents of the Pfister's Local-Global Principle is to compute the kernel of this total signature map.

Theorem 1.5.1 (Pfister's Local-Global Principle)**.** *For any field F, $Ker(sgn) = W_t(F)$, the torsion subgroup of the Witt group $W(F)$. Moreover, every element in $W_t(F)$ is 2-primary torsion.*

An equivalent way to state the first part of the theorem is that two quadratic forms q_1, q_2 over F has the same signature relative to all orderings on F iff $n \cdot q_1 = n \cdot q_2 \in W(F)$ for some integer $n \geq 1$. The second part of the theorem says that, in this case, we could taken n to be of the form 2^r for some r. Yet another way to express 1.5.1 is to say that, if a form q is hyperbolic in all real-closures of F, then for some integer $r \geq 0$, $2^r \cdot q$ is hyperbolic over F. These alternative formulations of 1.5.1 explain why this result is called a Local-Global Principle.

Before we proceed to the proof of 1.5.1, we need some technical results.

Theorem 1.5.2. *Let F be a field, $K = F(\sqrt{a})$ be a quadratic extension of F and q be an anisotropic form over F. Then q_K is isotropic over K if and only if contains a binary subform isometric to $\langle b \rangle \cdot \langle 1, -a \rangle$ for some $b \in \dot{F}$.*

Proof. ($\Rightarrow$) Is just the fact that $\langle 1, -a \rangle \cong \langle 1, -1 \rangle$.

($\Leftarrow$) Let $\langle b_1, ..., b_n \rangle$ be a diagonalization of q and assume that q_K is isotropic. Then there exists an equation

$$\sum_{i=1}^{n} b_i (x_i + y_i \sqrt{a})^2 = 0$$

where $x_i, y_i \in F$ are not all zero. Then

$$\sum_{i=1}^{n} b_i (x_i + y_i \sqrt{a})^2 = 0 \Rightarrow \sum_{i=1}^{n} b_i (x_i^2 + a y_i^2 + 2 x_i y_i \sqrt{a}) = 0$$
$$\Rightarrow \sum_{i=1}^{n} b_i x_i^2 + \sum_{i=1}^{n} b_i a y_i^2 = \sum_{i=1}^{n} b_i x_i y_i = 0,$$

[5] We could prove that the map sgn_α does not depend on the choice of F_α, or on the fact that F_α is uniquely determined up to an isomorphism.

hence the vectors $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$ are orthogonal in the quadratic space (F^n, q). Moreover, $q(x) = -aq(y)$, and this implies that x and y must both be nonzero (since q is anisotropic). Therefore, q contais the binary form

$$\langle q(x), q(y)\rangle = \langle -aq(y), q(y)\rangle \cong \langle q(y)\rangle \cdot \langle 1, -a\rangle.$$

□

Theorem 1.5.3. *Let F be a field and $K = F(\sqrt{a})$ be a quadratic extension of F. An anisotropic F-form q becomes hyperbolic over K if and only if $q \cong \theta \otimes \langle 1, -a\rangle$ for some F-form θ. In particular, the kernel of $r^* : W(F) \to W(K)$ is given by the principal ideal $W(F) \cdot \langle 1, -a\rangle$.*

Proof. The if part is just the fact that that $\langle 1, -a\rangle \cong \langle 1, -1\rangle$ and that $\theta \otimes \langle 1, -1\rangle \cong (\dim \theta) \cdot \langle 1, -1\rangle$. For the another part, we induct on $m = (\dim q)/2$. In the case $m = 0$ is nothing to do, and starts the induction. If $m > 0$, the theorem 1.5.2 gives an isometry $q \cong b\langle 1, -a\rangle \perp q'$, where $b \in \dot{F}$ and $(\dim q')/2 = m - 1$. By Witt's Cancellation Theorem, $(q')_K$ is hyperbolic over K. Our inductive hypothesis then gives a form θ' such that $q' \cong \theta' \otimes \langle 1, -a\rangle$. We now have $q \cong b\langle 1, -a\rangle \perp (\theta' \otimes \langle 1, -a\rangle) = \theta \otimes \langle 1, -a\rangle$, where $\theta = \langle b\rangle \perp \theta'$. □

Corollary 1.5.4. *Let q be an F-form of dimension $2m$ that becomes hyperbolic over $K = F(\sqrt{a})$. Then:*

a - $-a \cdot q \cong q$ over F.

b - If q is anisotropic over F, then $d(q) = (-a)^m$.

c - If q also becomes hyperbolic over $F(\sqrt{a})$, then $2q = 0 \in W(F)$.

Proof. a - By theorem 1.5.3, we can write $q \cong r \cdot \mathbb{H}_F \perp \theta \otimes \langle 1, -a\rangle$ for some F-form θ. Since $-a \cdot \mathbb{H}_F \cong \mathbb{H}_F$ and $-a\langle 1, -a\rangle \cong \langle 1, -a\rangle$, it follows that $-a \cdot q \cong q$.

b - If q is anisotropic over F, we have $r = 0$, so $\dim \theta = m$, and computing discriminants from $q \cong \theta \otimes \langle 1, -a\rangle$, show that $d(q) = (-a)^m$.

c - Assume that q is also hyperbolic over $K = F(\sqrt{a})$. If $K = F$, then $q = 0 \in W(F)$. If $K \neq F$, then by the item (a) (applied to the quadratic extension $K|F$), we have $a \cdot q \cong q$, along with $-a \cdot q \cong q$. Adding these, we get $2q = 0 \in W(F)$.

□

Now, our strategy for proving 1.5.1 is as follows. We first check the truth of 1.5.1 in two special cases, and then give the general proof by making a reduction to these special cases.

The first special case is when F is a euclidean field. In this case, F has a unique ordering α with $P_\alpha = F^2$, and the total signature map

$$\text{sgn} : W(F) \to W(F_\alpha) \cong \mathbb{Z}$$

is an isomorphism. Here $W_t(F) = \{0\}$, so 1.5.1 is certainly true.

The second special case of 1.5.1 is when F is a nonreal field, for which X_F is the empty space. Here, $\prod_{\alpha \in X_F} W(F_\alpha)$ is an "empty" direct product, which is, as usual, taken to be $\{0\}$. In this case, 1.5.1 asserts that $W(F)$ is a 2-primary torsion group. This is equivalent to saying that the ring $W(F)$ has characteristic 2^r for some integer r, so the proof of 1.5.1 boils down to checking this statement for any nonreal field F. We shall do this by appealing to the following observation on the prime ideals of $W(F)$ for any field F.

Lemma 1.5.5. *Let F be a field and $\mathfrak{p}$ be any (proper) prime ideal in $W(F)$.*

a - If $2 \in \mathfrak{p}$, then $\mathfrak{p} = IF$.

b - If $2 \notin \mathfrak{p}$, then $P := \{0\} \cup \{a \in \dot{F} : \langle a \rangle \equiv \langle 1 \rangle \, (mod\ \mathfrak{p})\}$ is an ordering on F.

Proof. Note that for any $a \in \dot{F}$, $\langle a \rangle^2 = 1 \in W(F)$ implies that $\langle a \rangle \equiv \pm 1 \, (\text{mod } \mathfrak{p})$ (since $W(F)/\mathfrak{p}$ is an integral domain). If $2 \in \mathfrak{p}$, then $\langle a \rangle \equiv 1 \, (\text{mod } \mathfrak{p})$, so for any $2n$-dimensional form q, we have $q \equiv 2n \equiv 0 \, (\text{mod } \mathfrak{p})$. Thus, $IF \subseteq \mathfrak{p}$ and the equality must hold (because IF is a maximal ideal with $WF/IF \cong \mathbb{Z}/2\mathbb{Z}$).

Now assume $2 \notin \mathfrak{p}$ and define $P := \{0\} \cup \{a \in \dot{F} : \langle a \rangle \equiv \langle 1 \rangle \, (\text{mod } \mathfrak{p})\}$. Is immediate that $P \cdot P \subseteq P$, $P \cup (-P) = F$ and $\langle -1 \rangle \not\equiv \langle 1 \rangle$ yelds $-1 \notin P$. We finish by checking that $a, b \in P$, $c := a + b \neq 0$ implies that $c \in P$. From the isometry $\langle a, b \rangle \cong \langle c \rangle \langle 1, ab \rangle$, we have $2 \equiv 2\langle c \rangle \, (\text{mod } \mathfrak{p})$. Since $2 \notin \mathfrak{p}$, we have $\langle c \rangle \equiv 1 \, (\text{mod } \mathfrak{p})$, as desired. □

For a nonreal field F, the above lemma implies that IF is the unique prime ideal of $W(F)$. But then, by a standard theorem in commutative algebra, IF must be the nilradical of $W(F)$. In particular, for the element $2 \in IF$, we have $2^r = 0 \in W(F)$ for some $r \geq 1$. This proves 1.5.1 for nonreal fields.

Now we are in a good position to complete the proof of 1.5.1.

Proof of Pfister's Local-Global Principle 1.5.1. For any F, we $W_t(F) \subseteq \text{Ker(sgn)}$ (since $\prod_\alpha \mathbb{Z}$ is torsion free). The main job is to show that if a form $q \in W(F)$ is not 2-primary torsion, then $\text{sgn}_\alpha q \neq 0$ for some ordering $\alpha \in X_F$. By Zorn's Lemma, there exists a field $K \supseteq F$ within the algebraic closure of F that is maximal with respect to the property that $q_K \in W(K)$ is not 2-primary torsion. We claim that K is euclidean.

Surely, K is formally real (for otherwise $2^r W(K) = 0$ for some r). Assume for the moment, that K has an element $a \notin \pm K^2$. By the "maximality" of K, q_K must become 2-primary torsion in $K(\sqrt{a})$ and $K(\sqrt{-a})$, and so for a large integer N, $2^N q_K$ is hyperbolic ober both $K(\sqrt{a})$ and $K(\sqrt{-a})$. But then, by corollary 1.5.4(c), $2 \cdot 2^N q_K = 0 \in W(K)$, a contradiction. This shows that K is euclidean, and we have $\text{sgn}_\alpha(q) \neq 0$ for the ordering $\alpha \in X_F$ induced on F by the unique ordering on K. □

1.6 Harrison Topology on X_F

Orderings seems to be an efficient tool to deal with questions in quadratic forms. So to accurate our results, we introduce the Harrison topology on the space X_F of orderings of a field F. For pratical reasons, let us assume that $X_F \neq \emptyset$ i.e, that F is formally real.

To set up the Harrison topology on X_F, first note that each ordering $\alpha \in X_F$ determines a map (actually a group epimorphism) $\dot{F} \to \{\pm 1\}$, given by $\alpha(x) = \text{sgn}_\alpha(x)$. Thus, we have an embedding $X_F \hookrightarrow \{\pm 1\}^{\dot{F}}$ (on the set of the functions from $\dot{F}$ to $\{\pm 1\}$).

The function space $\{\pm 1\}^{\dot{F}}$ has a natural product topology, if $\{\pm 1\}$ is given the discrete topology. Thus, there is a subspace topology induced on X_F; this is, by definition, the *Harrison topology*, named after David Harrison who first pointed out its existence in his work.

To get a better view of this topology, let us first write down the defining subbase of the product topology on $\{\pm 1\}^{\dot{F}}$:

$$H_{a,\varepsilon} = \{f : \dot{F} \to \{\pm 1\} : f(a) = \varepsilon\} \, (a \in \dot{F}, \varepsilon = \pm 1).$$

This is a clopen (closed and open) set, since its complement is $H_{a,-\varepsilon}$. Thus, $\{\pm 1\}^{\dot{F}}$ is a *Boolean space*; that is, it is compact, Hausdorff, and totally disconnected. [6] Here, of course, the Tychonoff Theorem is needed to guarantee the compactness of the space $\{\pm 1\}^{\dot{F}}$.

Theorem 1.6.1. *X_F, with the Harrison topology, is also a Boolean space.*

Proof. It is suffice to show that X_F is a closed subspace of $\{\pm 1\}^{\dot{F}}$ (since any closed subspace of a Boolean space remains Boolean). Take any map $s : \dot{F} \to \{\pm 1\}$ that does not yield an ordering. If s is identically 1 (or -1), the subbasic open set $H_{1,-1}$ (resp. $H_{1,1}$) separates s from X_F. We may thus assume that s is surjective. Using this s, we can thus talk about "positive" elements ($s(x) = 1$) and "negative" elements ($s(x) = -1$) in $\dot{F}$. However, there must exist some "positive" a, b such that $a+b$ or ab will be "negative" (since s does not yield an ordering). But then the basic open set $H_{a,1} \cap H_{b,1} \cap H_{c,-1}$ separates s from X_F. □

To get a subbasis (of open sets) for X_F, we need only take the following intersections:

$$H(a) := H_{a,1} \cap X_F = \{\alpha \in X_F : a >_\alpha 0\}\, (a \in \dot{F}).$$

The reason we can restrict our attention to $\varepsilon = 1$ is, of course, that $H_{a,-1} \cap X_F$ is given by $H(-a)$. The family $\{H(a) : a \in \dot{F}\}$ may be called the *Harrison subbasis* for the Boolean space X_F.

Corollary 1.6.2. *Let $K|F$ be a field extension. Then the map $\rho : X_K \to X_F$ obtained by the restriction of orderings is continuous and closed (with respect to the Harrison topologies on X_K and X_F).*

Proof. For any $a \in \dot{F}$, $\rho^{-1}(H_F(a)) = H_K(a)$, where the subscripts refer to the respective fields. Since $\{H_F(a) : a \in \dot{F}\}$ is a subbasis for X_F, the continuity of ρ follows. If C is a closed subset of X_K, then C is compact (since X_K is), and therefore $\rho(C)$ is also compact. It follows that $\rho(C)$ is closed in X_F. □

Next, we note that each quadratic form q over F defines a map

$$\hat{q} : X_F \to \mathbb{Z}, \text{ where } \hat{q}(\alpha) := \operatorname{sgn}_\alpha(q).$$

The significance of the Harrison topology is largely clarified by the following observation:

Proposition 1.6.3. *For each quadratic form q, the signature map is continuous with respect to the Harrison topology on X_F and the discrete topology on $\mathbb{Z}$. In fact, with the latter topology fixed, the Harrison topology is the coarsest topology on X_F that makes all the maps $\hat{q}$ continuous.*

Proof. To prove the continuity of $\hat{q}$, it is sufficient to treat the case $q = \langle a \rangle$ (since the sum of continuous functions into an additive topological group is continuous). In this case, we note that

$$\hat{q}^{-1}(i) = \{\alpha \in X_F : \operatorname{sgn}_\alpha\langle a\rangle = i\} = \begin{cases} \emptyset \text{ if } i \neq \pm 1, \\ H(a) \text{ if } i = 1, \\ H(-a) \text{ if } i = -1. \end{cases}$$

From these calculations, the desired conclusion in the proposition follow immediately. □

[6] A topological space is called *totally disconnected* if is Compact, Hausdorff and has a base of clopens.

Proposition 1.6.3 is another evidence that quadratic forms and orderings are "naturally" related.

Previously, we have written the total signature map in the form

$$\text{sgn} : W(F) \to \prod_{\alpha \in X_F} \mathbb{Z},$$

where the right hand side of the equation is just $\mathbb{Z}^{X_F}$ (the set of all functions $f : X_F \to \mathbb{Z}$). Since each $\hat{q}$ in 1.6.2 is continuous, we may as well use a smaller target set for "sgn", and re-express the latter as a ring homomorphism

$$\text{sgn} : W(F) \to C(X_F, \mathbb{Z}) \text{ given by } q \mapsto \hat{q},$$

where $C(X_F, \mathbb{Z})$ denotes the ring of continuous functions from X_F to $\mathbb{Z}$ (X_F with the Harrison topology and $\mathbb{Z}$ with discrete topology).

The advantage of using the smaller target group $C(X_F, \mathbb{Z})$ is that we can now more meaninfully study the cokernel of the map "sgn". In 1.5.1, we have shown that ker(sgn) is a 2-primary torsion group. Our first main result in this section is the following "dual" statement.

Theorem 1.6.4. *For the map sgn, coker(sgn) is also a 2-primary torsion group.*

The proof of this is based on the lemma below concerning to the existence of quadratic forms in $I^n F$ with certain prescribed signature properties. Here, $I^n F$ denotes the n-th power of the "fundamental ideal" IF.

Lemma 1.6.5. *For any clopen set $C \subseteq X_F$, there exists a form $q \in I^n F$ (for some $n \geq 0$) such that $2^n \chi_C = sgn(q)$, where χ_C denotes the characteristic function on X_F associated with the subset $C \subseteq X_F$.*

Proof. Step 1. If the lemma holds for two clopen sets C_1, C_2, then it holds for $C_1 \cup C_2$. Indeed, suppose $q_1, q_2 \in I^{m_i} F$ are such that $2^{m_1} \chi_{C_1} = \text{sgn}(q_1)$ and $2^{m_2} \chi_{C_2} = \text{sgn}(q_2)$. After multiplying these equations by powers of 2 if necessary, we may assume that $m_1 = m_2 = m$. Now take the equation

$$\chi_{C_1 \cup C_2} = \chi_{C_1} + \chi_{C_2} - \chi_{C_1} \chi_{C_2},$$

and multiply it by 2^{2m} to get

$$2^{2m} \chi_{C_1 \cup C_2} = 2^m \text{sgn}(q_1 + q_2) - \text{sgn}(q_1 q_2) = \text{sgn}(q),$$

where $q = 2^m(q_1 + q_2) - q_1 q_2 \in I^{2m} F$.

Step 2. A basis of open sets in X_F is given by the sets

$$H(a_1, ..., a_n) := H(a_1) \cap ... \cap H(a_n),\ a_i \in \dot{F}. \tag{1.1}$$

Since X_F is compact, so is the given clopen set C. Thus, C can be written as a finite union of sets of the form $H(a_1, ..., a_n)$. By Step 1, the proof of the lemma is now reduced to the case where $C = H(a_1, ..., a_n)$.

Step 3. Let $q_i = \langle 1, a_i \rangle \in IF$. We have $\text{sgn}(q_i) = 2\chi_{H(a_i)}$. Therefore, for $q = q_1 \cdot ... \cdot q_n \in I^n F$, we have

$$\text{sgn}(q) = 2^n \chi_{H(a_1)} \cdots \chi_{H(a_n)} = 2^n \chi_{H(a_1, ..., a_n)}.$$

This proves the lemma for the case $C = H(a_1, ..., a_n)$. □

We are now in a good position to supply the following:

Proof of Theorem 1.6.4. Given a continuous function $f \in C(X_F, \mathbb{Z})$, let $C_i = f^{-1}(i)$ $(i \in \mathbb{Z})$. These sets are clopens, and form a partition of X_F (remember that the topology in $\mathbb{Z}$ is discrete!). Since X_F is compact, all but a finite number of the C_i's must be empty. This means that f is a bounded function on X_F, so we can express f as a finite sum $\sum_{j=1}^{n} i \cdot \chi_{C_i}$. By 1.6.5,

$$2^{n_i}\chi_{C_i} \in \mathrm{Im(sgn)} \text{ for suitable } n_i \geq 0.$$

From this, it follows immediately that $2^n f \in \mathrm{Im(sgn)}$ for some n_i, as desired. □

Returning to 1.6.5, we note that there is a further self-strenghthening of this result that can be stated in the form of a "separation theorem". We shall call this "Urysohn Lemma", in view of its resemblance to the familiar topological results about separation in normal spaces.

Lemma 1.6.6 (Urysohn)**.** *For any two disjoint closed sets A, B in X_F, there exists $q \in I^n F$ (for some n) such that $sgn(q) \equiv 0$ on B, and $sgn(q) \equiv 2^n$ on A.*

Proof. The complement of B is a union of sets of the form 1.1. Since A is compact, a finite number of these, say $C_1, ..., C_r$, will cover A, and $C_i \cap B = \emptyset$. If we apply 1.6.5 to the clopen set $C = C_1 \cup ... \cup C_r$, the conclusion in Urysohn's Lemma follows immediately. □

As another application of 1.6.5, we shall give a characterization for quadratic forms q with the property that $\mathrm{sgn}_\alpha(q)$ is divisible by 2^n for every $\alpha \in X_F$, where n is a given integer. Note that these are precisely the forms q such that $\mathrm{sgn}(q) \in C(X_F, 2^n\mathbb{Z})$.

Theorem 1.6.7. *For $n \geq 0$ and any quadratic form q, the following are equivalent:*

i - $sgn(q) \in C(X_F, 2^n\mathbb{Z})$.

ii - $2^t \cdot q \in I^{t+n}F$ *for some integer* $t \geq 0$.

Proof. (ii)⇒(i): Since even-dimensional forms have even signature at any ordering, $\mathrm{sgn}(IF) \subseteq C(X_F, 2\mathbb{Z})$. Recalling that sgn is a ring homomorphism, we have $\mathrm{sgn}(I^m F) \subseteq C(X_F, 2^m\mathbb{Z})$ for any m. Thus, if $2^t \cdot q \in I^{t+n}F$, we get $2^t \cdot \mathrm{sgn}(q) \in C(X_F, 2^{t+n}\mathbb{Z})$, and cancelling 2^t, we have (i).

(i)⇒(ii): Assuming (i), let $D_i = (\mathrm{sgn}(q))^{-1}(2^n i)$: these clopen sets form a partition of X_F. As before, at most a finite number of these clopen sets can be nonempty, so we can resolve $\mathrm{sgn}(q)$ in a finite sum

$$\mathrm{sgn}(q) = \sum_i 2^n i \cdot \chi_{D_i}.$$

For each $D_i \neq \emptyset$, apply 1.6.5 to find a form $q_i \in I^{m_i}F$ such that $2^{m_i}\chi_{D_i} = \mathrm{sgn}(q_i)$. Since only a finite number of these are involved, we may again arrange that all m_i's be equal (say $= m$). Thus,

$$2^m \cdot \mathrm{sgn}(q) = \sum_i 2^n i \cdot 2^m \chi_{D_i} = \sum_i 2^n i \cdot \mathrm{sgn}(q_i).$$

By Pfister's Local-Global Principle 1.5.1, it follows that

$$2^m \cdot \mathrm{sgn}(q) = \sum_i 2^n i \cdot q_i + W_t(F).$$

Multiplying this by a sufficiently large power of 2, say 2^k, we can eliminate the torsion (error) term, and arrive at

$$2^{k+m}q = 2^{n+k}\sum_i i \cdot q_i \in I^{n+k+m}F,$$

which proves (ii) with $t = k + m$. □

There is another condition on the form q that is related to the two conditions in 1.6.7:

$$q \in I^n F + W_t(F). \tag{Lam}$$

The argument above on the elimination of torsion error terms shows that (Lam) implies 1.6.7(ii), and in any case, an application of the map sgn shows that (Lam) implies 1.6.7(i). In 1976, T. Y. Lam asked if (Lam) is equivalent to 1.6.7(i) and 1.6.7(ii). At around the same time, M. Marshall had raised the same question for formally real pythagorean fields F (for which $W_t(F) = 0$), and answered it affirmatively in the case where $|X_F| < \infty$. Later, a possible "yes" answer for this equivalence (for general fields F) became known as "Lam's Conjecture". More recently, this conjecture has been proved by M.Dickmann and F. Miraglia ([DM00]) using the solution of Milnor's Conjecture due to Voevodsky.

1.7 Prime ideals of $W(F)$

Returning to the "quadratic forms world", in this section we shall determine the prime ideal spectrum of the Witt Ring $W(F)$. Recall that, for any commutative ring A, the set of proper prime ideals of A, denoted by $\mathrm{Spec}(A)$, is called the *prime spectrum* of A. This is a topological space carrying the *Zarisk topology*, in which the closed sets are of the form

$$V(I) = \{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{p} \supseteq I\}, \tag{1.2}$$

where I is any ideal in A. This prime spectrum is usually not Hausdorff, but it is always compact, and a subbasis of its topology is given by the sets

$$D(a) = \{\mathfrak{p} \in \mathrm{Spec}(A) : a \notin \mathfrak{p}\}, \tag{1.3}$$

where a is any element of A.

If $\mathfrak{p} \in \mathrm{Spec}(A)$, then $A/\mathfrak{p}$ is an integral domain, so it has characteristic p, where p is a prime number or 0. We shall say, for short, that $\mathfrak{p}$ is a prime ideal of characteristic p (or symbolically, $\mathrm{char}(\mathfrak{p}) = p$).

The main idea needed for determine the prime spectrum of the Witt ring $W(F)$ is already implicit in lemma 1.5.5. Let us recall its two-part statement here. First, only prime ideal of characteristic 2 in $W(F)$ is IF; and second, if $\mathfrak{p} \in \mathrm{Spec}(W(F))$ has characteristic $\neq 2$, then

$$\alpha_{\mathfrak{p}} := \{0\} \cup \{a \in \dot{F} : \langle a \rangle \equiv 1 (\mathrm{mod}\ \mathfrak{p})\} \tag{1.4}$$

is an ordering on F. In the case where F is nonreal, therefore, we have $\mathrm{Spec}(W(F)) = \{IF\}$. We may dismiss this case in the following, and shall assume henceforth, until further notice, that F is formally real.

We start out by defining some prime ideals in $W(F)$. Eventually, these will be shown to be all

of the prime ideals. For any ordering $\alpha \in X_F$, we fix a real-closure F_α for (F, α), and define

$$\begin{aligned} \mathfrak{p}_\alpha &= \ker(\mathrm{sgn}_\alpha : W(F) \to W(F_\alpha) \cong \mathbb{Z}), \\ \mathfrak{p}_{\alpha,p} &= \{\varphi \in W(F) : \mathrm{sgn}_\alpha(\varphi) \equiv 0 (\mathrm{mod}\ p)\},\ (p = \text{ prime}). \end{aligned} \tag{1.5}$$

We have that $\mathfrak{p}_\alpha \subsetneq \mathfrak{p}_{\alpha,p}$ are both prime ideals of $W(F)$, with $\mathrm{char}(\mathfrak{p}_\alpha) = 0$ and $\mathrm{char}(\mathfrak{p}_{\alpha,p}) = p$. In fact, we have $W(F)/\mathfrak{p}_\alpha \cong \mathbb{Z}$ and $W(F)/\mathfrak{p}_{\alpha,p} \cong \mathbb{Z}/p\mathbb{Z}$.

Also, from our earlier remark about prime ideals of characteristic 2, we see that $\mathfrak{p}_{\alpha,2} = IF$ for every $\alpha \in X_F$. This means that the $\mathfrak{p}_{\alpha,2}$'s only gives one prime ideal (namely IF). But on the other hand, there is no more "collapsing" among the prime ideals defined in 1.5. First, the $\mathfrak{p}_\alpha$'s are parwise distinct from one another and from the $\mathfrak{p}_{\alpha,p}$'s. Second, if $\mathfrak{p}_{\alpha,p} = \mathfrak{p}_{\beta,q}$, considering characteristics we obtain $p = q$. Third, if $\mathfrak{p}_{\alpha,p} = \mathfrak{p}_{\beta,p}$, then

$$\begin{aligned} a >_\alpha 0 &\Rightarrow \langle a \rangle \equiv 1 (\mathrm{mod}\ \mathfrak{p}_{\alpha,p}) \\ &\Rightarrow \langle a \rangle \equiv 1 (\mathrm{mod}\ \mathfrak{p}_{\beta,p}) \\ &\Rightarrow a >_\beta 0 \end{aligned}$$

since $\mathrm{char}(\mathfrak{p}_{\beta,p}) = p \neq 2$. This shows that $\alpha = \beta \in X_F$.

Proposition 1.7.1. *The map $\alpha \mapsto \mathfrak{p}_\alpha$ gives a one-one correspondence between X_F and the set Y_F of prime ideals of characteristic 0 in $W(F)$.*

Proof. If $\mathfrak{p} \in Y_F$, 1.4 defines an ordering $\alpha_\mathfrak{p} \in X_F$. Now, we will check that $\alpha \mapsto \mathfrak{p}_\alpha$ and $\mathfrak{p} \mapsto \alpha_\mathfrak{p}$ are mutually inverse maps between X_F and Y_F.

Let $a \in \alpha_{\mathfrak{p}_\alpha}$, $a \neq 0$. Since

$$\begin{aligned} a \in \alpha_{\mathfrak{p}_\alpha} \cap \dot{F} &\Leftrightarrow \langle a \rangle \equiv 1 (\mathrm{mod}\ \mathfrak{p}_\alpha) \\ &\Leftrightarrow \langle a \rangle - 1 \in \ker(\mathrm{sgn}_\alpha) \\ &\Leftrightarrow \mathrm{sgn}_\alpha(\langle a \rangle - 1) = 0 \\ &\Leftrightarrow \mathrm{sgn}_\alpha(\langle a \rangle) = 1 \\ &\Leftrightarrow a \in \alpha, \end{aligned}$$

we have $\alpha_{\mathfrak{p}_\alpha} = \alpha$.

Now, we want to show that $\mathfrak{p}_{\alpha_\mathfrak{p}} = \mathfrak{p}$. For this, observe that if $a \in \dot{F}$, then $\langle a \rangle^2 = 1 \in W(F)$, and this implies that $\langle a \rangle \equiv \pm 1 (\mathrm{mod}\ \mathfrak{p})$. Now, let $\varphi = \langle a_1, ..., a_n \rangle \in \mathfrak{p}$. Then $\varphi \equiv 0 (\mathrm{mod}\ \mathfrak{p})$ implies $\langle a_1 \rangle + ... + \langle a_n \rangle \equiv 0 (\mathrm{mod}\ \mathfrak{p})$. Since $\langle a_i \rangle \equiv \pm 1 (\mathrm{mod}\ \mathfrak{p})$ and $\mathrm{char}(p) = 0$, we get $n = 2k$ and we can suppose without loss of generality that $\langle a_i \rangle \equiv 1 (\mathrm{mod}\ \mathfrak{p})$ for $i = 1, ..., k$ and $\langle a_i \rangle \equiv -1 (\mathrm{mod}\ \mathfrak{p})$ for $i = k+1, ..., n$. Hence, $\mathrm{sgn}_{\alpha_\mathfrak{p}}(\varphi) = 0$, and $\varphi \in \mathfrak{p}_{\alpha_\mathfrak{p}}$. Conversely, if $\varphi = \langle a_1, ..., a_n \rangle \in \ker(\mathrm{sgn}_{\varphi_\mathfrak{p}})$, we have $\mathrm{sgn}_{\varphi_\mathfrak{p}}\langle a_1 \rangle + ... + \mathrm{sgn}_{\varphi_\mathfrak{p}}\langle a_n \rangle = 0$, and again, we get $n = 2k$ and we can suppose without loss of generality that $\mathrm{sgn}_{\varphi_\mathfrak{p}}\langle a_i \rangle = 1$ if $i = 1, ..., k$ and $\mathrm{sgn}_{\varphi_\mathfrak{p}}\langle a_i \rangle = -1$ if $i = k+1, ..., n$. From this, we obtain $\langle a_1 \rangle + ... + \langle a_n \rangle \equiv 0 (\mathrm{mod}\ \mathfrak{p})$ and hence $\varphi \in \mathfrak{p}$. □

From this partial result, we get the full classification of prime ideals in $W(F)$:

Theorem 1.7.2 (Harrison)**.** *Spec$(W(F))$ consists of three types of prime ideals:*

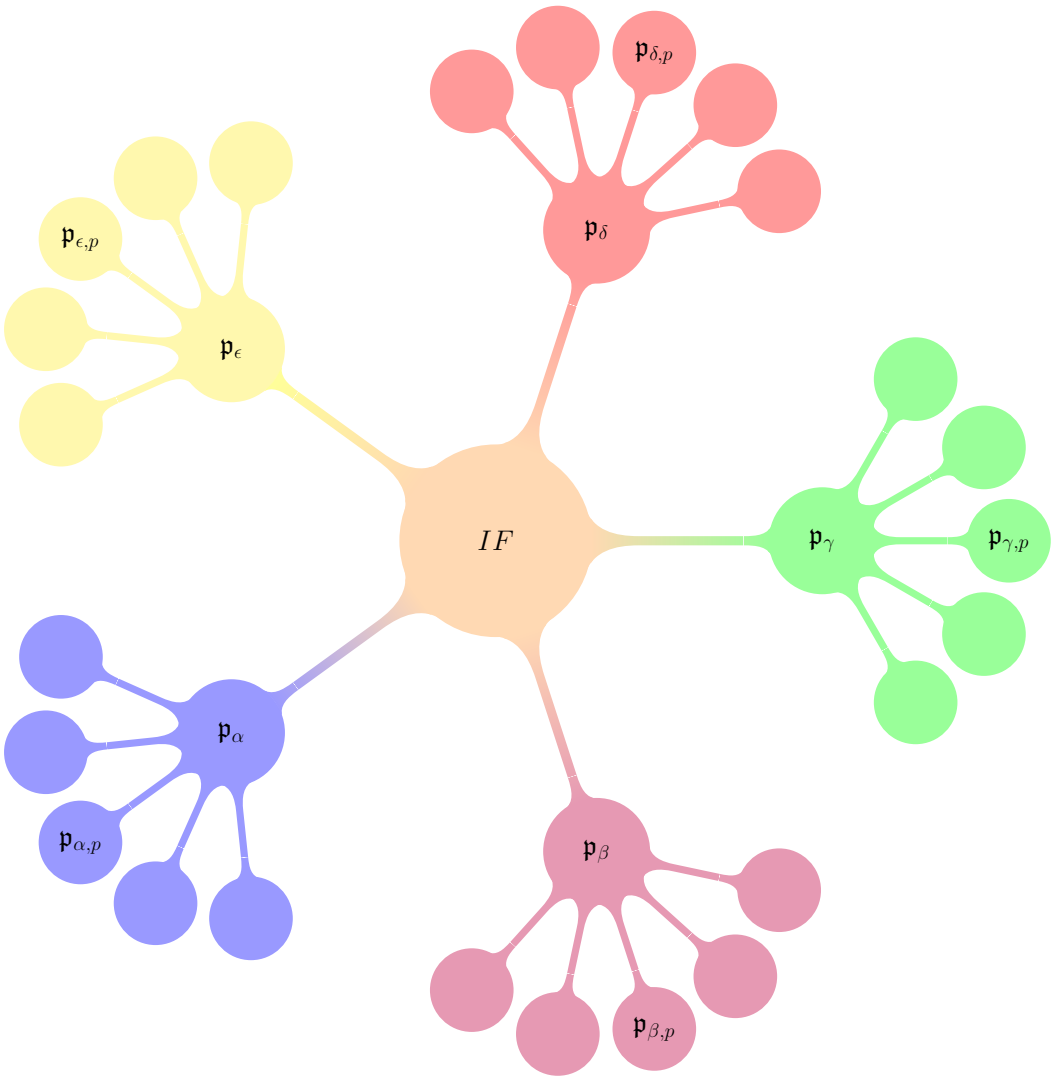
I - $\mathfrak{p}_\alpha$, $\alpha \in X_F$. *These are all prime ideals of characteristic* 0.

II - $\mathfrak{p}_{\alpha,p}$, $\alpha \in X_F$. *These are prime ideals of characteristic $p \neq 2$.*

III - $IF = \mathfrak{p}_{\alpha,2}$, $\alpha \in X_F$. *This is the unique prime ideal of characteristic* 2.

Proof. It only remains to analyze the prime ideals of odd prime characteristic p. Let $\mathfrak{p} \subseteq W(F)$ be such a prime ideal. Then the construction in 1.4 produces an ordering $\alpha = \alpha_{\mathfrak{p}}$. Consider $\varphi = \langle a_1, ..., a_n \rangle$ such that $\text{sgn}_\alpha(\varphi) = 0$. We already argue that $n = 2k$ and $\text{sgn}_{\varphi_{\mathfrak{p}}}\langle a_i \rangle = 1$ if $i = 1, ..., k$ and $\text{sgn}_{\varphi_{\mathfrak{p}}}\langle a_i \rangle = -1$ if $i = k+1, ..., n$. From this, we conclude that $\varphi \equiv 0 (\text{ mod } \mathfrak{p})$ and $\mathfrak{p}_\alpha \subseteq \mathfrak{p}$. Since $\mathfrak{p}_{\alpha,p}$ is the unique prime ideal of characteristic p that contains $\mathfrak{p}_\alpha$ ($\mathbb{Z}/p\mathbb{Z}$ is rigid), we conclude that $\mathfrak{p} = \mathfrak{p}_\alpha$. This completes the classification of prime ideals. □

Now, we have a picture to ilustrate the prime spectrum of $W(F)$:



The corollary below (especially its last statement) shows that the Harrison topology is indeed the most reasonable topology to be put on the space X_F.

Corollary 1.7.3. *Max$(W(F))$ (the maximal ideal spectrum of $W(F)$) consists of the height one primes $\mathfrak{p}_{\alpha,p}$. On the other hand, MinSpec$(W(F))$ (the minimal prime spectrum) is just the space Y_F in 1.7.1 consisting of the $\mathfrak{p}_\alpha$'s. The one-one correspondence in 1.7.1 is a homeomorphism between X_F (with the Harrison topology) and MinSpec$(W(F))$ (with the induced Zarisk topology).*

Proof. Only the last statement needs a verification. Using the notation in 1.3, consider a subbasic

open set in MinSpec($W(F)$), which has the form

$$\begin{aligned} D(q) \cap \text{MinSpec}(W(F)) &= \{\mathfrak{p}_\alpha : q \notin \mathfrak{p}_\alpha\} \\ &= \{\mathfrak{p}_\alpha : \text{sgn}_\alpha(q) \neq 0\}, \end{aligned}$$

where $q \in W(F)$. Under the one-one correspondence in 1.7.1, this corresponds to the following subset in X_F:

$$\{\alpha \in X_F : \text{sgn}_\alpha(q) \neq 0\},$$

which is open in X_F, since $\alpha \mapsto \text{sgn}_\alpha(q)$ is a continuous mapping from X_F to $\mathbb{Z}$. Conversely, specializing the above information to the form $q = \langle 1, a\rangle$ where $a \in \dot{F}$, we have

$$\{\alpha \in X_F : \text{sgn}_\alpha\langle 1, a\rangle \neq 0\} = \{\alpha \in X_F : a >_\alpha 0\},$$

which is the Harrison subbasic set $H(a) \subseteq X_F$. Therefore, under the one-one correspondence in 1.7.1, $H(a) \subseteq X_F$ also corresponds to a subbasic open set in MinSpec($W(F)$). This shows that the one-one correspondence in question is a homeomorphism. □

Corollary 1.7.4. *The Witt ring $W(F)$ has Krull dimension one if F is formally real, and Krull dimension zero if F is nonreal.*

Proof. This follows direclty from the enumeration of prime ideals in $W(F)$ 1.7.2. □

Another direct consequence of 1.7.2 follows below:

Corollary 1.7.5. *The following three statements are equivalent:*

i - F is nonreal;

ii - $W(F)$ has a unique prime ideal (which must be IF);

iii - $W(F)$ is a local ring (which maximal ideal IF).

1.8 Applications to the Structure of $W(F)$

We are in good position to make a more precise study of the Witt ring. In this section, we use the results of the three previous sections to determine the following objects which are of interest for the structure of the Witt Rings:

i - nil($W(F)$): this is the nilradical, consisting of all nilpotent elements in $W((F))$. By commutative ring theory, we know that nil($W(F)$) is the intersection of all prime ideals in $W(F)$.

ii - rad($W(F)$): this is the Jacobson radical of $W(F)$, i.e, the intersection of all maximal ideals of $W(F)$.

iii - zd($W(F)$): the set of zero-divisors in $W(F)$ (including 0).

iv - Id($W(F)$): the set of idempotents in $W(F)$.

v - $U(W(F))$: the multiplicative group of units in $W(F)$.

We begin with nil($W(F)$) and rad($W(F)$):

Theorem 1.8.1.

i - If F is nonreal, then nil$(W(F))$ = rad$(W(F)) = IF$.

ii - If F is formally real, then nil$(W(F))$ = rad$(W(F)) = W_t(F)$.

Proof. (i) is direct consequence of theorem 1.7.5. For (ii), note that, for any ordering α on F, the intersection $\bigcap \mathfrak{p}_{\alpha,p}$ (p ranging over all primes $\neq 0$) is just $\mathfrak{p}_\alpha$). Thus

$$\text{rad}(W(F)) = \bigcap_{\alpha,p} \mathfrak{p}_{\alpha,p} = \bigcap_{\alpha} \mathfrak{p}_\alpha. \tag{1.6}$$

This is just the intersection of all the prime ideals in $W(F)$. Consequently, $\text{rad}(W(F)) = \text{nil}(W(F))$. Further, 1.6 says that $\text{rad}(W(F))$ is the intersection of the kernels of $W(F) \to W(F_\alpha)$, where F_α ranges over all the real-closures of F. By Pfister's Local-Global Principle 1.5.1, we conclude that $\text{rad}(W(F)) = W_t(F)$. □

Next, we try to determine the set of zero-divisors $\text{zd}(W(F))$. We need the following general observation about $\text{zd}(R)$ for any commutative ring R.

Lemma 1.8.2. *If R is a comutative ring, zd(R) is the union of a certain set of prime ideals in R.*

Proof. It is suffices to show that any 0-divisor z is contained in a prime ideal $\mathfrak{p} \subseteq \text{zd}(R)$. Let S be the multiplicative set of all non 0-divisor ($S = R \setminus \text{zd}(R)$). By Zorn's Lemma, there exist an ideal $\mathfrak{p}$ maximal with respect to the properties $\mathfrak{p} \cap S = \emptyset$ and $z \in \mathfrak{p}$. We finish by showing that $\mathfrak{p}$ is prime. Indeed, suppose $xy \in \mathfrak{p}$ with $x, y \notin \mathfrak{p}$. By the maximality property of $\mathfrak{p}$, there exist $s, s' \in S$ such that $s \in \mathfrak{p} + xR$ and $s' \in \mathfrak{p} + yR$. Multiplying these equations, we get $ss' \in \mathfrak{p} \cap S$, which contradicts the choice of $\mathfrak{p}$. □

Theorem 1.8.3.

i - If F is nonreal, zd$(W(F)) = IF$.

ii - If F is formally real but not pythagorean, then also zd$(W(F)) = IF$.

iii - If F is formally real and pythagorean, then zd$(W(F))$ is the union of the minimal prime ideals $\mathfrak{p}_\alpha$, $\alpha \in X_F$.

Proof.

i - In this case, by corollary 1.7.5 $IF = \text{nil}(W(F))$ and $W(F) \setminus IF = U(W(F))$. Hence $\text{zd}(W(F)) = IF$.

ii - Suppose F is formally real but not pythagorean. Then there exists $0 \neq q \in W_t(F)$ (because if $W_t(F) = \{0\}$, we have for any $c = a^2 + b^2 \neq 0$ an isometry $\langle 1, 1\rangle \cong \langle c, c\rangle$, which implies that $\langle c\rangle = \langle 1\rangle \in W(F)$, so $c \in F^2$, i.e, F is formally real and pythagorean). Since the additive order of q is a power of 2 (i.e, q is 2-primary torsion), we see that $2 \in \text{zd}(W(F))$. Now, IF is the unique prime ideal of characteristic 2, so lemma 1.8.2 implies that $IF \subseteq \text{zd}(W(F))$. On the other hand, any prime ideal of the form $p_{\alpha,p}$ ($\alpha \in X_F$, $p \neq 2$) cannot be contained in $\text{zd}(W(F))$, since $p \cdot 1 \in p_{\alpha,p}$ is not a 0-divisor. The remaining primes p_α are already contained in $IF \subseteq \text{zd}(W(F))$. Thus lemma 1.8.2 yields $IF = \text{zd}(W(F))$.

iii - In this case, $W(F)$ is torsion free. For this, suppose that $q = \langle a_1, ..., a_n\rangle \in W(F)$ is an anisotropic form. Note that $r \cdot q$ is also anisotropic for any natural number r. Indeed, if $r \cdot q$ vanishes on a vector $(e_{11}, ..., e_{1r}, ..., e_{n1}, ..., e_{nr})$, i.e,

$$a_1 e_{11}^2 + ... + a_1 e_{1r}^2 + ... + a_n e_{n1}^2 + ... + a_n e_{nr}^2 = 0,$$

we can write $e_{i1}^2 + ... + e_{ir}^2 = e_i^2$ for suitable $e_i \in F$ (remember that F is pythagorean!) to get

$$a_1 e_1^2 + ... + a_n e_n^2 = 0.$$

This implies that $e_i = 0$ for all i, and there fore $e_{ij} = 0$ for all i, j (by formal reality). This implies, in particular, that $W(F)$ is torsion free.

Made this digression, if F is formally real and pythagorean, the prime ideals $\mathfrak{p}_{\alpha,p}$ ($\alpha \in X_F$, p any prime) cannot be contained in $\mathrm{zd}(W(F))$, since $W(F)$ is torsionfree. Therefore lemma 1.8.2 implies that $\mathrm{zd}(W(F)) \subseteq \bigcup \mathfrak{p}_\alpha$ (α ranging over X_F). We finish by proving that, for each $\alpha \in X_F$, $\mathfrak{p}_\alpha$ consists entirely of zero-divisors. If a form $q \in \mathfrak{p}_\alpha$, then

$$q = \langle a_1, ..., a_m, -b_1, ..., b_m \rangle$$

with all a_i, b_j positive at α. Letting q' be the product of the binary forms $\langle a_i, b_i \rangle$ ($1 \leq i \leq m$), we have $q' \neq 0$ in $W(F)$ (since $\mathrm{sgn}_\alpha(q') = 2^m\langle 1 \rangle \in W(F_\alpha)$), and $q \cdot q' = 0 \in W(F)$. Therefore, $q \in \mathrm{zd}(W(F))$, as desired.

□

It is perhaps a little surprising that, in the formally real case, the determination of $\mathrm{zd}(W(F))$ depends on wheter or not F is pythagorean. But, as we saw from the proof above, this distinction of cases is necessary since we need to know wheter or not 2 is a 0-divisor. There is, however, a nice piece of information that is common to all three cases in 1.8.3; we record this below.

Corollary 1.8.4. *For any field F, $q \in zd(W(F))$ only if $\dim q$ is even. In other words, odd-dimensional forms cannot be 0-divisors in $W(F)$.*

Proof. In the first two cases in theorem 1.8.3, we know that even the "if and only if" statement holds. But, in the formally real case, each prime ideal p_α ($\alpha \in X_F$) lies in IF, so even in case iii in theorem 1.8.3, we have

$$\mathrm{zd}(W(F)) \subseteq \bigcup_{\alpha \in X_F} p_\alpha \subseteq IF.$$

□

We come now to the determination of the idempotents in $W(F)$. It turns out, however, that there are no interesting ones!

Theorem 1.8.5. *The only idempotents in $W(F)$ are 0 and 1 (i.e, $W(F)$ is a "connected" ring).*

Proof. Suppose we have an equation $1 = e_1 + e_2 \in W(F)$, where e_1, e_2 are mutually orthogonal idempotents, other than $0, 1$. Then, $e_1, e_2 \in \mathrm{zd}(W(F)) \subseteq IF$ by corollary 1.8.4, and $1 = e_1 + e_2 \in IF$ gives the desired contradiction. □

Our final task is that of describing $U(W(F))$, the group of units of the Witt ring $W(F)$. A preliminar result is the following:

Theorem 1.8.6.

i - If F is nonreal, $U(W(F))$ consists of all odd-dimensional forms.

ii - If F is formally real, a form q lies in $U(W(F))$ iff $sgn_\alpha(q) = \pm 1$ for every $\alpha \in X_F$.

Proof.

i - Follows by theorem 1.7.5(iii), i.e, by the fact that if F is nonreal then $W(F)$ is a local ring with unique maximal ideal IF.

ii - $\Rightarrow$ follow by the fact that $U(\mathbb{Z}) = \{1, -1\}$. For $\Leftarrow$, consider any form q with the given signature property. Then $\mathrm{sgn}_\alpha(q^2) = 1$ for every $\alpha \in X_F$, and hence by Pfister's Local-Global principle

$$q^2 - 1 \in W_t(F) = \mathrm{nil}(W(F)).$$

We then have $q^2 \in 1 + \mathrm{nil}(W(F)) \subseteq U(F)$, so certainly $q \in U(W(F))$.

□

A more sofisticate computation is:

Theorem 1.8.7. *Let $I_t^2(F) = I^2F \cap W_t(F)$. Then $1 + I_t^2F$ is a multiplicative group, and*

$$U(W(F)) \cong (\dot{F}/\dot{F}^2) \times (1 + I_t^2F).$$

Here $\dot{F}/\dot{F}^2$ is identified with the subgroup of $W(F)$ consisting of the unary forms. In particular, I^2F is torsionfree iff $U(W(F)) \cong \dot{F}/\dot{F}^2$.

Proof. First, note that, by 1.8.1 $I_t^2(F)$ is a nil ideal. Thus, $1 + I_t^2F$ is a subgroup of $U(W(F))$. This subgroup has trivial intersection with $\dot{F}/\dot{F}^2$, since if $\langle a\rangle \in 1 + I_t^2F$, then $1 - \langle a\rangle \in I^2F$ implies that $\langle a\rangle = 1 \in W(F)$. It only remains to check that $\dot{F}/\dot{F}^2$ and $1 + I_t^2F$ generate $U(W(F))$. If $q \in U(W(F))$, then $\dim(q)$ must be odd, and we'll have $q_0 := q \perp \langle -a\rangle \in I^2F$ for some $a \in \dot{F}$. This gives $a \cdot q = 1 + q_1$, where $q_1 = a \cdot q_0 \in I^2F$. We are done if we can show that $q_1 \in W_t(F)$. We may assume that F is formally real (for otherwise $W(F) = W_t(F)$). Taking signatures with respect to any $\alpha \in X_F$, we have

$$\mathrm{sgn}_\alpha(a \cdot q) = 1 + \mathrm{sgn}_\alpha(q_1) \equiv 1 \,(\mathrm{mod}\ 4).$$

By theorem 1.8.6(ii), the left side of this equation can only be ± 1, so it must be 1, which implies that $\mathrm{sgn}_\alpha(q_1) = 0$. Now, Pfister's Local-Global principle implies that $q_1 \in W_t(F)$, as desired. □

Our more refinated result in calculation of $U(W(F))$ is

Theorem 1.8.8. *$U(W(F))$ is a 2-primary torsion group.*

In the following, we shall try to give an elementary proof for this result using solely the fact that $W_t(F)$ is a 2-primary torsion group. This will be done with the help of the following ring-theoretic lemma:

Lemma 1.8.9. *Let x be an element in any ring (with 1) such that $mx = 0 = x^{2^r}$, where $m > 1$ and $r \geq 0$ are given integers. Then $(1 + x)^{m^r} = 1$.*

Proof. The proof is by induction on r. The case $r = 0$ being clear, we assume $r > 0$. Since $mx = 0$, the binomial theorem gives $(1+x)^m = 1+x^2y$, where y is a polinomial in x with integer coefficients. Since $m(x^2y) = 0$ and $(x^2y)^{2r-1} = x^{2r}y^{2r-1} = 0$, the inductive hypothesis applied to the element x^2y implies that

$$1 = (1 + x^2y)^{m^r-1} = [(1 + x)^m]^{m^r-1} = (1 + x)^{m^r}.$$

□

We now return to

Proof of theorem 1.8.8. Let $q \in I_t^2 F$. Since $W_t(F)$ is 2-primary torsion, we have $mq = 0$ for some $m = 2^k$. By 1.8.1, q is also nilpotent, so $q^{2r} = 0$ for some r. Applying lemma 1.8.9, we see that $(1+q)^{2kr} = 1$. Thus the results follow by 1.8.7. □

We can obtain the following refinement of 1.8.8 in a special case:

Corollary 1.8.10. *If F is a field such that I^3F is torsionfree, then $U(W(F))$ is a group of exponent ≤ 2.*

Proof. In view of theorem 1.8.7, it suffices to show that $(1+q)^2 = 1$ for every $q \in I_t^2 F$. Now $2q \in 2 \cdot I_t^2 F \subseteq I^3F \cap W_t(F) = 0$ and $q^2 \in q \cdot I_t^2 F \subseteq I^3F \cap W_t(F) = 0$, so indeed $(1+q)^2 = 1+2q+q^2 = 1$, as desired. □

1.9 Pfister forms and chain P-equivalence

The so called Pfister forms provides an entire revolution in the study of quadratic forms. We reproduce some pieces of this work, with the climax in Hauptsatz, proved two sections later. We begin by formally defining Pfister forms:

Definition 1.9.1. *For an n-tuple of elements $a_1, ..., a_n \in \dot{F}$, we write $\langle\langle a_1, ..., a_n\rangle\rangle$ to denote the 2^n-dimensional form $\otimes_{i=1}^n \langle 1, a_i\rangle$ and will refer to this as an n-fold Pfister form (over F).*

A 0-fold Pfister form is, by convention, taken to be the form $\langle 1\rangle$.

In working with Pfister forms, it is useful to note that, if some $a_i = -1$, then $\langle\langle a_1, ..., a_n\rangle\rangle$ becomes hyperbolic. On the other hand, we have

$$\langle\langle 1, a_2, ..., a_n\rangle\rangle \cong 2\langle\langle a_2, ..., a_n\rangle\rangle$$

where $2q$ means $q \perp q$. In particular, $\langle\langle 1, ..., 1\rangle\rangle \cong 2^n\langle 1\rangle$. Another important motivation for studying Pfister forms is, of course, the following:

Proposition 1.9.2. *Let IF denote (as usual) the ideal of all even-dimensional forms in $W(F)$. Then I^nF is generated as an abelian group by all the n-fold Pfister forms over F.*

Proof. We have shown in 1.3.3 that IF is additively generated by $\langle 1, a\rangle = \langle\langle a\rangle\rangle$, $a \in \dot{F}$. Thus, I^nF is additively generated by the n-fold product

$$\langle\langle a_1\rangle\rangle ... \langle\langle a_n\rangle\rangle = \langle\langle a_1, ..., a_n\rangle\rangle, a_i \in \dot{F}.$$

□

We'll begin our study by assembling some basic formulas for 2-fold Pfister forms. Recall that $D(q) = D_F(q)$ denotes the set of values in $\dot{F}$ represented by q.

Proposition 1.9.3.

i - For any $x \in D\langle\langle a\rangle\rangle$, $\langle\langle a, b\rangle\rangle \cong \langle\langle a, bx\rangle\rangle$.

ii - For any $y \in D\langle a, b\rangle$, $\langle\langle a, b\rangle\rangle \cong \langle\langle a, by\rangle\rangle$.

Proof. These follow from the following isometries:

$$\langle\langle a, b\rangle\rangle \cong \langle 1, a\rangle \perp \langle b\rangle\langle x, xa\rangle \cong \langle\langle a, bx\rangle\rangle;$$
$$\langle\langle a, b\rangle\rangle \cong \langle 1, ab, a, b\rangle \cong \langle 1, ab, y, aby\rangle \cong \langle\langle y, ab\rangle\rangle.$$

□

The goal of this section is to build up the properties of n-fold Pfister forms from those of 1-fold and 2-fold Pfister forms. To this end, we proceed in analogy with Witt's notion of chain equivalence 1.2.4

Definition 1.9.4. *Let $\langle\langle a_1, ..., a_n\rangle\rangle$ and $\langle\langle b_1, ..., b_n\rangle\rangle$ be two n-fold Pfister forms. We say that they are simply P-equivalent if there exist two indices i and j, $1 \leq i, j \leq n$ such that*

i - $\langle\langle a_i, a_j\rangle\rangle \cong \langle\langle b_i, b_j\rangle\rangle$, *and*

ii - $a_k = b_k$ *for any* $k \neq i, j$.

In condition (i) above, if i is equal to j, the expression $\langle\langle a_i, a_j\rangle\rangle$ is understood to be just $\langle\langle a_i\rangle\rangle$. More generally, we say that two n-fold Pfister forms φ, γ are chain P-equivalent if there exists a sequence of n-fold Pfister forms $\varphi = \varphi_0, \varphi_1, ..., \varphi_n = \gamma$, and that each φ_i is simply P-equivalent to φ_{i+1} $(0 \leq i \leq m-1)$.

Chain P-equivalence is an equivalence relation on all n-fold Pfister forms; it will be denoted by the symbol $\approx$. Of course, $\varphi \approx \gamma$ implies that $\varphi \equiv \gamma$. It is by no means obvious, at this point, that the converse also holds. Nevertheless, this turns out to be the case, and will be one of the theorems we prove in this section. To this end, let us first observe that, if π is any permutation of $\{1, ..., n\}$, then

$$\langle\langle a_1, ..., a_n\rangle\rangle \approx \langle\langle a_{\pi(1)}, ..., a_{\pi(n)}\rangle\rangle.$$

This follows immediately from the fact that, for $n \geq 2$, the symmetric group on n letters is generated by the transpositions.

Since any n-fold Pfister form φ represents 1, we may write $\varphi \cong \langle 1\rangle \perp \varphi'$. We shall call φ' the *pure subform* of φ (in analogy with the "pure quaternions"). This terminology is justified, since the isometry type of φ' is uniquely determined by that φ, according to Witt's Cancellation Theorem. From here, we shall write φ' for the pure subform of a Pfister form φ.

Theorem 1.9.5 (Pure subform)**.** *Let $\varphi = \langle\langle a_1, ..., a_n\rangle\rangle$ be an n-fold Pfister form ($n \geq 1$), and let $b \in D_F(\varphi')$. Then there exist $b_2, ..., b_n \in \dot{F}$ such that $\varphi \approx \langle\langle b, b_2, ..., b_n\rangle\rangle$.*

Proof. We induct on n. If $n = 1$, then $\varphi = \langle 1, a_1\rangle$. Since $b \in D_F(\varphi') = D_F(a_1)$, we have $\langle b\rangle \cong \langle a_1\rangle$, and the result follows. Now assume the result for $(n-1)$-fold Pfister forms. Let

$$\tau = \langle\langle a_1, ..., a_{n-1}\rangle\rangle \cong \langle 1\rangle \perp \tau'.$$

Then $\varphi \cong \tau\langle 1, a_n\rangle \cong \tau \perp \langle a_n\rangle\tau$, so $\varphi' \cong \tau' \perp \langle a_n\rangle\tau$. Since by hypothesis $b \in D_F(\varphi')$, there exist

$$x \in D_F(\tau') \cup \{0\} \text{ and } y \in D_F(\tau) \cup \{0\}$$

such that $b = x + a_n y$. We may further write $y = t^2 + y_0$, where $y_0 \in D_F(\tau') \cup \{0\}$. Then, we have two cases:

Case 1 - If $y = 0$, then $0 \neq b = x \in D_F(\tau')$. By induction hypothesis, there exist $d_2, ..., d_{n-1} \in \dot{F}$ such that $\tau \approx \langle\langle x, d_2, ..., d_{n-1}\rangle\rangle$. Thus

$$\varphi \approx \langle\langle x, d_2, ..., d_{n-1}, a_n\rangle\rangle = \langle\langle b, d_2, ..., d_{n-1}, a_n\rangle\rangle$$

and we are done.

Case 2 - Suppose $y \neq 0$. We claim that

$$\varphi \approx \langle\langle a_1, a_2, ..., a_{n-1}, a_n y\rangle\rangle.$$

There is nothing to prove if $y_0 = 0$, for then $y = t^2$. So we may assume $y_0 \in D_F(\tau')$. By the inductive hypothesis again, $\tau \approx \langle\langle y_0, c_2, ..., c_{n-1}\rangle\rangle$ for some $c_i \in \dot{F}$. Thus,

$$\begin{aligned}\varphi &\approx \langle\langle y_0, c_2, ..., c_{n-1}, a_n\rangle\rangle \\ &\approx \langle\langle y_0, c_2, ..., c_{n-1}, a_n(t^2 + y_0)\rangle\rangle \text{ (by 1.9.3(i))} \\ &\approx \langle\langle a_1, ..., a_{n-1}, a_n y\rangle\rangle,\end{aligned}$$

proving our claim. If $x = 0$, then the last entry $a_n y$ above is just b, and we are done. So we may assume that $x \in D_F(\tau')$. Again, our inductive hypothesis implies that $\tau \approx \langle\langle x, d_2, ..., d_{n-1}\rangle\rangle$ for some $d_i \in \dot{F}$, and so

$$\begin{aligned}\varphi &\approx \langle\langle x, d_2, ..., d_{n-1}, a_n y\rangle\rangle \\ &\approx \langle\langle x + a_n y, d_2, ..., d_{n-1}, a_n xy\rangle\rangle \text{ (by 1.9.3(ii))} \\ &\approx \langle\langle b, d_2, ..., d_{n-1}, a_n xy\rangle\rangle.\end{aligned}$$

□

For the later reference, we record here one of the key steps used in the proof of 1.9.5:

Proposition 1.9.6. *Let $\tau = \langle\langle a_1, ..., a_{n-1}\rangle\rangle$ and $y \in D_F(\tau)$. Then for any $a_n \in \dot{F}$:*

$$\langle\langle a_1, ..., a_{n-1}, a_n\rangle\rangle \approx \langle\langle a_1, ..., a_n y\rangle\rangle.$$

In particular, $\langle\langle a_1, ..., a_{n-1}, y\rangle\rangle$ is isometric to 2τ, and $\langle\langle a_1, ..., a_{n-1}, -y\rangle\rangle$ is hyperbolic.

Proof. This is just the "Claim" in case 2 in the proof of 1.9.5. Since 1.9.5 is now fully proved, this "Claim" is valid for all n. The last statement of the proposition follows immediately from this, by setting $a_n = \pm 1$. □

Using the Pure subform theorem 1.9.5, we shall now derive two of the principal properties of Pfister forms. The first one is

Theorem 1.9.7. *If a Pfister form φ is isotropic, then it is hyperbolic.*

Proof. Since φ contains a hyperbolic plane, we have $-1 \in D_F(\varphi')$ by Witt's cancellation. By 1.9.5 $\varphi \approx \langle\langle -1, ..., \rangle\rangle$, which is hyperbolic. □

The next property has to do with the similarity factors of a Pfister form. For any quadratic form q over F, $G_q(F) = G_F(q) = \{c \in \dot{F} : \langle c\rangle q \cong q\}$ denotes the *group of similarity factors of q*.

Theorem 1.9.8. *For any Pfister form φ over F, $D_F(\varphi) = G_F(\varphi)$. In particular, φ is a group form over F.*

Proof. Since φ represents 1, we have that $G_F(\varphi) \subseteq D_F(\varphi)$. To prove that $c \in D_F(\varphi) \Rightarrow \langle c\rangle\varphi \cong \varphi$, we appeal to some argument on the Witt ring. The Pfister form $\varphi\langle\langle -c\rangle\rangle \cong \varphi \perp \langle -c\rangle\varphi$ (of one higher fold) contains a subform $\langle c, -c\rangle \cong \mathbb{H}$, so by proposition 1.9.6 $\varphi\langle\langle -c\rangle\rangle$ is hyperbolic. Hence $\varphi\langle\langle -c\rangle\rangle = 0 \in W(F)$ and since $\dim(\langle c\rangle\varphi) = \dim(\varphi)$, it follows that $\langle c\rangle\varphi = \varphi \in W(F)$, then $\langle c\rangle\varphi \cong \varphi$. □

The special case of theorem 1.9.8 for the Pfister form $\langle\langle 1, ..., 1\rangle\rangle$ is already worthy of some celebration:

Corollary 1.9.9. *For any $n \geq 0$, the nonzero sums of 2^n squares in F form a subgroup of $\dot{F}$.*

Next, we shall further generalize the Pure Subform Theorem 1.9.5. This generalization will be the key step in our subsequent proof of the theorem that isometry of Pfister forms implies their chain P-equivalence.

Theorem 1.9.10. *If $\tau = \langle\langle b_1, ..., b_r\rangle\rangle$ $(r \geq 0)$, $\gamma = \langle\langle d_1, ..., d_s\rangle\rangle$ $(s \geq 1)$, and $e_1 \in D_F(\tau\gamma')$, then there exist $e_2, ..., e_s \in \dot{F}$ such that*

$$\langle\langle b_1, ..., b_r, d_1, ..., d_s\rangle\rangle \approx \langle\langle b_1, ..., b_r, e_1, ..., e_s\rangle\rangle.$$

Proof. We prove by induction on s. If $s = 1$, then $e_1 \in D_F(\langle d_1\rangle\tau)$, so $e_1 = d_1x$, where $x \in D_F(\tau)$. Proposition 1.9.6 implies that

$$\langle\langle b_1, ..., b_r, d_1\rangle\rangle \cong \langle\langle b_1, ..., b_r, d_1x\rangle\rangle \cong \langle\langle b_1, ..., b_r, e_1\rangle\rangle.$$

By induction, we may assume the result for $\langle\langle b_1, ..., b_r, d_1, ..., d_{s-1}\rangle\rangle$. Let $\sigma = \langle\langle d_1, ..., d_{s-1}\rangle\rangle$, so

$$\gamma = \sigma\langle d_s, 1\rangle \cong \langle d_s\rangle\sigma \perp \sigma \text{ and } \gamma' \cong \langle d_s\rangle\sigma \perp \sigma'.$$

Therefore, $\tau\gamma' \cong \langle d_s\rangle\tau\sigma \perp \tau\sigma'$. Since $e_1 \in D_F(\tau\gamma')$, there exist $x \in D_F(\tau\sigma) \cup \{0\}$ and $y \in D_F(\tau\sigma') \cup \{0\}$ such that $e_1 = d_sx + y$. If $x \neq 0$ and $y \neq 0$ we get the desired in the following two steps:

Step 1 - $\langle\langle b_1, ..., b_r, d_1, ..., d_s\rangle\rangle \approx \langle\langle b_1, ..., b_r, d_1, ..., d_sx\rangle\rangle$ by 1.9.9.

Step 2 - By induction, there exist $e_2, ..., e_{s-1} \in \dot{F}$ such that

$$\langle\langle b_1, ..., b_r, d_1, ..., d_{s-1}\rangle\rangle \approx \langle\langle b_1, ..., b_r, y, e_2, ..., e_{s-1}\rangle\rangle. \qquad (*)$$

Therefore, by Step 1,

$$\begin{aligned}\langle\langle b_1, ..., b_r, d_1, ..., d_{s-1}, d_s\rangle\rangle &\approx \langle\langle b_1, ..., b_r, d_1, ..., d_{s-1}, d_sx\rangle\rangle \\ &\approx \langle\langle b_1, ..., b_r, y, e_2, ..., e_{s-1}, d_sx\rangle\rangle \\ &\approx \langle\langle b_1, ..., b_r, e_1, e_2, ..., e_{s-1}, d_sxy\rangle\rangle,\end{aligned}$$

where the last "$\approx$" follows from 1.9.3(ii).

We are now left with the case where one of x, y is zero. If $y = 0$, then $0 \neq e_1 = d_sx$, and Step 1 provides the needed proof. If $x = 0$, then $e_1 = y$, and from (*), we get

$$\langle\langle b_1, ..., b_r, d_1, ..., d_s\rangle\rangle \approx \langle\langle b_1, ..., b_r, e_1, ..., e_{s-1}d_s\rangle\rangle,$$

which completes the proof. □

The following special case of 1.9.10 (with $r = 1$) is already noteworthy.

Corollary 1.9.11. *Let q be a Pfister form. If $q \cong \langle 1, b, e, ...\rangle$ with $b, e \in \dot{F}$, then*

$$q \cong \langle\langle b, e, e_2, ..., e_s\rangle\rangle$$

for suitable $e_i \in \dot{F}$.

Proof. By the Pure Subform Theorem, $q \cong \langle\langle b\rangle\rangle\gamma$ for a suitable Pfister form $\gamma = \langle\langle b_2, ..., b_{s+1}\rangle\rangle$. Comparing $\langle\langle b\rangle\rangle\gamma \cong \langle\langle b\rangle\rangle \perp \langle\langle b\rangle\rangle\gamma'$ with $q \cong \langle\langle b\rangle\rangle \perp \langle e, ...\rangle$, we see that $e \in \langle\langle b\rangle\rangle\gamma'$. We are now done by applying 1.9.10 with $\tau = \langle\langle b\rangle\rangle$. □

We are now in position to prove the following main result on chain P-equivalence:

Theorem 1.9.12 (Chain P-equivalence)**.** *Let φ, ψ be n-fold Pfister forms. Then $\varphi \cong \psi$ iff $\varphi \approx \psi$.*

Proof. It suffices to prove the $\Rightarrow$ part. Write $\varphi = \langle\langle a_1, ..., a_n\rangle\rangle$ and $\psi = \langle\langle b_1, ..., b_n\rangle\rangle$. Assuming that $\varphi \cong \psi$, we claim that, for any integer r such that $0 \leq r \leq n$ holds:

$$\varphi \approx \langle\langle b_1, ..., b_r, c_{r+1}, ..., c_n\rangle\rangle \text{ for some } c_{r+1}, ..., c_n \in \dot{F}. \qquad (A_r)$$

If this is estabilished, then for $r = n$, the statement (A_n) implies the desired conclusion that $\varphi \approx \psi$. Now we prove (A_r) by induction on r. There is nothing to prove in case $r = 0$. Assume inductively, that (A_r) is true, where $r < n$. We must proceed to prove (A_{r+1}). Set $\tau = \langle\langle b_1, ..., b_r\rangle\rangle$, $\beta = \langle\langle b_{r+1}, ..., b_n\rangle\rangle$ and $\gamma = \langle\langle c_{r+1}, ..., c_n\rangle\rangle$. Then γ is an s-fold Pfister form, where $s = n - r$. We have, from the various hypothesis, $\tau \cdot \beta = \psi \cong \varphi \cong \tau\gamma$; that is, $\tau \perp \tau\beta' \cong \tau \perp \tau\gamma'$. By cancellation theorem, it follows that $\tau\beta \cong \tau\gamma'$. But then

$$b_{r+1} \in D_F(\beta') \subseteq D_F(\tau\beta') = D_F(\tau\gamma').$$

By 1.9.10, we get

$$\langle\langle b_1, ..., b_r, c_{r+1}, ..., c_n\rangle\rangle \approx \langle\langle b_1, ..., b_r, b_{r+1}, c'_{r+2}, ..., c'_n\rangle\rangle$$

for suitable $c'_i \in \dot{F}$. From this and the inductive hypothesis (A_r), we deduce

$$\varphi \approx \langle\langle b_1, ..., b_r, b_{r+1}, c'_{r+2}, ..., c'_n\rangle\rangle,$$

which estabilishes the truth of (A_{r+1}). □

1.10 Function Fields

In view of Hauptsatz proof, we must present a brief introduction to function fields. The main idea is that in algebraic geometry, a function field is associated with every irreducible algebraic variety. In the case of an irreducible quadratic form φ, we have therefore a function field associated with the quadratic hypersurface defined by the quadratic equation $\varphi = 0$. Not surprisingly, the study of such function fields holds the key to many basic issues in the algebraic theory of quadratic forms over fields.

In this section, we give a introduction to the idea of the function field of a quadratic form as soon as some basic results derived from this. A preamble for the construction of such a function field is the following.

Lemma 1.10.1. *Let $\varphi(x_0, ..., x_n)$ be a regular $(n+1)$-dimensional quadratic form over F, where $n \geq 1$. Then φ is reducible as a polynomial in $F[x_0, ..., x_n]$ iff $n = 1$ and $\varphi \cong \mathbb{H}$.*

Proof. If $\varphi(x_0, ...x_n)$ factors nontrivially, it must factor into a product of two linear forms. Since φ is regular and $n \geq 1$, this happens iff φ is isometric to the quadratic form x_0x_1, that is, iff $\varphi \cong \mathbb{H}$. □

Definition 1.10.2. *The ("big") function field of φ, if φ is irreducible in $(n+1)$-variables, is defined to be the quotient field of the integral domain $F[X]/(q(X))$. This is a field of transcendence degree n over F; we shall denote it by $F[\varphi]$.*

As we mentioned at the beggining of this section, $F[\varphi]$ is the usual function field, in the sense of algebraic geometry, of the affine quadric hypersurface $\varphi(X) = 0$ in F^{n+1}. Besides this, we have that $F[\varphi]$ depends (up to an F-isomorphism) only on the isometry class of φ.

A computation shows that $F[\varphi]$ can be expressed as a quadratic extension of a *rational* function field in n variables over F. Indeed, if we write $F[\varphi]$ as $F(x_0, ..., x_n)$ (where the x_i's should have been written as $\overline{x}_i$'s), the relation $a_0x_0^2 + ... + a_nx_n^2 = 0$ shows that

$$F[\varphi] = F(x_1, ..., x_n)\left(\sqrt{-(a_1x_1^2 + ... + a_nx_n^2)/a_0}\right) \tag{1.7}$$

as claimed.

The reason we called $F[\varphi]$ the "big" function field is that we could have formed a smaller one, defined by

$$F(\varphi) := F(x_1/x_0, x_2/x_0, ..., x_n/x_0) \subseteq F[\varphi]. \tag{1.8}$$

Note that this subfield of $F[\varphi]$ is uniquely determined, i.e, it does not depend on the choice of x_0 as the denominators in 1.8. Indeed, since

$$\frac{x_i}{x_j} = \left(\frac{x_i}{x_0}\right) / \left(\frac{x_j}{x_0}\right) \in F[\varphi],$$

$F(\varphi)$ could have been expressed as $F(\{x_i/x_j\}) \subseteq F[\varphi]$, which exhibts no dependence on any particular subscript. The field $F(\varphi)$ may be called the *homogeneous function field* of φ, since, in algebraic geometry, it is just the function field of the *projective variety* defined by the homogeneous equation $\varphi(X) = 0$ in $\mathbb{P}^n(F)$.

The two function field $F[\varphi]$ and $F(\varphi)$ are related by the relation

$$F[\varphi] = F(\varphi)(x_0),$$

and they have pretty much the same behavior. In practice, it is sufficient to work with just one of them.

Note that $F(\varphi)$ is also a quadratic extension of a rational function field (this time in $n-1$ variables). Indeed, if we write $t_i = x_i/x_0$ $(1 \leq i \leq n)$, the equation

$$a_0 + a_1t_1^2 + ... + a_nt_n^2 = 0$$

show that

$$F(\varphi) = F(t_1, ..., t_{n-1})\left(\sqrt{-(a_0 + a_1t_1^2 + ... + a_{n-1}t_{n-1}^2)/a_0}\right),$$

which is to be compared with 1.7.

Now, we shall develop the main properties of function fields of quadratic forms. The main focus will be on the nature of the quadratic forms that become isotropic or hyperbolic over these function fields. From here, it will be more convenient to work with the "big" function fields $F[\varphi]$, although we could have equally well used the small function fields $F(\varphi)$. We remind the reader again that, whenever the notation $F[\varphi]$ is used, it will be assumed that $\dim(\varphi) \geq 2$ and $\varphi \neq \mathbb{H}$, for otherwise $F[\varphi]$ is undefined.

Theorem 1.10.3. *A function field $F[\varphi]$ is purely transcendental[7] iff the form φ is isotropic over F.*

[7] A field extension $K|F$ is purely transcedental if there is a subset S of K that is algebraically independent over

In particular, any two isotropic quadratic forms of the same dimension have isomorphic function fields.

To prove this theorem, we will need the following lemma:

Lemma 1.10.4. *Let γ be a quadratic form over a field F. If γ is anisotropic over F, then γ remains anisotropic over the rational function field $F(x)$. In particular, the Witt kernel $W(F(x)/F)$ is the zero ideal in $W(F)$.*

Proof. Let $\gamma = \langle a_1, ..., a_n \rangle$, $a_i \in \dot{F}$. Assume that γ is isotropic over $F(x)$. After clearing denominators, we obtain an equation $\sum a_i f_i(x)^2 = 0$, where $f_i(x) \in F[x]$ are not all zero. Changing the f_i's if necessary, we may further assume that x does not divide all of the polynomials $f_i(x)$. Setting $x = 0$, we get $\sum a_i f_i(0)^2 = 0$, where the $f_i(0) \in F$ are not all zero. This says that γ is isotropic over F. The last part of the theorem now follows immediately. □

Proof of Theorem 1.10.3. First assume $F[\varphi]$ is purely transcendental. Since φ becomes isotropic over $F[\varphi]$, lemma 1.10.4 implies that φ must already be isotropic over F. Conversely, assume that φ is isotropic over F. After changing variables, we may express φ in the form $x_0x_1 + \psi(x_2, ..., x_n)$, where ψ is a regular quadratic form in $x_2, ..., x_n$. Using the expression of ψ to calculate $F[\varphi]$, we see that $F[\varphi]$ is isomorphic to the rational function field $F(x_1, ..., x_n)$. □

Since φ always becomes isotropic over $F[\varphi]$, it is of interest to ask what other forms over F might also become isotropic, or even hyperbolic, over $F[\varphi]$. Although various results have been obtained on this direction, a full answer to the above question has remained unknown up to this date.

Now, we introduce some notation to facilitate our discussions:

Definition 1.10.5. *For any quadratic form q, we write $q > \varphi$ (resp. $q \gg \varphi$)[8] to express the fact that q becomes isotropic (resp. hyperbolic) over the function field $F[\varphi]$ of the quadratic form φ.*

Definition 1.10.6. *Let φ and γ be forms. If φ is isometric to a subform of the form γ we will write $\varphi \subseteq \gamma$.*

For any field extension $K|F$, we have introduced earlier the Witt kernel notation $W(K|F)$ for the kernel of the functorial map $W(F) \to W(K)$. This ideal of $W(F)$ is called the *Witt kernel* of the extension $K|F$. In terms of this Witt kernel notation, the relation $q \gg \varphi$ in 1.10.5 simply amounts to $q \in W(F[\varphi]/F)$.

Example 1.10.7.

a - Of course, $\varphi > \varphi$.

b - Suppose $q_1 = q_2 + q_3 \in W(F)$. If $q_i \gg \varphi$ holds for two values of i, then it holds for all three.

c - If $\dim(q) > 0$, then $q \gg \varphi \Rightarrow q > \varphi$. The converse fails in general, but does hold when q is a Pfister form (by 1.9.7).

We will end this section with the following theorem, that gives a significant necessary conditions on the forms $q \gg \varphi$ (for a given φ).

K (i.e, the elements of S do not satisfy any non-trivial polynomial equation with coefficients in K) and such that $L = K(S)$.

[8] It will be convenient sometimes to write also $q < \varphi$ instead of $q > \varphi$ and $\varphi \ll q$ instead of $q \gg \varphi$.

Theorem 1.10.8. *Suppose $q \gg \varphi$ where q, φ are quadratic forms over F, with $1 \in D_F(\varphi)$. Then $\varphi(X) \in G_{F(X)}(q)$, where $X = (x_0, ..., x_n)$, and $\dim(\varphi) = n+1$ (in other words, we have $\varphi(X) \cdot q \cong q$ over the rational function field $F(X)$). If q is anisotropic, then $a \cdot \varphi \subseteq q$ (over F) for any $a \in D_F(q)$; in particular, we must have $\dim(q) \geq \dim(\varphi)$ (if $\dim(q) \neq 0$).*

Unfortunately, the proof of theorem 1.10.8 involve some techniques of quadratic forms under transcendental extensions that escape from the scope of this dissertation. However, the reader can found the proof in theorem 4.5 on chapter 10 of [Lam05], and read about this methods on chapter 9 of the same book.

1.11 Hauptsatz and Forms in I^nF

This section offers the begginings of an in-depth study of the quadratic forms in I^nF, the n-power of the fundamental ideal IF. The first word in the section title above refers to the following beautiful result of Arason and Pfister proved in 1971 in their joint paper:

Theorem 1.11.1 (Hauptsatz)**.** *Let q be a positive-dimensional anisotropic form over F. If $q \in I^nF$, then $\dim q \geq 2^n$.*

An equivalent way to state this result is the following: if a form q belongs to $I^n(F)$ and $\dim(q) < 2^n$, then q must be a hyperbolic form.

The significance of the Hauptsatz lies in the fact that it offers an important dimension-theoretic sufficient condition for a form to belong to I^nF. This Hauptsatz may be regarded as the first step towards finding a set of necessary and sufficient conditions for the quadratic forms in I^nF (for given n).

Before we proof 1.11.1, we will estabilish the power of the Hauptsatz given a few immediate consequences. The first one is the "Krull Intersection Property" in part (i) below.

Corollary 1.11.2.

i - In the Witt ring $W(F)$, $\cap_{j=0}^{\infty} I^jF = 0$.

ii - More generally, if $K|F$ is any field extension, and J is the kernel of the functorial map $r^* : W(F) \to W(K)$, then $\cap_{j=0}^{\infty}(J + I^jF) = J$.

Proof.

a - Let q be a form belonging to $\cap_{j=0}^{\infty} I^jF$. Pick a large integer n such that $\dim(q) < 2^n$. Since $q \in I^nF$, the Hauptsatz implies that $q = 0 \in W(F)$.

b - This is a self-strenghthening of item (a). If $q \in \cap_{j=0}^{\infty}(J + I^jF)$, then $r^*(q) = q_K \in I^iK$ for all i (since $r^*(I^iF) \subseteq I^iK$). By item (a), we have $r^*(q) = 0 \in W(K)$, so $q \in J$.

□

Corollary 1.11.3. *Let φ, γ be a pair of 2^n-dimensional forms which represent a common value $a \in \dot{F}$. Then*

$$\varphi \equiv \gamma \, (mod \; I^{n+1}F) \Rightarrow \varphi \cong \gamma.$$

Proof. Since $a \in D_F(\varphi) \cap D_F(\gamma)$, there exist forms φ_0 and γ_0 such that $\varphi \cong \langle a \rangle \perp \varphi_0$ and $\gamma \cong \langle a \rangle \perp \gamma_0$. Consider $\sigma := \varphi_0 \perp \langle -1 \rangle \gamma_0$. Since

$$\varphi \perp \langle -1 \rangle \gamma \cong \langle a, -a \rangle \perp \varphi_0 \perp \langle -1 \rangle \gamma_0 \cong \mathbb{H} \perp \sigma,$$

the hypothesis $\varphi \equiv \gamma \,(\mathrm{mod}\ I^{n+1}F)$ leads to $\sigma \in I^{n+1}F$. Since $\dim(\sigma) < 2^n + 2^n = 2^{n+1}$, the Hauptsatz implies that σ is hyperbolic, and hence $\varphi \cong \gamma$. □

Corollary 1.11.4. *Let $r, s \in \dot{F}$, and let φ, γ be n-fold Pfister forms over F. Then*

$$\varphi \cong \gamma \Leftrightarrow \langle r\rangle\varphi \equiv \langle s\rangle\gamma (mod\ I^{n+1}F).$$

Proof. We have that $\varphi \equiv \langle r\rangle\varphi$ and $\psi \equiv \langle s\rangle\psi$ modulo $I^{n+1}F$. This proves $\Rightarrow$ and reduces $\Leftarrow$ to the case $r = s = 1$. This case follows from 1.11.3 since φ and ψ represents 1. □

Although we can prove 1.11.1 and 1.11.2 in several special cases, the methods used for this proves do not generalize to the case for arbitrary n and arbitrary fields F. In order to prove 1.11.1 in general, we'll need the method of function fields. As it turns out, with the function field results in the last section at our disposal, the proof of 1.11.1 boils down to a simple induction, as follows.

Proof of theorem 1.11.1. Let $q \in I^nF$ be as in 1.11.1. Since the n-fold Pfister forms additively generate I^nF, there exists an expression

$$q = \varepsilon_1\varphi_1 + ... + \varepsilon_r\varphi_r \in I^nF,$$

where $\varepsilon_i = \pm 1$ and φ_i are anisotropic n-fold Pfister forms. To show that $\dim(q) \geq 2^n$, we induct on r. If $r = 1$, we have $q \cong \langle\pm 1\rangle\varphi_1$, so $\dim(q) = 2^n$. For the general case, we go up to the function field $L = F[\varphi_1]$. Over this field, we have a shorter expression

$$q_L = \varepsilon_2(\varphi_2)_L + ... + \varepsilon_r(\varphi_r)_L \in I^nL.$$

If q_L is hyperbolic, 1.10.8 yields direclty $\dim(q) \geq \dim(\varphi_1) = 2^n$. Thus we may assume that $(q_L)_{an}$ (the anisotropic part of q_L) is a positive-dimensional form in I^nL. Thus, the inductive hypothesis (invoked over the field L) implies that $\dim_L(q_L)_{an} \geq 2^n$. But then,

$$\dim_F(q) = \dim_L(q_L) \geq \dim_L(q_L)_{an} \geq 2^n.$$

□

The very short proof of the Hauptsatz above perhaps belies its true depth. Of course, this proof made crucial use of 1.10.8, which is a centerpiece in the function field theory of quadratic forms.

1.12 How quadratic forms are useful to mathematicians?

As promised, we cover in this chapter all the concepts that will be taken as primitive in the chapters 3-6. However, you probably thought:

Why all this matters? Where are the connections with maistream mathematics?

This is a central question and we are not in position to give a full answer. But the work seems to be incomplete if we do not include some substantial application of algebraic theory of quadratic forms. So in this section, we give a few comments about Milnor's algebraic K-theory (as developed in [Mil70]), that in our point of view, are a beatiful way to illustrate the applications of the theory of algebraic quadratic forms.

So, let us start. To any field F we associate a graded ring

$$K_*F = (K_0F, K_1F, K_2F, ...)$$

as follows. By definition, $K_0 \cong \mathbb{Z}$ and K_1F is the multiplicative group $\dot{F}$ written additively. To keep notation straight, we introduce the canonical isomorphism

$$l : \dot{F} \to K_1F,$$

where $l(ab) = l(a) + l(b)$ (the "logarithm"). Then K_*F is defined to be the quotient of the tensor algebra

$$(\mathbb{Z}, K_1F, K_1F \otimes K_1F, K_1F \otimes K_1F \otimes K_1F, ...)$$

by the ideal generated by all $l(a) \otimes l(-a)$, with $a \neq 0, 1$. In other words each K_nF, $n \geq 2$, is the quotient of the n-fold tensor product $K_1F \otimes K_1F \otimes ... \otimes K_1F$ by the subgroup generated by all $l(a_1) \otimes ... \otimes l(a_n)$ such that $a_i + a_{i+1} = 1$ for some i. If mentally we relate $l(a)$ with the Pfister form $\langle 1, -a \rangle$, this relation is just saying that "an n-fold hyperbolic Pfister form is zero in I^n/I^{n+1}."

In terms of generators and relations, K_*F can be described as the associative ring with unit which is generated by the symbols $l(a)$, $a \in \dot{F}$, subject only to the defining relations $l(ab) = l(a) + l(b)$ and $l(a)l(-a) = 0$.

Think in K_nF in terms of relations between Pfister forms is not worthless: setting $k_nF = K_nF/2K_nF$, we have the following:

Theorem 1.12.1 ([Mil70] Theorem 4.1)**.** *There is one and only one homomorphism*

$$s_n : k_nF \to I^nF/I^{n+1}F$$

which carries each product $l(a_1)...l(a_n)$ in k_nF to $\langle\langle a_1, ..., a_n \rangle\rangle$ modulo $I^{n+1}F$. The homomorphisms s_0, s_1 and s_2 are bijective and every s_n is surjective.

Theorem 1.12.1 surprisingly (or not) is saying that k_*F works almost like the graded Witt ring

$$W_*(F) = (W(F)/IF, IF/I^2F, ..., I^nF/I^{n+1}F, ...).$$

But we have even more interesting connections: to any field F, let F_s be a separable closure and $G = G_F = \mathrm{Gal}_F(F_s)$ be the Galois group of F_s over F. Then the exact sequence

$$1 \to \{\pm 1\} \to \dot{F}_S \xrightarrow{2} \dot{F}_S \to 1$$

upon which G operates, leads to an exact sequence

$$H^0(G, \dot{F}_s) \xrightarrow{2} H^0(G, \dot{F}_s) \to H^1(G, \{\pm 1\}) \to H^1(G, \dot{F}_s)$$

of cohomology groups, where the right hand group is zero. Idenfying the first two groups with $\dot{F}$, and substituing $\mathbb{Z}/2\mathbb{Z}$ for $\{\pm 1\}$, this yields

$$\dot{F} \xrightarrow{2} \dot{F} \xrightarrow{\delta} H^1(G, \mathbb{Z}/2\mathbb{Z}) \to 0.$$

The quotient $\dot{F}/\dot{F}^2$ can of course be identified with $H^1(G, \mathbb{Z}/2\mathbb{Z})$.

Theorem 1.12.2 ([Mil70] Lemma 6.1)**.** *The isomorphism $l(a) \mapsto \delta(a)$ from k_1F to $H^1(G, \mathbb{Z}/2\mathbb{Z})$*

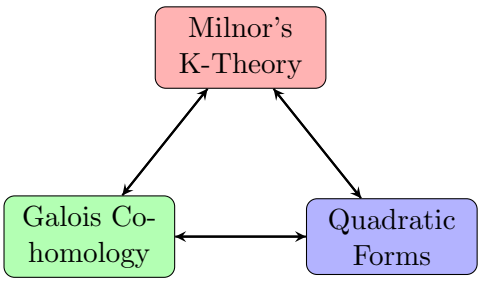
extends uniquely to a graded ring homomorphism

$$h_* : k_F \to H^*(G, \mathbb{Z}/2\mathbb{Z}).$$

With these two results, a natural question is:

Are s_* and h_* isomorphisms?

This question is known as "Milnor's Conjecture". A positive answer is given by V. Voevodsky and colaborators late 1990's, given to us a "triangle"

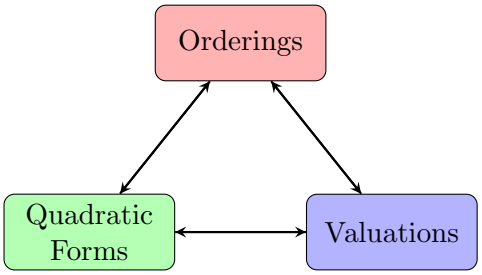


These relations are being object of research even today.

Chapter 2

The Reduced Theory of Quadratic Forms

Even though the reduced theory is not yet an "abstract theory", it is an immediate generalization of the concepts in chapter 1. In this chapter, we work in "Lam's triangle" of reduced theory of quadratic forms:



In our context, chapter 1 is the "Heart" and this chapter is the "Blood" of the generalizations in the next chapters. Here, we follow chapters 1-7 of Lam's book [Lam83] and for valuations, we follow chapter 4 of [End72]. Some examples of valuations are extracted from [Efr06].

2.1 Preorderings and Orderings

Firstly, we need to develop more the theory of orderings on a field[1].

Definition 2.1.1. *A preordering on a field F is a proper subset $T \subseteq F$ such that $F^2 \subseteq T$, $T+T \subseteq T$ and $T \cdot T \subseteq T$.*

Note that, in view of the last three properties of a preordering, the requirement that $T \neq F$ may be stregthened into $-1 \notin T$. For, if $-1 \in T$, then for any $x \in F$, we can write $x = y^2 - z^2$, where $y = (1+x)/2$ and $z = (1-x)/2$, and so we would have $x \in F^2 + T \cdot F^2 \subseteq T + T \cdot T \subseteq T$.

For any preordering $T \subseteq F$, the set $\dot{T} = T \setminus \{0\}$ is a subgroup of the multiplicative group $\dot{F}$ (because $1 \in \dot{F}^2 \subseteq \dot{T}$ and if $x \in \dot{T}$, then $x^{-1} = (x^{-1})^2 \cdot x \in \dot{T}$).

Let $T \subseteq F$ be a preordering, and $\{a_i : i \in I\}$ be a set of elements in F. We shall let $T[a_i : i \in I]$ denote the *subsemiring of F generated by T and $\{a_i : i \in I\}$*. This consists of all "polynomial expressions" in $\{a_i : i \in I\}$ with elements of T as "coefficients". This will be a preordering in F iff it does not contain -1. In the special case when I is a singleton set, note that $T[a] = T + aT$.

[1] Of course, all fields of this chapter are considered with characteristic different of 2.

Lemma 2.1.2. *Let $T \subseteq F$ be a preordering and $a \in \dot{F}$. Then $T[a]$ is a preordering iff $a \notin -T$.*

Proof. If $a \notin -T$, we claim that $-1 \notin T[a]$. In fact, if we could write $-1 = t_1 + t_2 a$ for some $t_1, t_2 \in T$, then $-t_2 a = 1 + t_1 \in \dot{T}$, and so $a \in -\dot{T}$, a contradiction. Then $T[a]$ is a preordering.

If $a \in -T$, then $T[a]$ contains $(-a) \cdot a$ and hence -1, so $T[a]$ is not a preordering. □

Corollary 2.1.3. *A preordering $T \subseteq F$ is maximal (with respect to set-theoretic inclusion) iff T is and ordering.*

Proof. ($\Rightarrow$) If T is a maximal preordering, then for any $a \notin T$, the above lemma implies $a \in -T$. This means that $F = T \cup (-T)$, so T is an ordering in F.

($\Leftarrow$) Suppose that there exist another proper preordering T', $T \supsetneq T'$ and an element $x \in T' \cap (-T)$, $x \neq 0$. Then $-1 = (x^{-1})^2 \cdot x \cdot x^{-1} \in T'$, contradiction. □

Corollary 2.1.4. *Any preordering $T \subseteq F$ is contained in at least one ordering of F.*

Proof. Applying the Zorn's lemma to the family $\mathcal{F}$ of all preorderings containing T. Pick any member $P \in \mathcal{F}$ which is maximal with respect to inclusion. By corollary 2.1.3, P is an ordering of F containing T. □

Theorem 2.1.5 (Artin-Schreier)**.** *A field is formally real iff it has an ordering.*

Proof. We already know that a field F is formally real iff F has a preordering. Then, applying the above corollary we have the desired result. □

For any preordering $T \subseteq F$, we shall write X_T for the (nonempty) subset of X_F consisting of all orderings $P \supseteq T$. We claim that X_T is a closed set of X_F, so X_T will also be a Boolean space with induced topology. To prove our claim, let $P \in X_F \setminus X_T$, and fix an element $a \in T \setminus P$. Then $-a \in P$ and $H(-a)$ is a neighborhood of P disjoint from X_T. This shows that $X_F \setminus X_T$ is open, so X_T is closed. Note that a subbasis for the topology of X_T is given by the relative Harrison sets $H_T(a) := H(a) \cap X_T = \{P \in X_T : a \in P\}$.

Theorem 2.1.6. *For any preordering $T \subseteq F$, we have $T = \bigcap_{P \in X_T} P$.*

Proof. It is suffices to show that $\bigcap_{P \in X_T} P \subseteq T$. Let $a \notin T$. Then by lemma 2.1.2, $T[-a]$ is a preordering and by corollary 2.1.4, there exists an ordering $P_0 \supseteq T[-a]$. Since $-a \in \dot{P}_0$, we have $a \notin P_0$, so $a \notin \bigcap_{P \in X_T} P$. □

In the special case when $T = \sum F^2$, the theorem above was first proved by Artin. In this case, the theorem states that, in a formally real field F, an element $a \in F$ is a sum of squares in F iff it is nonnegative in every ordering of F (this statement is, of course, also correct for nonreal fields F, since, in that case, $\sum F^2 = F$ and X_F is empty). We shall refer to theorem 2.1.6 as Artin's Theorem.

Note that the intersection of any nonempty family of preorderings is always a preordering. conversely, Artin's Theorem tels us that any preordering $T \subseteq F$ arises in this way.

For the later reference, we record the following consequence of 2.1.6:

Corollary 2.1.7. *Let $T \subsetneq T'$ be two preorderings in F. Then:*

i - There exists a preordering T'' such that $T \subseteq T'' \subseteq T'$ and $[\dot{T}' : \dot{T}''] = 2$.

ii - T' is minimal (as a preordering) over T iff $[\dot{T}' : \dot{T}] = 2$

Proof.

i - By 2.1.6, we have $X'_T \subsetneq X_T$. Pick any ordering $P \in X_T \setminus X'_T$ and let $T'' : P \cap T'$. We have $T \subseteq T'' \subseteq T'$, and $[\dot{T}' : \dot{T}''] = [\dot{F} : \dot{P}] = 2$.

ii - Follow by item (i).

□

Suppose $T \subsetneq T'$ and T' is minimal over T. Then, for any $a \in T'$, the following equation holds:

$$T[a] = T + T \cdot a = T \cup T \cdot a.$$

In fact, if $a \in T$, both sides are equal to T, while, if $a \in T' \setminus T$, both sides are equal to T' (in view of 2.1.7).This leads to a useful definition:

Definition 2.1.8. *For a given preordering T, an element $a \in F$ is said to be T-rigid if $T + T \cdot a = T \cup T \cdot a$, i.e, if $[T(a) : \dot{T}] \leq 2$.*

Elements of T are always T-rigid. For some preorderings T, it may happens that T is already the set of all T-rigid elements. This is the case, for instance, if T is the weak preordering $\sum F^2$ in the field $F = \mathbb{Q}(x)$. Note that if T is a preordering such that all T-rigid elements are already in T, then no preordering $T' \supsetneq T$ can be minimal over T, and so the set of preorderings properly containing T will not satisfy the descending chain condition.

The notion of T-rigid elements will emerge again to play a central role when we study the class of preorderings called "fans".

2.2 The Reduced Theory

The main goal of this section is to set up a theory of quadratic forms "relative to" a preordering T (or "reduced" modulo T). This theory will lead to a relative Witt ring, denoted by $W_T F$, which shares many of the formal properties of the ordinary Witt ring WF. Actually, $W_T F$ turns out to be isomorphic to a certain quotient ring of WF, namely

$$W_T F \cong WF / \sum_{t \in \dot{T}} WF \cdot \langle 1, -t \rangle.$$

Therefore, one could legitimately take this to be the definition of $W_T F$. Such a definition, however, would be awkward to work with and would obscure the fact that there is actually a reasonable quadratic form theory naturally associated with $W_T F$. For better motivation, one should therefore first develop the relevant "reduced" quadratic form theory relative to T, and then construct the Witt ring $W_T F$ from it.

In the following, let T be a fixed preordering in F. By a (diagonal) *T-form*, of dimension n, we shall mean a formal expression $\varphi = \langle a_1, ..., a_n \rangle_T$, where $a_1, ..., a_n \in \dot{F}$. If the preordering T is clear from the context, we shall often drop the subscript T and simply write $\varphi = \langle a_1, ..., a_n \rangle$. For such T-form φ, and any ordering $P \in X_T$, we define the *P-signature* of φ by

$$\operatorname{sgn}_P(\varphi) = \sum_{i=1}^{n} \operatorname{sgn}_P(a_i) \in \mathbb{Z},$$

where

$$\mathrm{sgn}_P(a) = \begin{cases} 1 \text{ if } a \in \dot{P}, \\ -1 \text{ if } a \notin \dot{P}. \end{cases}$$

Follow that $\mathrm{sgn}_P(\varphi) \cong \dim \varphi \,(\mathrm{mod}\ 2)$.

We can define the *orthogonal sum* and the *tensor product* of T-forms as we did for ordinary forms, namely:

$$\langle a_1, ..., a_n\rangle \perp \langle b_1, ..., b_m\rangle := \langle a_1, ..., a_n, b_1, ..., b_m\rangle,$$
$$\langle a_1, ..., a_n\rangle \otimes \langle b_1, ..., b_m\rangle := \langle a_1b_1, ..., a_ib_j, ..., a_nb_m\rangle.$$

A straightforward calculation shows that

$$\mathrm{sgn}_P(\varphi \perp \psi) = \mathrm{sgn}_P(\varphi) + \mathrm{sgn}_P(\psi)$$
$$\mathrm{sgn}_P(\varphi \otimes \psi) = \mathrm{sgn}_P(\varphi)\mathrm{sgn}_P(\psi)$$

for any T-forms φ, ψ and any ordering $P \in X_T$. To simplify the notation, we shall use the same conventions adopted in chapter 1: write $\varphi \cdot \psi$, or just $\varphi\psi$, for the tensor product $\varphi \otimes \psi$. For any natural number r, we write $r \cdot \varphi$ or just $r\varphi$ for the r-fold orthogonal sum $\varphi \perp ... \perp \varphi$.

Definition 2.2.1. *We say that two T-forms φ, ψ are T-**isometric** (in symbols, $\varphi \cong_T \psi$) if φ, ψ have the same dimension and the same signature with respect to any $P \in X/T$.*

From this definition, we can verify that following two types of T-isometries:

$$\langle a_1, ..., a_n\rangle_T \cong_T \langle a_1t_1, ..., a_nt_n\rangle_T \,(a_i \in \dot{F},\, t_1 \in \dot{T}), \tag{2.1}$$
$$\langle a, b\rangle_T \cong_T \langle a + b, ab(a + b)\rangle_T \,(a, b, a + b \in \dot{F}). \tag{2.2}$$

These two basics types of T-isometries are particularly important, because it will turn out later that they can be used to "account for" all T-isometries.

Another immediate consequence of 2.2.1 is the **Witt's Cancellation**:

$$\varphi \oplus \psi_1 \cong_T \varphi \oplus \psi_2 \Rightarrow \psi_1 \cong_T \psi_2.$$

A T-form φ is said to be T-*hyperbolic* (or *hyperbolic over* T) if $\mathrm{sgn}_P(\varphi) = 0$ for every $P \in X_T$. Such a form must have even dimension. If $\dim \varphi = 2n$, we have in fact $\varphi \cong_T \langle 1, -1\rangle_T$, i.e, up to T-isometry, there is only one hyperbolic T-form of dimension $2n$. The binary hyperbolic T-form $\langle 1, -1\rangle_T$ is called the T-*hyperbolic plane* and is denoted by $\mathbb{H}_T$.

Definition 2.2.2. *A T-form $\varphi = \langle a_1, ..., a_n\rangle_T$ is said to be T-**isotropic** (or isotropic over T) if there exist $t_1, ..., t_n \in T$, not all zero, such that $a_1t_1 + ... + a_nt_n = 0$. If such $t_i's$ does not exist, φ is said to be T-**anisotropic**.*

To illustrate this notion of T-isotropy, consider the case when T is the weak preordering $\sum F^2$ in a formally real field F. To say that φ above is $(\sum F^2)$-isotropic means that there exists an equation

$$\sum_{i=1}^{n} a_i(x_{i1}^2 + ... + x_{ir_i}^2) = 0,$$

where the x_{ij}'s are not all zero. This means, therefore, that, for some natural number r, $r \cdot \varphi$ is isotropic as an ordinary quadratic form. If this is the case, we shall say that the form φ is *weakly*

isotropic. If F happens to be a pythagorean field (i.e, $\sum F^2 = F^2$), this will, of course, imply that φ is isotropic. If F is not pythagorean, the implication may no longer be true: for $x_1^2 + x_2^2 \notin F^2$, the form $\varphi = \langle 1, -(x_1^2 + x_2^2)\rangle$ is weakly isotropic (with $2\varphi = 2\langle 1, -1\rangle$), but φ is anisotropic.

Returning to T-forms $\varphi = \langle a_1, ..., a_n\rangle_T$ over a general preordering T, we define $D_T(\varphi)$ to be the set

$$D_T(\varphi) = \left\{ \sum_{i=1}^{n} a_i t_i \neq 0 : t_1, ..., t_n \in T \right\} = \left(\sum T \cdot a_i \right) \setminus \{0\}.$$

This is called the *set of values* of the T-form φ; it is a union of $\dot{T}$-cosets in $\dot{F}$. If $b \in D_T(\varphi)$, we shall say that b is *T-represented by φ* (or represented by φ over T). It will turn out later that the set $D_T(\varphi)$ depends only on the T-isometry class of φ, but this is not at all clear from the definition above.

Proposition 2.2.3. *Let $\varphi = \langle a_1, ..., a_n\rangle_T$. Then:*

i - *For any $t_1, ..., t_r \in \dot{T}$,*
$$D_T(\langle t_1, ..., t_r\rangle\varphi) = D_T(\varphi) = D_T(r \cdot \varphi)$$

ii - *For any natural number r, φ is T-isotropic iff $r \cdot \varphi$ is T-isotropic.*

iii - *φ is T-isotropic iff, for suitable $t_1, ..., t_n \in \dot{T}$, $\langle t_1, ..., t_r\rangle\langle a_1, ..., a_n\rangle$ is isotropic as an ordinary quadratic form.*

Proof. All three conclusions follow from the axioms $T \cdot T \subseteq T$, $T + T \subseteq T$ for the preordering T and the definition of T-representation. □

Note that the conclusion (iii) above relates the notion of T-isotropy to the usual notion of isotropy for quadratic forms. The next result, which is considerably deeper, gives the analog of this for the notion of hyperbolicity.

Theorem 2.2.4. *For any T-form φ, the following statements are equivalent:*

i - *φ is hyperbolic over T.*

ii - *$\langle\langle t_1, ..., t_r\rangle\rangle\varphi = 0 \in WF$ for some $t_1, ..., t_n \in \dot{T}$.*

iii - *$\langle t_1, ..., t_r\rangle\varphi = 0 \in WF$ for some $t_1, ..., t_n \in \dot{T}$.*

Proof. (ii)⇒(iii) and (iii)⇒(i) are immediate. So we need only prove (i)⇒(ii). The proof will be based on the following "Witt Formula", which holds in the Witt ring WF for all $a_i \in \dot{F}$:

$$2^n\langle a_1, ..., a_n\rangle = \sum_{\varepsilon} \langle \varepsilon_1, ..., \varepsilon_n\rangle\langle\langle \varepsilon_1 a_1, ..., \varepsilon_n a_n\rangle\rangle \in WF. \tag{2.3}$$

Here ε ranges over all n-tuples $\langle \varepsilon_1, ..., \varepsilon_n\rangle$ with $\varepsilon_i \in \pm 1$. To prove 2.3, first note that $\varepsilon_i\langle\langle \varepsilon_i a_i\rangle\rangle \cong a_i\langle\langle \varepsilon_i a_i\rangle\rangle$, so

$$\langle \varepsilon_1, ..., \varepsilon_n\rangle\langle\langle \varepsilon_1 a_1, ..., \varepsilon_n a_n\rangle\rangle \cong \langle a_1, ..., a_n\rangle\langle\langle \varepsilon_1 a_1, ..., \varepsilon_n a_n\rangle\rangle.$$

Therefore, we are reduced to proving that

$$\sum_{\varepsilon} \langle\langle \varepsilon_1 a_1, ..., \varepsilon_n a_n\rangle\rangle = 2^n\langle 1\rangle \in WF,$$

for all $a_i \in \dot{F}$. This is checked by induction on n. For $n = 1$, the sum is $\langle\langle a_1\rangle\rangle + \langle\langle -a_1\rangle\rangle = 2\langle 1\rangle \in WF$. Inductively, if we let $\varepsilon' = \langle \varepsilon_1, ..., \varepsilon_{n-1}\rangle$, then the sum breaks up into

$$\begin{aligned}\sum_{\varepsilon'}\langle\langle \varepsilon_1 a_1, ..., \varepsilon_{n-1}a_{n-1}, a_n\rangle\rangle + \sum_{\varepsilon'}\langle\langle \varepsilon_1 a_1, ..., \varepsilon_{n-1}a_{n-1}, -a_n\rangle\rangle \\ = \sum_{\varepsilon'}\langle\langle \varepsilon_1 a_1, ..., \varepsilon_{n-1}a_{n-1}\rangle\rangle(\langle\langle a_n\rangle\rangle + \langle\langle -a_n\rangle\rangle) \\ = 2\sum_{\varepsilon'}\langle\langle \varepsilon_1 a_1, ..., \varepsilon_{n-1}a_{n-1}\rangle\rangle = 2^n\langle 1\rangle \in WF.\end{aligned}$$

Now, let $\varphi = \langle a_1, ..., a_n\rangle_T$ be T-hyperbolic. To get (ii), we shall try to apply 2.3. For a given n-tuple $\varepsilon = (\varepsilon_1, ..., \varepsilon_n)$ as above, we have the following two possible cases:

Case 1. $T[\varepsilon_1 a_1, ..., \varepsilon_n a_n] \neq F$. In this case, there exists an ordering $P \supseteq T[\varepsilon_1 a_1, ..., \varepsilon_n a_n]$. For this P, we have $\mathrm{sgn}_P(\varepsilon_i) = \mathrm{sgn}_P(a_i)$ for all i, so $\mathrm{sgn}_P(\langle \varepsilon_1, ..., \varepsilon_n\rangle) = \mathrm{sgn}_P(\varphi) = 0$. Thus, half of the ε_i's are 1's and the other half are -1's. This gives $\langle \varepsilon_1, ..., \varepsilon_n\rangle = 0 \in WF$, so we can drop the corresponding term on the right side of 2.3.

Case 2. $T[\varepsilon_1 a_1, ..., \varepsilon_n a_n] = F$. Note that $T[\varepsilon_1 a_1, ..., \varepsilon_n a_n] \setminus \{0\}$ is just $D_T(\varphi_\varepsilon)$ where $\varphi_\varepsilon := \langle \varepsilon_1 a_1, ..., \varepsilon_n a_n\rangle$; in particular $-1 \in D_T(\varphi_\varepsilon)$. This implies that $2\varphi_\varepsilon$ is T-isotropic, so by 2.2.3(ii) and (iii), there exist $t'_1, ..., t'_m \in \dot{T}$ such that $\langle t'_1, ..., t'_m\rangle\varphi_\varepsilon$ is isotropic as an ordinary quadratic form. Hence $\langle\langle t'_1, ..., t'_m, \varepsilon_1 a_1, ..., \varepsilon_n a_n\rangle\rangle$ is isotropic. Since this is a Pfister form, it must be hyperbolic. Therefore, multiplying the twos sides of 2.3 by a suitably chosen Pfister form $\langle\langle t_1, ..., t_r\rangle\rangle$ ($t_i \in \dot{T}$), we get $\langle\langle t_1, ..., t_r\rangle\rangle\varphi = 0 \in WF$.

□

Corollary 2.2.5. *If φ is T-hyperbolic, then φ is T-isotropic. The converse holds if φ is a Pfister form.*

Proof. For ordinary quadratic forms, we know that hyperbolicity does imply isotropy. Therefore, the first conclusion follows from 2.2.3(iii) and 2.2.4(iii). For the second conclusion, let $\varphi = \langle\langle b_1, ..., b_n\rangle\rangle$ be T-isotropic. By definition, there is an equation

$$t_0 + t_1 b_1 + ... + t_n b_n + t_{12} b_1 b_2 + ... = 0,$$

where $t_i, t_{ij}, ... \in T$ are not all zero. Consider any $P \in X_T$. The equation above implies that the b_i's cannot all be in P, say $b_1 \in -P$. Then

$$\mathrm{sgn}_P(\varphi) = \mathrm{sgn}_P\langle 1, b_1\rangle \mathrm{sgn}_P\langle\langle b_2, ..., b_n\rangle\rangle = 0,$$

so φ is T-hyperbolic. □

We can now prove the following powerful

Theorem 2.2.6 (Representation Criteria)**.** *Let $b_1 \in \dot{F}$ and $\varphi = \langle a_1, ..., a_n\rangle_T$. Then $b_1 \in D_T(\varphi)$ iff there exists $b_2, ..., b_n \in \dot{F}$ such that $\varphi \cong_T \langle b_1, b_2, ..., b_n\rangle_T$. In particular, $D_T(\varphi)$ depends only on the T-isometry class of φ.*

Proof. First assume $b_1 \in D_T(\varphi)$, say $b_1 = a_1 t_1 + ... + a_n t_n$, where $t_i \in T$. We may assume that $a_1 t_1 + ... + a_r t_r \neq 0$ for all r (for otherwise we can just work with $\langle a_{r+1}, ..., a_n\rangle$). Using repeatedly

the two basic types of T-isometries in 2.1 and 2.2 we obtain

$$\begin{aligned}\varphi &\cong_T \langle a_1t_1, ..., a_nt_n\rangle\\ &\cong_T \langle a_1t_1 + a_2t_2, a_1a_2t_1t_2(a_1t_1 + a_2t_2), a_3t_3, ..., a_nt_n\rangle\\ &\cong_T \langle a_1t_1 + a_2t_2, a_3t_3, a_1a_2t_1t_2(a_1t_1 + a_2t_2), a_4t_4, ..., a_nt_n\rangle\\ &\cong_T \langle a_1t_1 + a_2t_2 + a_3, a_3t_3(a_1t_1 + a_2t_2)(a_1t_1 + a_2t_2 + a_3t_3), a_1a_2t_1t_2(a_1t_1 + a_2t_2), a_4t_4, ..., a_nt_n\rangle\end{aligned}$$

and so on. Repeating this process, we get $\varphi \cong_T \langle b_1, b_2, ..., b_n\rangle_T$ for suitable $b_2, ..., b_n \in \dot{F}$.

Conversely, assume we have $\varphi \cong_T \langle b_1, b_2, ..., b_n\rangle_T$. Then

$$\langle a_1, ..., a_n, -b_1, ..., -b_n\rangle_T$$

is T-hyperbolic. By 2.2.4(iii), there exist $t_1, ..., t_r \in \dot{T}$ such that

$$\langle t_1, ..., t_r\rangle\langle a_1, ..., a_n\rangle = \langle t_1, ..., t_r\rangle\langle b_1, ..., b_n\rangle \in WF.$$

Since the left hand side and the right hand side above are forms of the same dimension, they must be isometric (as ordinary forms). In particular, $t_1b_1 \in D_T(\langle t_1, ..., t_r\rangle\varphi)$. In view of 2.2.3(i), this implies that $b_1 \in t_1^{-1}D_T(\varphi) = D_T(\varphi)$. □

Corollary 2.2.7. *For any T-form φ, the following statements are equivalent:*

i - φ is T-isotropic;

ii - $\varphi \cong_T \mathbb{H}_T \perp \psi$ for some T-form ψ;

iii - φ is T-universal;

iv - There exists an element $b \in \dot{F}$ such that both $\pm b \in D_T(\varphi)$.

Proof. (ii)⇒(iii)⇒(iv) is immediate.

(iv)⇒(i) From $b \in D_T(\varphi)$, by 2.2.6 we get $\varphi \cong_T \langle b, a_2, ..., a_n\rangle_T$ for suitable $a_2, ..., a_n \in \dot{F}$. Similarly, from $-b \in D_T(\varphi)$ we get $\varphi \cong_T \langle -b, c_2, ..., c_n\rangle_T$ for suitable $c_2, ..., c_n \in \dot{F}$. Then

$$2\varphi \cong \langle b, -b, a_2, ..., a_n, c_2, ..., c_n\rangle_T$$

that is T-isotropic. By 2.2.3(ii) we conclude that φ is itself T-isotropic.

(i)⇒(ii) If $\varphi = \langle a_1, ..., a_n\rangle_T$ is T-isotropic, write $a_1t_1 + ... + a_nt_n = 0$ where $t_i \in T$, and say $t_1 \neq 0$. Then

$$-1a_1t_1 = a_2t_2 + ... + a_nt_n \in D_T(a_2, ..., a_n),$$

so by 2.2.6, $\langle a_2, ..., a_n\rangle_T \cong_T \langle -a_1t_1\rangle_T \perp \psi$ for some T-form ψ. Therefore

$$\varphi \cong_T \langle a_1t_1, -a_1t_1\rangle_T \perp \psi \cong_T \langle 1, -1\rangle_T \perp \psi.$$

□

Note that the characterizations (iii),(iv) above for T-isotropy are special features in the "mod T" theory; they do not have analogues in the "absolute" theory of quadratic forms.

Corollary 2.2.8. *For any T-form φ, there exists a "Witt decomposition" $\varphi \cong_T \psi \perp r\mathbb{H}_T$, where $r \geq 0$ and ψ is T-anisotropic. Here, r is uniquely determined by φ, and so is the T-isometry class of ψ. We call r the **Witt index** of φ (over T), and call ψ the T-anisotropic part of φ.*

Proof. This proof follows the same sketch of proof of theorem 1.2.3.

For existence part, if φ is anisotropic, take $\psi = \varphi$ and $r = 0$. Let φ is isotropic, say $\varphi \cong \langle 1, -1\rangle_T \perp \psi_1$. Observe that $\dim \psi_1 < \dim \varphi$. Then we repeat this analysis for ψ_1: if ψ_1 is anisotropic, take $\psi = \psi_1$ and $r = 1$, if is not, write $\psi_1 = \langle 1, -1\rangle_T \perp \psi_2$ (and of course, $\varphi = 2\langle 1, -1\rangle_T \perp \psi_2$, with $\dim \varphi_2 < \dim \varphi_1 < \dim \psi$). After a finite number of steps (instead, maximum $\dim \varphi/2$), we achieve a decomposition

$$\varphi \cong_T r\langle 1, -1\rangle \perp \psi_r,$$

where ψ_r is anisotropic (or 0). This proves the existence part.

To estabilish the uniqueness part, suppose φ has another Witt decomposition $\varphi \cong_T s\langle 1, -1\rangle_T \perp \psi'$. So

$$r\langle 1, -1\rangle \perp \psi \cong_T s\langle 1, -1\rangle \perp \psi',$$

and if $r < s$, by Witt's cancellation we have $\psi \cong_T (s - r)\langle 1, -1\rangle \perp \psi'$, contradicting the fact that ψ is anisotropic. Similarly for $s < r$, then we force $r = s$. Now, the resulting equation is

$$r\langle 1, -1\rangle \perp \psi \cong_T s\langle 1, -1\rangle \perp \psi',$$

and by Witt's cancellation (again!) we get $\psi \cong_T \psi'$, finalizing the proof. □

Having developed the "mod T" theory thus far, it is now an easy matter to set up the relative Witt ring W_TF and derive its basic properties. Since the procedure here is substantially the same as that used for ordinary Witt ring WF, we can suppress most of the details in the following discussion.

By definition, W_TF is the Grothendieck group of the T-isometry classes of all T-forms modulo the ideal generated by the T-hyperbolic plane. Addition in the Grothendieck group is given by the orthogonal sum of T-forms. Defininig multiplication in W_TF by using the tensor product of T-forms, we make W_TF into a commutative ring (with identity $\langle 1\rangle_T$). The elements of W_TF are in a one-one correspondence with the T-isometry classes of T-anisotropic forms (including, by convention, the "zero form"). Two T-forms φ, φ' will give the same element in W_TF iff their T-anisotropic parts are T-isometric (in which case we say that φ, φ' are "Witt similar", over T). Just as in the absolute theory, it follows that

$$\varphi \cong_T \psi \text{ iff } \dim(\varphi) = \dim(\psi) \text{ and } \varphi = \psi \in W_TF. \tag{2.4}$$

In particular, $\langle a\rangle \cong_T \langle b\rangle$ if and only if $ab \in \dot{T}$.

There is, however, one main phenomenon which distinguishes W_TF from WF. For any T-form φ and any integer $r \geq 1$, $r \cdot \varphi$ is T-hyperbolic iff φ is; this implies that W_TF is never torsion-free, unless F is formally real and pythagorean.

By viewing a form $\langle a_1, ..., a_n\rangle$ as a T-form, we can define a surjective ring homomorphism $WF \to W_TF$. The image of IF under this homomorphism is I_TF, the ideal of T-isometry classes of even-dimensional T-forms. Again, the n-th power I_T^nF is additively generated by the T-Pfister forms $\langle\langle a_1, ..., a_n\rangle\rangle_T$ ($a_i \in \dot{F}$). The isomorphisms $W_TF/I_TF \cong \mathbb{Z}/2\mathbb{Z}$, $I_TF/I_T^2F \cong \dot{F}/\dot{T}$ can be checked in the same way as in the absolute theory. For the second isomorphism, however, we need to know that there is a good notion of discriminants for T-forms. Since this requires a separate argument, we include it in the following

Proposition 2.2.9. *For any T-form $\varphi = \langle a_1, ..., a_n\rangle_T$, $\det \varphi := a_1 \cdot ... \cdot a_n \cdot \dot{T} \in \dot{F}/\dot{T}$ is uniquely determined by the T-isometry class of φ.*

Proof. Suppose $\varphi \cong_T \psi = \langle b_1, ..., b_n \rangle_T$, and let $c = a_1...a_n$, $d = b_1...b_n$. We want to show that $cd \in \dot{T}$; by Artin's Theorem 2.1.6, it suffices to show that $\text{sgn}_P(c) = \text{sgn}_P(d)$ for every $P \in X_T$. Given P, suppose (say) $a_1, ..., a_R \in -\dot{P}$, $a_{r+1}, ..., a_n \in \dot{P}$, $b_1, ..., b_s \in -\dot{P}$, $b_{s+1}, ..., b_n \in \dot{P}$. Since

$$n - 2r = \text{sgn}_P(\varphi) = \text{sgn}_P(\psi) = n - 2s,$$

we have $r = s$, hence

$$\text{sgn}_P(c) = (-1)^r = (-1)^s = \text{sgn}_P(d).$$

□

Using the idea of the discriminant, we can also compute $U(W_TF)$, the group of units in W_TF.

Proposition 2.2.10. $U(W_TF) = \{\langle a \rangle_T : a \in \dot{F}\}$.

Proof. It suffices to show that, if φ, ψ are T-forms such that $\varphi\psi = 1 \in W_TF$, then $\varphi = \langle a \rangle \in W_TF$ for some $a \in \dot{F}$. For any $P \in X_T$, we have $\text{sgn}_P(\varphi)\text{sgn}_P(\psi) = 1$ so $\text{sgn}_P(\varphi) = \pm 1$. In particular, φ has odd dimension, say $\varphi = \langle a_1, ..., a_{2n+1} \rangle$. We claim that $a := (-1)^n a_1...a_{2n+1}$ (the "signed" discriminant) is what we want. To see this, let $P \in X_T$. We may assume that $a_1, ..., a_n \in -\dot{P}$, and $a_{n+1}, ..., a_{2n} \in \dot{P}$. Then

$$\text{sgn}_P a = (-1)^n(-1)^n \text{sgn}_P a_{2n+1} = \text{sgn}_P(a_{2n+1}) = \text{sgn}_P(\varphi).$$

This implies that $\varphi \cong_T n\langle 1, -1 \rangle_T \perp \langle a \rangle_T$, so $\varphi = \langle a \rangle_T \in W_TF$. □

In the proof above, we have implicitly used the idea that a T-form φ may be "identified" with the signature function it defines on the Boolean space X_T. We shall now formulate this idea more precisely. In the following, we shall write $C(X_T, \mathbb{Z})$ for the ring of continuous functions from X_T to $\mathbb{Z}$. Whenever we use this notation, it will always be understood that $\mathbb{Z}$ is given the discrete topology.

Since X_T is compact, the image of any continuous function $f : X_T \to \mathbb{Z}$ must be a finite set, and, for r ranging over this image, the sets $f^{-1}(r)$ form a finite partition of X_T into clopens sets. Conversely, given any finite partition of X_T into clopens $C_1, ..., C_k$, we can define continuous functions $f \in C(X_T, \mathbb{Z})$ by sending $C_1, ..., C_k$ to arbitrary integers $n_1, ..., n_k$. Therefore, as an abelian group, $C(X_T, \mathbb{Z})$ is generated by the characteristic functions of the clopen sets in X_T.

For any T-form φ, we can define its "signature function" $\hat{\varphi} : X_T \to \mathbb{Z}$ by $\hat{\varphi}(P) = \text{sgn}_P(\varphi)$, for every $P \in X_T$. Follows that

$$\varphi \hat{\perp} \psi = \hat{\varphi} + \hat{\psi} \text{ and } \widehat{\psi\varphi} = \hat{\varphi}\hat{\psi}.$$

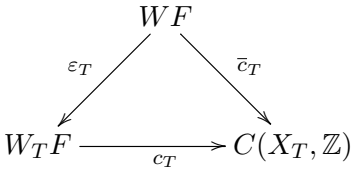
In case φ is a unary form $\langle a \rangle_T$, we have $\hat{\varphi}(X_T) \subseteq \{\pm 1\}$, with

$$\hat{\varphi}^{-1}(1) = H_T(a) \text{ and } \hat{\varphi}^{-1}(-1) = H_T(-a). \tag{2.5}$$

Therefore $\hat{\varphi}$ is continuous. By the first formula in 2.5, we see that the same is true for higher-dimensional T-forms φ.

If we define $c_T(\varphi) = \hat{\varphi}$ for any T-form φ, we get a well-defined map $c_T : W_TF \to C(X_T, \mathbb{Z})$ (the "cap" map). By 2.5, c_T is a ring homomorphism. If $c_T(\varphi) = 0$, then by definition φ is a T-hyperbolic form, so $\varphi = 0 \in W_TF$: this shows that c_T is a monomorphism. Now consider the

diagram



where $\varepsilon_T\langle a_1, ..., a_n\rangle = \langle a_1, ..., a_n\rangle$, and $\bar{c}_T = c_T \circ \varepsilon_T$.

Theorem 2.2.11 (Pfister, Becker,...)**.** *$Ker(\varepsilon_T) = Ker(\bar{c}_T) = WF/\sum_{t\in\dot{T}} WF \cdot \langle 1, -t\rangle$.*

Proof. Since c_T is injective, we have $\mathrm{Ker}(\varepsilon_T) = \mathrm{Ker}(\bar{c}_T)$ so it suffices to compute the latter. Of course, it contains $\mathfrak{U} := \sum_{t\in\dot{T}} WF \cdot \langle 1, -t\rangle$. Conversely, let $\varphi = \langle a_1, ..., a_n\rangle \in \ker(\bar{c}_T)$; we shall show that $\varphi \in \mathfrak{U}$ by induction on n. The case $n = 0$ is immediate. If $n > 0$, since φ is T-hyperbolic as a T-form, there exists an equation $\sum t_i a_i = 0$ where $t_i \in T$ are not all zero (see 2.2.5). Let

$$a'_i = \begin{cases} a_i \text{ if } t_i = 0 \\ t_i a_i \text{ if } t_i \neq 0 \end{cases}$$

and consider $\varphi' = \langle a'_1, ..., a'_n\rangle$. Working in WF, we have

$$\varphi - \varphi' = \sum_{t_i\neq 0} a_i\langle 1, -t_i\rangle \in \mathfrak{U},$$

so it suffices to show that $\varphi' \in \mathfrak{U}$. Since φ' is isotropic, we have $\varphi' \cong_T \langle 1, -1\rangle \perp \varphi''$ for some $(n-2)$-dimensional form φ''. Then

$$\bar{c}_T(\varphi'') = \bar{c}_T(\varphi') = \bar{c}_T(\varphi) = 0,$$

so by the inductive hypothesis, we have $\varphi'' \in \mathfrak{U}$, hence $\varphi \in \mathfrak{U}$. □

In the case when $T = \sum \dot{F}^2$. Thus, we get back Pfister Local-Global Principle, 1.5.1. Note that if w is a sum of 2^n squares, then $2^n\langle 1, -w\rangle$ is isotropic, and hence (by Pfister form theory) hyperbolic. This shows that the kernel above is in W_tF, the torsion subgroup of WF. On the other hand, since $C(X_F, \mathbb{Z})$ is torsion-free, W_tF must be contained in $\ker(WF \to C(X_F, \mathbb{Z}))$. Therefore, this kernel equals W_tF, and we get

$$W_TF \cong WF/\sum WF \cdot \langle 1, -w\rangle = WF/W_tF$$

for $T = \sum \dot{F}^2$. This ring, usually denoted by $W_{red}F$ is called the **reduced Witt ring** of F.

Returning to a general preordering T, we record for later reference the following consequence of 2.2.11:

Corollary 2.2.12. *W_TF is isomorphic to the group G with generators $[a]$, $a \in \dot{F}$, and relations*

1. $[1] + [-1] = 0$,
2. $[a] + [b] = [a + b] + [ab(a + b)]$, $a, b, a + b \in \dot{F}$,
3. $[a] = [at]$, $a \in \dot{F}$, $t \in \dot{T}$.

Proof. If we use only relations of the type (1), (2), together with the following special case of (3):

$$(3')\ [a] = [ac^2]\ (a, c \in \dot{F}),$$

the group we get is isomorphic to WF, via $[a] \mapsto \langle a\rangle$ (see 1.3.18). According to 2.2.11, W_TF is isomorphic to WF modulo the subgroup generated by $\langle a\rangle\langle 1,-t\rangle = \langle a,-at\rangle$ ($a \in \dot{F}$, $t \in \dot{T}$), and this finalize the proof. □

Another way to prove 2.2.12 is to first estabilish a "chain-equivalence" theorem for T-isometries, generalizing Witt's Chain Equivalence Theorem for ordinary isometries (1.2.5). To this end, we define the notion of chain-T-equivalence as follows: given two T-forms φ, ψ of the same dimension n, φ is chain-T-equivalent to ψ if we can change φ to ψ by a finite sequence of transformations of the following types:

A - $\langle a_1,...,a_n\rangle_T \to \langle t_1a_1,...,t_na_n\rangle$ ($t_i \in \dot{T}$);

B - $\langle a_1,...,a_i,...,a_j,...,a_n\rangle_T \mapsto \langle a_1,...,a_i+a_j,...,a_ia_j(a_i+a_j),...,a_n\rangle_T$,
($a_i, a_i+a_j \in \dot{F}$, $1 \le i \le j \le n$);

C - $\langle a_1,...,a_i,...,a_j,...,a_n\rangle_T \mapsto \langle a_1,...,a_j,...,a_i,...,a_n\rangle_T$.

If φ is chain-T-equivalent to ψ then $\varphi \cong_T \psi$. Not surprisingly, we have the following analog of Witt's Chain Equivalence Theorem:

Theorem 2.2.13. *Let $\varphi = \langle a_1,...,a_n\rangle_T$ and $\psi = \langle b_1,...,b_n\rangle_T$. If $\varphi \cong_T \psi$ then φ is chain T-equivalent to ψ.*

Proof. Since the symmetric group S_n is generated by transpositions, (C) implies that $\langle a_1,...,a_n\rangle_T$ is chain-T-equivalent to $\langle a_{\sigma(1)},...,a_{\sigma(n)}\rangle_T$ for any permutation σ. If $\varphi \cong_T \psi$, 2.2.6 implies that $b_1 \in D_T(\varphi)$, so, after permuting the a_i's, we may assume that $b_1 = t_1a_1 + ... + t_ra_r$ (for some $r \le n$) where no subsum is equal to zero, and $t_i \in \dot{T}$. Applying the transformations (A) and (B) repeatedly (as we made in the proof of 2.2.6), we see that φ is chain-T-equivalent to some $\langle b_1, a_2',...,a_n'\rangle_T$. After cancelling $\langle b_1\rangle_T$, we have

$$\langle a_2',...,a_n'\rangle_T \cong_T \langle b_2,...,b_n\rangle_T$$

so, the proof proceeds by induction. □

In the definition of chain-T-equivalence, one could have dropped the transformations of type (C) without affecting the definition. To see this, it suffices to show that $\langle a,b\rangle_T$ can be changed into $\langle b,a\rangle_T$ by transformations of the type (A), (B). If $a+b=0$, we are done by

$$\langle a,-a\rangle \overset{(A)}{\to} \langle a,-2a\rangle \overset{(B)}{\to} \langle -a,2a^3\rangle \overset{(A)}{\to} \langle -a,a\rangle.$$

If $c := a+b \neq 0$, we have instead

$$\langle a,b\rangle \overset{(B)}{\to} \langle c,abc\rangle \overset{(A)}{\to} \langle b^2c,abc\rangle \overset{(B)}{\to} \langle bc^2, bc^2\cdot b^2c\cdot abc\rangle \overset{(A)}{\to} \langle b,a\rangle.$$

Using 2.2.13, we could give another proof for 2.2.12: for the group G in 2.2.12, we have a group homomorphism $f : G \to W_TF$ defined by $f[a] = \langle a\rangle_T \in W_TF$. By 2.2.13, we check that

$$g(\langle a_1,...,a_n\rangle_T) = [a_1] + ... + [a_n] \in G$$

gives a well-defined inverse for f. Therefore f is an isomorphism.

2.3 Some basic stuff about Valuations

We already talk about orderings and quadratic forms. To complet our "Lam's tripé" we shall talk about valuations. The concept of valuations are like an Hydra: have many heads and each time you cut one, three or more borns again! Here, we restrict our atention to three heads of this "Hydra": Krull valuations, valuation rings and places.

So, let us start with valuation rings.

Definition 2.3.1. *A subring A of a field K is called a* ***valuation ring*** *of K, if $x \in A$ or $x^{-1} \in A$ for any non-zero $x \in K$. Is immediate that K is the quotient field of A.*

A non-trivial binary relation $|\subseteq K \times K$ (i,e, $|\neq K \times K$) of a field K is a called a **divisibility** if:

i - $|$ is a preordering (i.e, is reflexive and transitive);

ii - $x \mid y \Rightarrow xz \mid yz$ for all $x, y, z \in K$;

iii - $x \mid y$ and $x \mid z \Rightarrow x \mid y - z$ for all $x, y, z \in K$.

Note that $x \mid 0$ and does not hold $0 \mid x$ for any $x \in \dot{K}$. Beside this, the divisibilities $|$ of K are in one-to-one correspondence with the subrings D of K by

$$\{x \mid y \Leftrightarrow yx^{-1} \in D\} \text{ and } D = \{x \in K : 1 \mid x\}.$$

Moreover, $U_D = \{x \in D : x \mid 1\}$ is the group of units of D.

Theorem 2.3.2. *A subring R of K is a valuation ring of K if and only if the corresponding divisibility $|_R$ is an ordering.*

Proof. ($\Rightarrow$) Suppose R is a valuation ring and let $x \nmid y$. If $x = 0$, then $y \mid x$. If $x \neq 0$, then $yx^{-1} \notin R$, so $(yx^{-1})^{-1} = xy^{-1} \in R$. Then $1 \mid xy^{-1}$ and $y \mid x$, showing that $|$ is an ordering.

($\Leftarrow$) Suppose $|_R$ is an ordering an let $x \in K \setminus R$ with $1 \nmid x$. Since $|$ is an ordering, $x \mid 1$, and $1 \cdot x^{-1} \in R$. Then R is a valuation ring. □

A subset M of K is called R**-stable** if $R \cdot M \subseteq M$, i.e, $ax \in M$ for all $a \in R$ and $x \in M$. We show that in the case of a valuation ring R any R-stable non-empty subset of R (resp. K) is an ideal of R (resp. an R-submodule of K) and this property characterizes valuation rings.

Theorem 2.3.3. *Let K be the quotient field of R and J (resp. $\mathcal{J}$) the set of all R-stable non-empty subsets of R (resp. K). Then the following conditions are equivalent:*

i - R is a valuation ring of K;

ii - $\mathcal{J}$ is totally ordered;

iii - J is totally ordered;

iv - The subset of J consisting of all principal ideals of R is totally ordered.

In this case, J (resp. $\mathcal{J}$) is the set of all ideals of R (resp. R-submodules of K).

Proof. (i)$\Rightarrow$(ii) Suppose that $M, N \in \mathcal{J}$. $M \nsubseteq N$ and $N \nsubseteq M$. Let $x \in M \setminus N$ and $y \in N \setminus M$. Since $x = (xy^{-1})y \notin N$ we have $xy^{-1} \notin R$, and since $y = (yx^{-1})x \notin M$, we have $yx^{-1} \notin R$; therefore R is not a valuation ring of K.

(ii)$\Rightarrow$(iii) Is immediate since every R-stable set in $\mathcal{J}$ provides an R-stable set in J.

(iii)⇒(iv) Is immediate since this is a subset of a (totally) ordered set.

(iv)⇒(i) Let $x = a/b \in K$, $a \neq b$, $a, b \neq 0$. If $x \notin R$, then $R \cdot a \nsubseteq R \cdot b$. By (iv), $R \cdot b \subseteq R \cdot a$, and then $x^{-1} = b/a \in R$. Hence R is a valuation ring of K.

For the last statement, it suffices to show that for any $M \in \mathcal{J}$ and $x, y \in M \setminus \{0\}$ we have $x - y \in M$. In fact, if $R \cdot x \subseteq R \cdot y$ then $x - y = (xy^{-1} - 1) \cdot y \in R \cdot y \subseteq M$; if $R \cdot x \nsubseteq R \cdot y$, then $R \cdot y \subseteq R \cdot x$ and $x - y = (1 - yx^{-1})x \in R \cdot x \subseteq M$. □

Corollary 2.3.4. *Any valuation ring is a local ring.*

Proof. For any valuation ring A the set $A \setminus U_A$ is A-stable, hence by 2.3.3 we get that $A \setminus U_A$ is an ideal. □

Valuation rings are not noetherian, in general. However,

Corollary 2.3.5. *Any finitely generated ideal of a valuation ring A is principal.*

Proof. Let $\mathfrak{U} = A \cdot a_1 + ... + A \cdot a_m$. By 2.3.3, $\{A \cdot a_1, ..., A \cdot a_m\}$ has a largest element, say $A \cdot a_1 \supseteq A \cdot a_i$, $i = 1, ..., m$. Then $\mathfrak{U} \subseteq A \cdot a_1 \subseteq \mathfrak{U}$. □

We shall use the fact that, for any subring R of K and any prime ideal $\mathfrak{p}$ of R, the prime ideals $\mathfrak{q}$ of the ring of fractions $R_\mathfrak{p}$ are in one-to-one correspondence with those prime ideals $\mathfrak{r}$ of R which are contained in $\mathfrak{p}$, by $\mathfrak{q} = \mathfrak{r} \cdot R_\mathfrak{p}$ and $\mathfrak{r} = \mathfrak{q} \cap R$. In particular, $R_\mathfrak{p}$ is a local ring with the maximal ideal $\mathfrak{p}R_\mathfrak{p}$.

Theorem 2.3.6. *Let A be a valuation ring of K, $\mathfrak{P}$ the set of all prime ideals $\mathfrak{p}$ of A and $\mathcal{B}$ the set of all subrings B of K which contains A. Then any $B \in \mathcal{B}$ is a valuation ring of K with $\mathfrak{m}_B \subseteq A$, and there is an inclusion inverting one-to-one correspondence $\mathcal{B} \leftrightarrow \mathfrak{P}$ given by $\mathfrak{p} = \mathfrak{m}_B$ and $B = A_\mathfrak{p}$.*

Proof. Let $B \in \mathfrak{B}$. For any $x \in K$, $x \notin B$ implies $x \notin A$, hence $x^{-1} \in A \subseteq B$, whereas $x \in \mathfrak{m}_B$ implies $x^{-1} \notin B$, hence $x \in A$.

For any $B \in \mathcal{B}$, $\mathfrak{m}_B \cap A = \mathfrak{m}_B$ is a prime ideal of A, with $A_{\mathfrak{m}_B} \subseteq B$. Even $A_{\mathfrak{m}_B} = B$, since if $x \in B \setminus A$ then $x^{-1} \in A \subseteq B$, $x^{-1} \notin \mathfrak{m}_B$, hence $x \in A_{\mathfrak{m}_B}$. For any $\mathfrak{b} \in \mathfrak{B}$ we have $A_\mathfrak{b} \in \mathcal{B}$, and

$$\mathfrak{m}_{A_\mathfrak{b}} = \mathfrak{m}_{A_\mathfrak{b}} \cap A = \mathfrak{b} \cdot A_\mathfrak{b} \cap A = \mathfrak{b}.$$

Finally, by construction (i.e, by general properties of ideals and fractions) the correspondence $\mathfrak{B} \leftrightarrow \mathcal{B}$ is inclusion reversing. By 2.3.3 $\mathfrak{B}$ is (totally) ordered, hence so is $\mathcal{B}$. □

Definition 2.3.7. *A **Krull valuation** of a field K is a mapping $v : \dot{K} \to \Gamma \cup \{\infty\}$ onto a (totally) ordered abelian group Γ, the **value group** of v, satisfying the axioms:*

V0 - $v(x) = \infty \Leftrightarrow x = 0$ *for all* $x \in K$;

V1 - $v(xy) = v(x) + v(y)$ *for any* $x, y \in \dot{K}$;

V2 - $v(x + y) \geq \min\{v(x), v(y)\}$ *for* $x, y \in \dot{K}$.

Two Krull valuations v_1, v_2 of K with the value groups Γ_1, Γ_2 respectively, are called **equivalent** if there is an isomorphism (of ordered groups) $t : \Gamma_1 \to \Gamma_2$ such that $v_2 = t \circ v_1$ (with the convention $t(\infty) = \infty$). Note that any bijective order-preserving homomorphism $\Gamma_1 \to \Gamma_2$ is an isomorphism. In particular, its inverse is also order-preserving.

Theorem 2.3.8. *For any Krull valuation v of K, the set $A_v = \{x \in K : v(x) \geq 0\}$ is a valuation ring of K.*

The mapping $v \mapsto A_v$ induces a bijection from the set of all equivalence classes of Krull valuations of K onto the set of all valuation rings of K.

Proof. A_v is a valuation ring of K, since $x \in K \setminus A_v$ implies $v(x) < 0$, and $v(x^{-1}) > 0$, so $x^{-1} \in A_v$. For equivalent v_1, v_2 we have $v_1(x) \geq 0$ iff $v_2(x) \geq 0$ for all $x \in K$, hence $A_{v_1} = A_{v_2}$.

For any valuation ring A of K we define a (the canonical) Krull valuation as follows: the divisibility of K corresponding to A is an ordering of the multiplicative group $\dot{K}$ of K, by 2.3.2. The factor group $\Gamma_A = \dot{K}/U_A$ is an ordered abelian group; we write it additively and denote its ordering by $\leq$. The canonical homomorphism $v_A : \dot{K} \to \Gamma_A$, extended to K by setting $v_A(0) = \infty$, is a Krull valuation of K with value group Γ_A and $A_v = A$. In fact, $v_A : K \to \Gamma_A \cup \{\infty\}$ is surjective and satisfies V0 and V1, as well as $x \in A \Leftrightarrow v(x) \geq 0$ for all $x \in K$. Now, let $x, y \in K$ such that $v(x) \leq v(y)$. Then $x^{-1}y \in A$ and so $1 + x^{-1}y \in A$. Hence

$$v_A(x+y) = v_A(x(1+x^{-1}y)) = v_A(x) + v_A(1+x^{-1}y) \geq v_A(x) = \min\{v(x), v(y)\};$$

therefore V2 is satisfied too. We have still to show that if $A = A_v$ then v is equivalent to A_v. In fact, since v is surjective and has kernel U_A, it induces an ordering preserving bijection ι from $\Gamma_A = \dot{K}/U_A$ onto the value group Γ of v, and this is even an isomorphism $\iota : \Gamma_A \to \Gamma$ such that $v = \iota \circ v_A$. □

The preceding proof shows that the Krull valuations of K are essentially (up to equivalence) the canonical mappings $v_A : \dot{K} \to \Gamma_A = \dot{K}/U_A$ corresponding to valuation rings A of K. In fact, it would be possible (but sometimes inconvenient) to work only with these canonical Krull valuations.

Here are some examples of valuations.

Example 2.3.9 (Valuations on $\mathbb{Q}$)**.** *Let p be a prime number. We define the **p-adic valuation** v_p on $\mathbb{Q}$ by*

$$v_p(p^r n/p^s m) = r - s$$

for $n, m \in \mathbb{Z}$ are not divisible by p. It is a discrete valuation[2] with residue field $\mathbb{F}_p$.

Example 2.3.10 (The Degree valuation)**.** *Let K be a field and $F = K(t)$. For a polynomial $f \in K[t]$, define $v(f(t)) = -\deg(f)$, and for $f/g \in K(t)$, set $v(f/g) = \deg g - \deg f$. This mapping define a valuation on $K(t)$, called the **degree valuation**.*

Example 2.3.11 (Laurent Series)**.** *Let $K((t))$ be the field of Laurent series. An typical element in $K((t))$ is a serie $\sum_N^\infty a_i t^i$, where $N \in \mathbb{Z}$, $a_i \in K$ for all $i \geq N$. When $a_N \neq 0$, we define*

$$v\left(\sum_N^\infty a_i t^i\right) = N.$$

This mapping prescribes a valuation on $K((t))$.

Now, we show that the valuation rings A of K are in one-to-one correspondence with the equivalence classes of places of K and that the places corresponding to A are essentially the canonical homomorphisms from A onto the residue field $A/\mathfrak{m}_A$.

[2] A valuation v on a field F is **discrete** if $v(\dot{F}) \cong \mathbb{Z}$.

For the definition of places, we have to extend fields to **projective fields**, adjoining an element ∞. More precisely, the projective fields obtained from the field K is the set $\tilde{K} = K \cup \{\infty\}$ endowed with the addition and the multiplication of K extended to $\tilde{K}$ by

$$x + \infty = \infty + x = \infty \text{ for all } x \in K;$$
$$x \cdot \infty = \infty \cdot x = \infty \text{ for all } x \in K.$$

Moreover, we set $0^{-1} = \infty$, $\infty^{-1} = 0$, and $-\infty = \infty$. Note that $\infty + \infty$, $0 \cdot \infty$ and $\infty \cdot 0$ are not all defined.

Definition 2.3.12. *A **place** of K into L is a mapping $\pi : \tilde{K} \to \tilde{L}$ satisfying the following conditions for all $x, y \in \tilde{K}$:*

P1 - *If $x + y$ and $\pi(x) + \pi(y)$ are defined then $\pi(x + y) = \pi(x) + \pi(y)$;*

P2 - *If xy and $\pi(x)\pi(y)$ are defined then $\pi(xy) = \pi(x)\pi(y)$;*

P3 - *There is some $z \in \tilde{K}$ such that $\pi(z) = 1$.*

We state some elementary properties of places:

Proposition 2.3.13. *a -* $\pi(1) = 1$, $\pi(0) = 0$, $\pi(\infty) = \infty$.

b - If $\pi(x) + \pi(y)$ (resp $\pi(x)\pi(y)$) is defined then so is $x + y$ (resp xy).

c - $\pi(-x) = -\pi(x)$.

d - $\pi(x^{-1}) = \pi(x)^{-1}$.

e - $\pi^{-1}(L)$ is a valuation ring A_π of K, and $\pi|_{A_\pi} : A_\pi \to L$ is a ring homomorphism with kernel $\mathfrak{m}_{A_\pi}$.

f - $\pi^{-1}(\dot{L}) = U_{A_\pi}$ and $\pi|_{U_{A_\pi}} : U_{A_\pi} \to \dot{L}$ is a multiplicative homomorphism with kernel $1 + \mathfrak{m}_{A_\pi}$.

Proof.

a - Let $z \in \tilde{K}$ such that $\pi(z) = 1$. Then $z \cdot 1$ and $\pi(z) \cdot \pi(1)$ are defined, hence

$$1 = \pi(z) = \pi(z \cdot 1) = \pi(z)\pi(1) = 1\pi(1) = \pi(1).$$

Since $1 + 0$ and $\pi(1) + \pi(0)$ are defined, we have

$$1 = \pi(1) = \pi(1 + 0) = \pi(1) + \pi(0) = 1 + \pi(0),$$

so $\pi(0) = 0$. Since $1 + \infty$ and $\pi(1) + \pi(\infty)$ are defined, we have

$$\pi(\infty) = \pi(1 + \infty) = \pi(1) + \pi(\infty) = 1 + \pi(\infty),$$

so $\pi(\infty) = \infty$.

b - If $\pi(x)+\pi(y)$ is defined then $(\pi(x), \pi(y)) \neq (\infty, \infty)$, hence $(x, y) \neq (\infty, \infty)$ by (a), so $x+y$ is defined. If $\pi(x)\pi(y)$ is defined then $(\pi(x), \pi(y)) \notin \{(0, \infty), (\infty, 0)\}$, since $(x, y) \notin \{(0, \infty), (\infty, 0)\}$ by (a), xy is defined.

c - If $\pi(-x)+\pi(x)$ is not defined, then $\pi(x)=\pi(-x)=\infty$, then $-\pi(x)=\infty$. If $\pi(-x)+\pi(x)$ is defined then so is $-x+x$, then

$$0=\pi(-x+x)=\pi(-x)+\pi(x)$$

provides $\pi(-x)=-\pi(x)$.

d - If $\pi(x^{-1})\pi(x)$ is not defined then $(\pi(x^{-1}),\pi(x))\in\{(0,\infty),(\infty,0)\}$, so $\pi(x^{-1})=\pi(x)^{-1}$. If $\pi(x^{-1}\pi(x)$ is defined, then so is $x^{-1}x$, hence

$$1=\pi(1)=\pi(x^{-1}x)=\pi(x^{-1})\pi(x),$$

then $\pi(x^{-1})=\pi(x)^{-1}$.

e - We have $\pi^{-1}(L)\subseteq K$ since $\pi(\infty)=\infty$. By (b) and (c) we get that $\pi^{-1}(L)$ is a subring A_π of K. If $x\in K\setminus A_\pi$ then $\pi(x)=\infty$, so $\pi(x^{-1})=0$ by (d), providing $x^{-1}\in A_\pi$. Therefore A_π is a valuation ring of K. Of course, $\pi|_{A_\pi}$ is a ring homomorphism with kernel $\mathfrak{m}_\pi\subseteq\mathfrak{m}_{A_\pi}$. We have even $\mathfrak{m}_\pi=\mathfrak{m}_{A_\pi}$, since $x\in\mathfrak{m}_{A_\pi}$ implies $x^{-1}\notin A_\pi$, $(\pi(x))^{-1}=\pi(x^{-1})=\infty$, $\pi(x)=0$.

f - $\pi^{-1}(\dot{L})=\{x\in A_\pi:\pi(x)\neq 0\}=A_\pi/\mathfrak{m}_{A_\pi}$, so $\pi|_{U_{A_\pi}}$ is a multiplicative morphism. Its kernel is $1+\mathfrak{m}_{A_\pi}$, since $\pi(x)=1$ if and only if $\pi(x-1)=0$, if and only if $x-1\in\mathfrak{m}_{A_\pi}$.

□

By 2.3.13(e), any place of K into L induces a homomorphism $\lambda:A\to L$ from a valuation ring A of K into L, with kernel $\mathfrak{m}_A$. The converse is also true:

Theorem 2.3.14. *Let A be a valuation ring of K and $\lambda:A\to L$ a homomorphism into a field L, with kernel $\mathfrak{m}_A$. Then the mapping $\pi:\tilde{K}\to\tilde{L}$, defined by $\pi(x)=\lambda(x)$ for all $x\in A$ and $\pi(x)=\infty$ for all $x\in\tilde{K}\setminus A$ is a place of K into L with $A_\pi=A$.*

Proof. It suffices to verify P1 and P2. $\pi(x)+\pi(y)$ is defined if and only if $(\pi(x),\pi(y))\neq(\infty,\infty)$. If $\pi(x)\neq\pi(y)$ and $\pi(y)=\infty$, then $x\in A$, $y\in\tilde{K}\setminus A$, then $\pi(x+y)=\infty=\pi(x)+\pi(y)$. If $\pi(x),\pi(y)\neq\infty$, then $x,y\in A$, so

$$\pi(x+y)=\lambda(x+y)=\lambda(x)+\lambda(y)=\pi(x)+\pi(y).$$

The proof of P2 is a similar argument. □

A place $\pi:\tilde{K}\to\tilde{L}$ is called **trivial** if $A_\pi=K$, or equivalently, $\mathfrak{m}_{A_\pi}=(0)$. The trivial places of K into L are exactly the monomorphisms $\mu:K\to L$ extended by $\mu(\infty)=\infty$.

Let K_0 be any subfield of K. Then $\tilde{K}_0$ is a projective subfield of $\tilde{K}$ (i.e, addition and multiplication in $\tilde{K}_0$ are induced by those in $\tilde{K}$) and that, for any place $\pi:\tilde{K}\to\tilde{L}$, the restriction $\pi|_{\tilde{K}_0}:\tilde{K}_0\to\tilde{L}$ is a place of K_0 into L. In particular, the restriction of π to the prime field of K is non-trivial if and only if $\mathrm{Char}(L)\neq\mathrm{Char}(K)$, and in this case, $\mathrm{Char}(K)=0$.

For any place $\pi:\tilde{K}\to\tilde{L}$, the image $\pi(A_\pi)$ of A_π is a subfield of L, called the **residue field** of π, and π can also be considered as a place of K into $\pi(A_\pi)$. We have $L=\pi(A_\pi)$ if and only if $\pi:\tilde{K}\to\tilde{L}$ is surjective; in this case, π is called a place of K onto L, or a surjective place. In particular, for any valuation ring A of K, the canonical homomorphism $q_A:A\to A/\mathfrak{m}_A$ extends to a place π_A of K onto $A/\mathfrak{m}_A$, by 2.3.14; π_A is called the **canonical place** corresponding to A.

Places can be composed similarly as homomorphisms:

Proposition 2.3.15. *Let $\pi : \tilde{K} \to \tilde{L}$ and $\xi : \tilde{L} \to \tilde{M}$ be places and let A_π (resp. B_ξ) be the valuation ring of K (resp. L) corresponding to π (resp. L). Then $\xi \circ \pi : \tilde{K} \to \tilde{M}$ is a place and $A_{\xi\circ\pi} = \pi^{-1}B_\xi \subseteq A_\pi$. If π is a place of K onto L, then $\pi(A_{\xi\circ\pi}) = B_\xi$.*

Proof. $\xi \circ \pi$ satisfies P1, since if $(\xi \circ \pi)(x) + (\xi \circ \pi)(y)$ is defined then, by 2.3.13(b), $\pi(x) + \pi(y)$ and $x + y$ are defined and

$$(\xi \circ \pi)(x) + (\xi \circ \pi)(y) = \xi(\pi(x) + \pi(y)) = (\xi \circ \pi)(x + y).$$

Similarly P2 is verified. P3 follows from $\xi(\pi(1)) = \xi(1) = 1$. For any $x \in \tilde{K}$ we have $x \in A_{(\xi\circ\pi)}$ if and only if $\xi(\pi(x)) \neq \infty$, if and only if $\pi(x) \in B_\xi$, if and only if

$$x \in \pi^{-1}(B_\xi) \subseteq \pi^{-1}(L) = A_\pi.$$

If $\pi : \tilde{K} \to \tilde{L}$ is surjective, then $A_{(\xi\circ\pi)} = \pi^{-1}(B_\xi)$ implies $\pi(A_{(\xi\circ\pi)}) = B_\xi$. □

We use the composition of places for defining a preordering on the class of all surjective places of a fixed field K:

Proposition 2.3.16. *Let π_0, π_1 be surjective places of K. Are equivalent:*

i - $A_1 \subseteq A_0$;

ii - *There exists a mapping $\xi : \tilde{L}_0 \to \tilde{L}_1$ such that $\pi_1 = \xi \circ \pi_0$. In this case ξ is a uniquely determined place of L_0 onto L_1.*

We write $\pi_1 \preceq \pi_0$ if one (and therefore all) of the equivalent conditions above holds.

Proof. (i)⇒(ii) It suffices to prove that $\xi : \pi_0(x) \mapsto \pi_1(x)$ $(x \in \tilde{K})$ is well-defined. Let $x, y \in \tilde{K}$ such that $\pi_0(x) = \pi_0(y)$.

If $x \notin A_0$, then $\pi_0(x) = \pi_0(y) = \infty$, $y \notin A_0$, and then $x, y \notin A_1$, hence $\pi_1(x) = \pi_1(y) = \infty$.

If $x \in A_0$ then $\pi_0(x) \neq \infty$, hence $\pi_0(x) + \pi_0(-y)$ is defined and

$$\pi_0(x - y) = \pi_0(x) - \pi_0(y) = 0.$$

So $x - y \in \mathfrak{m}_{A_0} \subseteq \mathfrak{m}_{A_1} \subseteq A_1$, by 2.3.6. Let $x \notin A_1$; then $y \notin A_1$, $\pi_1(x) = \infty = \pi_1(y)$. Let $x \in A_1$; then $\pi_1(x) \neq \infty$, hence $\pi_1(x) + \pi_1(-y)$ is defined and $\pi_1(x - y) = 0$, so $\pi_1(x) = \pi_1(y)$.

(ii)⇒(i) To prove that ξ is a place of L_0, it suffices to verify P1 and P2 for ξ. Let $\overline{x}, \overline{y} \in \tilde{L}_0$ such that $\overline{x} + \overline{y}$ and $\xi(\overline{x}) + \xi(\overline{y})$ are defined, and let $x, y \in \tilde{K}$ such that $\overline{x} = \pi_0(x)$, $\overline{y} = p_0(y)$; then $\pi_1(x) = \xi(\overline{x})$, $\pi_1(y) = \xi(\overline{y})$. Since $\pi_0(x) + \pi_0(y)$ (resp. $\pi_1(x) + \pi_1(y)$) is defined, we have $\pi_0(x + y) = \pi_0(x) + \pi_0(y)$ (resp. $\pi_1(x + y) = \pi_1(x) + \pi_1(y)$), by 2.3.13(b). Then

$$\xi(\overline{x} + \overline{y}) = \xi(\pi_0(x + y)) = \pi_1(x + y) = \pi_1(x) + \pi_1(y) = \xi(\overline{x}) + \xi(\overline{y}).$$

P2 is proven similarly. Hence ξ is a place of L_0, and (i) follow from 2.3.15. Since π_0 and π_1 are surjective, ξ is uniquely determined and it is a place of L_0 onto L_1. □

In particular, for any surjective place π of K we have $\pi \preceq t_K$ (the trivial place determined by the identity of K), and $t_K \preceq \pi$ if and only if π is trivial.

Two surjective places π_0, π_1 of K are called **equivalent** if $\pi_0 \preceq \pi_1$ and $\pi_1 \preceq \pi_0$. We conclude from 2.3.16:

Proposition 2.3.17. *With the notation of 2.3.16 the following conditions are equivalent:*

i - $A_1 = A_0$.

ii - $\pi_1 = \xi \circ \pi_0$ *for some bijective mapping* $\xi : \tilde{L}_0 \to \tilde{L}_1$.

iii - $\pi_1 = \xi \circ \pi_0$ *for some trivial place* ξ *of* L_0.

iv - π_1 *is equivalent to* π_0.

Moreover, 2.3.14, 2.3.17 yield the following statement, similar to 2.3.8:

Proposition 2.3.18. *The mapping* $\pi \to A_\pi$ *induces a bijection from the set of all equivalence classes of surjective places of* K *onto the set of all valuation rings of* K.

By means of the composition of places, one gets a survey on the set of all valuation rings of K contained in some given valuation ring A_0 of K. In fact, these valuations rings are in one-to-one correspondence with the valuation rings of the residue field $A_0/\mathfrak{m}_{A_0}$, as the following theorem shows:

Theorem 2.3.19. *Let* A_0 *be a valuation ring of* K *and* π_0 *a place of* K *onto* L_0 *with* $A_{\pi_0} = A_0$. *Then there is an inclusion preserving one-to-one correspondence between the set* G_0 *of all valuation rings* A *of* K *contained in* A_0 *and the set* $\mathcal{B}$ *of all valuation rings* B *of* L_0, *given by* $B = \pi_0(A)$ *and* $A = \pi^{-1}(B)$.

Proof. For any $A \in G_0$ we have $\pi_A = \xi \circ \pi_0$ for some place ξ of L_0 onto $A/\mathfrak{m}_A$, by 2.3.16, and $\pi_0(A) = B_\xi \in \mathcal{B}$ by 2.3.15. Since $A = \pi_0^{-1}(B_\xi)$ by 2.3.15, the mapping $G_0 \to \mathcal{B}$ defined by $A \mapsto \pi_0(A)$ is injective. It is also surjective, since if $B \in \mathcal{B}$ then $B = B_\xi$ for some place ξ of L_0, and $\pi = \xi \circ \pi_0$ is a place of K with $A_\pi \in G_0$ and $\pi_0(A_0) = B$, by 2.3.15. Moreover, this mapping is inclusion-preserving and so is its inverse. □

2.4 Compatibility between Valuations and Orderings

In this section, we shall introduce the important notion of "compatibility between valuations and orderings in (formally real) fields. This notion provides the main link between valuation theory and the theory of ordered fields.

Remembering: by a valuation on a field F, we shall always mean a "Krull valuation" $v : F \to \Gamma \cup \{\infty\}$ in the sense of definition 2.3.7.

The *value group* Γ will always be written additively, unless it is stated otherwise. For a given valuation v as above, we can define the following collection of associated objects:

i - The valuation ring of v, $A := \{x \in F : x = 0 \text{ or } v(x) \geq 0\}$.

ii - The maximal ideal of v, $\mathfrak{m} := \{x \in F : x = 0 \text{ or } v(x) > 0\}$.

iii - The group of valuation units, $U := A \setminus \mathfrak{m}$.

iv - The residue class field of v, $\overline{F} := A/\mathfrak{m}$.

v - The place associated with v, $\pi : F \cup \{\infty\} \to \overline{F} \cup \{\infty\}$, defined by

$$\pi(x) = \begin{cases} x + \mathfrak{m} \in \overline{F} \text{ if } x \in A, \\ \infty \text{ if } x \notin A \end{cases}$$

Usually, we work with one valuation at a time, so given $x \in A$, we shall simply write $\overline{x}$ for $x + \mathfrak{m}$, its image in the residue class field. In the same vein, we shall adopt the following notation: for any set $T \subseteq F$, let $\overline{T}$ denote the image of $T \cap A$ in the residue field $\overline{F}$. We shall refer to $\overline{T}$ as the "pushdown" of T (along v) into $\overline{F}$.

Given a valuation v, we shall often need to refer to one or more of the objects associated with v and listed above. Therefore, instead of saying "let v be a valuation", we shall often say "let $(v, A, \mathfrak{m}, \Gamma, ...)$ be a valuation", with the understanding that we shall be using the notation above for the valuation v. For instance, if we are dealing with a given valuation ring A in a field F [3], we shall refer freely to "the valuation associated with A", and assume the reader knows that we mean the valuation $\dot{F} \twoheadrightarrow \Gamma : \dot{F}/U$, where U is the group of units of A, and $\dot{F}/U$ (a multiplicative group) is given the natural ordered group structure.

We shall also use the notion of one valuation being **finer** (or **coarser**) than another. Roughly, to "coarsen" a valuation $v : F \twoheadrightarrow \Gamma$ means composing v with an ordered group homomorphism $\Gamma \to \Gamma'$. From the viewpoint of valuation rings, a coarsening of v corresponds to a valuation ring **containing** that of v. Of course, the coarsest valuation is the **trivial valuation** (with value group zero), whose valuation ring is F. In our discussion, however, we shall never exclude the trivial valuation, unless it is otherwise stated explicitly.

Theorem 2.4.1. *Let $P \in X_F$, and let $(\nu, A, \mathfrak{m}, \Gamma, ...)$ be a valuation of F. Then the following statements are equivalent:*

i - $0 < a \leq b$ *(with respect to P)* $\Rightarrow \nu(a) \geq \nu(b)$ *in* Γ*;*

ii - *A is convex with respect to P;*

iii - *$\mathfrak{m}$ is convex with respect to P;*

iv - $1 + \mathfrak{m} \subseteq P$.

Proof. To say that A is convex means that

$$x < y < z \text{ and } x, z \in A \Rightarrow y \in A.$$

(i)⇒(ii) Upon a translation, it is sufficient to show that

$$0 < a < b \in A \Rightarrow a \in A.$$

By (i), the left hand side implies that $v(a) \geq v(b) \geq 0$, so indeed $a \in A$.

(ii)⇒(iii) Assume that $0 < a < b \in \mathfrak{m}$. Then $0 < b^{-1} < a^{-1}$. But $b^{-1} \notin A$, so by (ii), $a^{-1} \notin A$ and hence $a \in \mathfrak{m}$.

(iii)⇒(iv) Let $a \in \mathfrak{m}$. If $1 + a \notin P$, then we have $0 < 1 < -a$, and (iii) implies $1 \in \mathfrak{m}$, a contradiction.

(iv)⇒(i) Assume that $0 < a \leq b$, but $v(a) < v(b)$. Then $m := b/a \in \mathfrak{m}$, and so, by (iv), $1 - b/a > 0$, which leads to the contradiction $a > b$. □

Definition 2.4.2. *If any (and hence all) of the conditions in theorem 2.4.1 hold for ν and P, we shall say that ν is* ***compatible*** *with P (or P is compatible with ν).*

Let A be the valuation ring of v. Since v is essentially determined by A (and vice versa), it is reasonable to say that A is compatible with P if v is. Similarly, if π is the place associated with v, it is reasonable to say that π is compatible with P if v is.

[3] By saying that A is a valuation ring in F, we shall always assume implicitly that F is the quotient field of A.

If $(v, A, \mathfrak{m}, ...)$ is compatible with $P \in X_F$, then so is any coarser valuation $(v', A', \mathfrak{m}', ...)$. This follows by using either (i) or (iv) in the characterization theorem 2.4.1 for compatibility (if we use (iv), note that $A \subseteq A'$ implies that $\mathfrak{m} \supseteq \mathfrak{m}'$).

Theorem 2.4.3. *Let $P \in X_F$. Then the family $\mathcal{F}$ of valuation rings in F compatible with P forms a chain under inclusion, with a smallest member given by the convex hull of $\mathbb{Q}$ in F with respect to P, i.e, $A(P) = \{a \in F : \exists\, r \in \mathbb{Q}$ such that $-r \leq_p a \leq_p r\}$.*

In fact, $\mathcal{F}$ consists of all subrings of F containing $A(P)$.

Proof. The fact that members of $\mathcal{F}$ form a chain under inclusion is essentially a consequence of convexity and trichotomy: suppose $A, B \in \mathcal{F}$, but $A \nsubseteq B$. Fix $a \in A \setminus B$, with, say $a > 0$ (with respect to P). To show that $B \subseteq A$, consider $0 < b \in B$. By convexity of B we cannot have $0 < a \leq b$, so we must have $0 < b \leq a$, and by convexity of A, we have $b \in A$.

Now let $A(P) = \{a \in F : \exists\, r \in \mathbb{Q}$ such that $-r \leq_p a \leq_p r\}$. We have that $A(P)$ is a subring of F. To see that it is, in fact, a valuation ring of F, we must check that $b \notin A(P) \Rightarrow b^{-1} \in A(P)$. We may assume that $b \geq 0$. Since $b \notin A(P)$, we have, in particular, $b \geq 1$. Therefore, $0 < b^{-1} \leq 1$ implies that $b^{-1} \in A(P)$. By definition $A(P)$ is convex, so $A(P) \in \mathcal{F}$.

Now consider $A \in \mathcal{F}$. Since $A \supseteq \mathbb{Z}$ and is convex, it contains the convex hull of $\mathbb{Z}$, which is the same as the convex hull of $\mathbb{Q}$ (here we are implicitly using the fact that P induces the usual order on $\mathbb{Q}$: this is true because $\mathbb{Q}$ has only one ordering). Therefore $A \supseteq A(P)$. Finally, any subring of F containing a valuation ring of F must itself be a valuation ring of F. Hence $\mathcal{F}$ consists precisely of all subrings of F containing $A(P)$. □

The elements in $F \setminus A(P)$ are those whose "absolute values" with respect to P are larger than any rationals. The inverses of these elements comprise the maximal ideal of $A(P)$, so this maximal ideals consists of elements which (in the ordering P) are "infinitesimal" with respect to the rational numbers.

Definition 2.4.4. *We shall call $A(P)$ the **canonical valuation ring** of P; its associated valuation $\nu = \nu_P$ will be called the **canonical valuation** of P. Note that ν_P is the trivial valuation iff, with respect to P, every $a \in F$ is bounded "in absolute value" by some $r \in \mathbb{Q}$ i.e, iff P is an archimedean ordering.*

Proposition 2.4.5. *Let $P \in X_F$, and $(v, A, \mathfrak{m}, U, \overline{F}, ...)$ be a valuation compatible with P. Then the pushdown $\overline{P}$ (i.e the image of P under $A \to \overline{F} = A/\mathfrak{m}$) is an ordering on $\overline{F}$. For any valuation unity $u \in U$, we have $u \in P$ iff $\overline{u} \in \overline{P}$.*

Proof. By definition, is immediate that $\overline{P}$ is closed under addition and multiplication, and that $\overline{P} \cup -\overline{P} = \overline{F}$. Thus, to see that $\overline{P}$ is an ordering on $\overline{F}$, we need only check that $-1 \notin \overline{P}$. Indeed, if $-1 \in \overline{P}$, we would have $-1 = \overline{a}$ for some $a \in P \cap A$. Then $1 + a \in \mathfrak{m}$, so $-a \in 1 + \mathfrak{m} \subseteq P$ by 2.4.1(iv). This forces $a = 0$, which is absurd. This proves the first conclusion in the proposition. Since $U = A \setminus \mathfrak{m}$ and $1 + \mathfrak{m} \subseteq P$, the second assertion follows. □

2.5 Compatibility between Valuations and Preorderings

In the last section, we have defined the important notion of compatibility between a valuation v and an ordering P on a field F. In this section, we shall focus our attention on preorderings instead of orderings. The first natural question to ask is, therefore: **How does one generalize the notion of valuation-compatibility from orderings to preorderings**?

A moment of thought will reveal that we can generalize the compatibility notion to preorderings in two different ways. One is a "weak" generalization and the other is a "strong" generalization.

Both are natural, and will play important roles for our future investigations. We set forth these generalizations in the following basic definition:

Definition 2.5.1. *A valuation ν on F is said to be **compatible with** a preordering T if ν is compatible with some ordering $P \in X/T$. ν is said to be **fully compatible** with T if ν is compatible with all orderings $P \in X/T$.*

Theorem 2.5.2. *Let $(v, A, \mathfrak{m}, ...)$ be a valuation on F, and $T \subseteq F$ be a preordering. Then:*

i - v is fully compatible with T iff $1 + \mathfrak{m} \subseteq T$;

ii - v is compatible with T iff $(1 + \mathfrak{m}) \cap -T = \emptyset$ iff $\overline{T}$ is a preordering on $\overline{F}$.

Recall that $\overline{F}$ denotes the residue field of the valuation, and $\overline{T}$ denotes the image of $T \cap A$ in $\overline{F}$.

In this theorem, (i) is consequence of Artin's theorem 2.1.6 and characterization theorem 2.4.1. Indeed, for v to be compatible with all $P \in X_T$, the necessary and sufficient condition is that $1+\mathfrak{m} \subseteq \bigcap\{P : P \in X_T\}$. Since by 2.1.6 this intersection is just T, statement (i) follows. The proof of (ii) requires more work. For convenience, this proof will be preceded by a lemma:

Lemma 2.5.3 (Wedge Product Lemma)**.** *Let $(v, A, \mathfrak{m}, U, ...)$ be a valuation on F, and $\pi : A \to \overline{F}$ be the projection map. Let T be a preordering on F, and S a preordering on $\overline{F}$ such that $S \supseteq \overline{T}$. Define the "wedge product" $T \wedge S$ to be $T \cdot \pi^{-1}(\dot{S})$. Then $T \wedge S$ is a preordering on F; it is fully compatible with v, and $\overline{T \wedge S} = S$.*

Proof. The definition of $T \wedge S$ provides the fact that this set is multiplicative closed and contains $\dot{F}^2$. Furthermore, $-1 \notin T \wedge S$ for, if $-1 = t \cdot u$ where $t \in T$ and $u \in A$ with $\overline{u} \in \dot{S}$, then $t \in A$ and $-1 \in \overline{T} \cdot S = S$, a contradiction. Thus, it only remains to show that $T \wedge S$ is additively closed. Consider $a = t_1u_1+t_2u_2$, where $t_i \in \dot{T}$, and $u_i \in U$ with $\overline{u}_i \in \dot{S}$ $(i = 1, 2)$. Without loss of generality, we may assume that $t_2u_2/t_1u_1 \in A$ (since A is a valuation ring). Then $a = t_1u_1(1 + t_2u_2/t_1u_1)$, so it will be sufficient to deal with the simpler case $a' = 1 + tu$, where $t \in T \cap A$, and $u \in U$ with $\overline{u} \in \dot{S}$. In this case, we have $\overline{a}' = \overline{1} + \overline{t}\overline{u} \in \dot{S}$ so $a' \in \pi^{-1}(\dot{S})$. This shows that $T \wedge S$ is a preordering on F. Since $T \wedge S$ contains $\pi^{-1}(\dot{S}) \supseteq 1 + \mathfrak{m}$, it is fully compatible with v by 2.5.2(i).

Finally, to show that $T \wedge S$ pushes down to S, take $a = tu \in A$, where $t \in T$, and $u \in U$ with $\overline{u} \in \dot{S}$. Then $t \in A$ too and $\overline{a} = \overline{t}\overline{u} \in \overline{T} \cdot S = S$. Hence $\overline{T \wedge S} = S$. □

Remark 2.5.4. *In the proof above, we have never used the fact that T is additively closed. Thus, as long as T is a subset of F containing $\dot{F}$, such that $\dot{T} = T \setminus \{0\}$ is a group under multiplication (with $\overline{T} \subseteq S$), then the wedge product construction will be meaningful, and all conclusions n the lemma will remain valid.*

This important remark will be used consistently in the rest of this chapter, since we will have several future occasions to invoke the wedge product construction in its more general form. As an explict example, we can take $T = \dot{F}^2$: the wedge product $\dot{F}^2 \wedge S := \dot{F}^2 \cdot \pi^{-1}(S)$ obtained in 2.5.3 may be called the **"pullback"** os S. we shall denote this by $\hat{S}$; it is a preordering on F which is fully compatible with b, and pushes down to the given preordering S in $\overline{F}$.

Let T be as in 2.5.4. Then the set of orderings in F containing the wedge product $T \wedge S$ can be explicitly determined as follows:

$$X_{T\wedge S} = \{\text{orderings } P : P \supseteq T \text{ and } \overline{P} \in X_S\}.$$

For, if P lies in the right hand side, then $P \supseteq \pi^{-1}(\dot{S})$ so $T \wedge S \subseteq P \cdot P = P$. Conversely, if $P \in X_{T\wedge S}$, then P is compatible with v, so $\overline{P}$ is an ordering containing $\overline{T \wedge S} = S$. In view of

Artin's Theorem 2.1.6, the equation above leads to the following alternative characterization of the wedge product preordering:

$$T \wedge S = \bigcap \{\text{orderings } P : P \supseteq T \text{ and } \overline{P} \in X_S\}.$$

With the preparation above, we are in position to finalize the proof of 2.5.2:

Proof of the Theorem 2.5.3. We already have proved statement (i), so we just need to prove statement (ii). Assume v is compatible with the preordering T, say it is compatible with $P \in X_T$. Then by proposition 2.4.5 $-1 \notin \overline{P} \supseteq \overline{T}$. Hence $-1 \notin \overline{T}$, i.e, $(1+\mathfrak{m}) \cap (-T) = \emptyset$. Conversely, assume $-1 \notin \overline{T}$. Then $\overline{T}$ is a preordering on $\overline{F}$, and we can form the "wedge product" $T \wedge \overline{T}$ in the sense of 2.5.3. This is a preordering on F, which is fully compatible with v. Take any $P \in X_{T \wedge \overline{T}}$. Then v is compatible with P, hence (by definition) compatible with T (because $P \supseteq T$). □

In the proof above, the wedge product $T \wedge \overline{T}$ could have been replaced by the more direct expression $T \cdot (1+\mathfrak{m})$. The inclusion $T \wedge \overline{T} \supseteq T \cdot (1+\mathfrak{m})$ is immediate. For the reverse inclusion, note that if $u \in \pi^{-1}(\dot{\overline{T}})$, then $\overline{u} = \overline{t}$ for some $t \in T \cap U$. But then $m := u - t \in \mathfrak{m}$ and so $u = t(1+t^{-1}m) \in T \cdot (1+\mathfrak{m})$. Then, $T \wedge \overline{T} = T \cdot (1+\mathfrak{m})$ is the smallest preordering containing T which is fully compatible with v.

Definition 2.5.5. *In the sequel, this preordering will by denoted by T^v. X_{T^v} consists of all orderings in X_T which are compatible with v.*

As an example, consider the weak preordering $T_0 = \sum F^2$ in a formally real field F. To understand what it means for a valuation v to be compatible with T_0, we need a definition and a lemma.

Definition 2.5.6. *We say that a valuation $(v, A, \mathfrak{m}, \overline{F}, ...)$ is real if its residue field $\overline{F} = A/\mathfrak{m}$ is a formally real field. If this is the case, we shall say that the valuation ring A is residually real.*

Lemma 2.5.7. *Let $(v, A, \mathfrak{m}, \overline{F}, ...)$ be a real valuation on F with value group Γ. Let $a = a_1^2 + ... + a_n^2$ where $a_i \in \dot{F}$ for all i. Then $a \neq 0$ and $v(a) = 2\min\{v(a_i)\} \in \Gamma$. In particular, F must be formally real and $v(\sum \dot{F}^2) = 2\Gamma$.*

Proof. Say $v(a_1) = \min\{v(a_i)\} \in \Gamma$. Then $a_i/a_1 \in A$ for all i, and

$$a = a_1^2(1 + (a_2/a_1) + ... + (a_n/a_1)^2).$$

Since $\overline{F}$ is formally real, the expression in parenthesis above cannot lie in $\mathfrak{m}$. Therefore, it is a unit, and we get $a \neq 0$, $v(a) = v(a_1)^2 = 2v(a_1)$. □

Proposition 2.5.8. *A valuation v on a formally real field F is compatible with the weak preordering $T_0 = \sum F^2$ iff v is a real valuation. If this is the case, then T_0 pushes down to the weak preordering in $\overline{F}$ (i.e, $\overline{\sum F^2} = \sum \overline{F}^2$).*

Proof. Suppose v is compatible with T_0. Then $\overline{T}_0$ is a preordering in $\overline{F}$, so $\overline{F}$ is formally real, i.e, v is a real valuation. Conversely, suppose v is a real valuation. Consider an element $a \in \dot{T}_0 \cap A$, say $a = a_1^2 + ... + a_n^2$ where $a_i \in \dot{F}$. By 2.5.7, $2v(a_i) \geq v(a) \geq 0$, so $a_i \in A$ for all i. Going down to the residue field we have, therefore, $\overline{a} = \overline{a}_1^2 + ... + \overline{a}_n^2 \in \sum \overline{F}^2$. This proves that $\overline{T}_0 = \sum \overline{F}^2$. Since this is a preordering in $\overline{F}$, we conclude that v is compatible with T_0. □

Recall that, to any ordering P, we can associate its canonical valuation ring, $A(P)$ defined in 2.4.3. If we consider a preordering T instead, we can associate with two subrings of F, namely

$$A^T = \prod\{A(P) : P \in X_T\}^4 \text{ and } A_T = \bigcap\{A(P) : P \in X_T\},$$

with $A_T \subseteq A^T$. If there is only one valuation ring in $\{A(P) : P \in X_T\}$, then $A_T = A^T$. If there are at least two distinct valuation rings, then we have $A_T \not\subseteq A^T$. The larger ring, A^T, is always a valuation ring; in fact, it is the smallest valuation ring F which is fully compatible with T (of course, A^T may very well be the trivial valuation ring F: this is the case iff no nontrivial valuation is fully compatible with T). The smallest ring, A_T, is not a valuation ring in general.

For the rest of this section, we shall assume that $(v, A, \mathfrak{m}, U, \Gamma, ...)$ is a valuation on F which is compatible (but not necessarily fully compatible) with the preordering T.

Definition 2.5.9. *We shall write X_T^v for the set of orderings in X_T which are compatible with v.*

Recalling the earlier notation $T^v := T \wedge \overline{T} = T \cdot (1 + \mathfrak{m})$, we see that X_T^v is just X_{T^v}. In particular, X_T^v is a closed set of X_F, hence a compact Hausdorff space.

Our next goal will be to analyze the exact relationship between X_T^v and $X_{\overline{T}}$. This analysis will involve looking at a given ordering $Q \supseteq \overline{T}$ on $\overline{F}$, and studying the various ways of "lifting" it to orderings on F. For this purpose, the group

$$\Gamma/v(\dot{T}) \cong \dot{F}/U\dot{T}$$

turns out to play a very important role. To simplify the notation, we shall write G for this group, and write v' for the composition

$$\dot{F} \xrightarrow{v} \Gamma \longrightarrow G$$

Since $v(\dot{T}) \supseteq 2\Gamma$, G has exponent ≤ 2 and therefore may be viewed as a vector space over $\mathbb{Z}_2$, the field with two elements.

To begin our analysis, we fix a set $\{a_i\}_{i \in I}$ of elements in $\dot{F}$ such that $\{v'(a_i)\}$ form a $\mathbb{Z}_2$-basis for G. Given $P \in X_T$, we can define a $\mathbb{Z}_2$-linear functional $P^* : G \to \{\pm 1\}$ uniquely by specifying its effect on the basis $\{v'(a_i)\}$:

$$P^*(v'(a_i)) = \text{sgn}_P(a_i).$$

Thus $P^* \in G^*$, the $\mathbb{Z}_2$-dual, or the character group, of G (we note however, that P^* is not "naturally" defined, since its definition depends on the choice of the a_i's).

Now let $P \in X_T^v$. Then P gives rise to two objects:

1. a characther $P^* \in G^*$ (defined above), and
2. an ordering $\overline{P} \in X_{\overline{T}}$.

We have therefore, a mapping $g : X_T^v \to G^* \times X_{\overline{T}}$, defined by $g(P) = (P^*, \overline{P})$.

Theorem 2.5.10 (Baer-Krull)**.** *This mapping g, is a bijection.*

Proof. To prove injectivity, let $P \in X_T^v$. It suffices to show that given $x \in \dot{F}$, the sign of x with respect to P is uniquely determined if we know P^* and $\overline{P}$. In fact, write $x = a_{i_1}...a_{i_n} \cdot tu$, where

[4]This notation is supposed to mean the product of the subrings $A(P)$ inside F, not the direct product of the $A(P)$'s

$t \in \dot{T}$, $u \in U$, and $i_1, ..., i_n$ are distinct ($n \geq 0$). Since $T \subseteq P$, we have $\mathrm{sgn}_P(t) = 1$, and by 2.4.5, $\mathrm{sgn}_P(u) = \mathrm{sgn}_{\overline{P}}\overline{u}$. Therefore

$$\mathrm{sgn}_P(x) = (\mathrm{sgn}_P(u)) \prod_i \mathrm{sgn}_P(a_i) = (\mathrm{sgn}_{\overline{P}}\overline{u}) \prod_i P^*(v'(a_i)),$$

which proves what we want. To prove the surjectivity of g, let $\chi \in G^*$ and $Q \in X_{\overline{T}}$ be given. We shall try to find an ordering $P \in X_T^v$ such that $P^* = \chi$ and $\overline{P} = Q$. The idea is to construct a certain set $T' \supseteq T$ and obtain P as the wedge product $T' \wedge Q$. In order to form this wedge product, T' must be chosen to satisfy the following conditions (conform 2.5.3, 2.5.4):

a - $\dot{T}'$ is a subgroup of $\dot{F}$ containing $\dot{F}^2$;

b - $\overline{T'} \subseteq Q$.

By composing χ with v', we have a map $\dot{F} \to \{\pm 1\}$, which for simplicity, we shall again denote by χ. We now define T' by

$$T' := \{t\varepsilon a_{i_1}...a_{i_n} : t \in T,\ \varepsilon = \pm 1,\ i_1, ..., i_n \text{ are distinct } (n \geq 0) \text{ and } \chi(a_{i_1}...a_{i_n}) = \varepsilon\}. \qquad (*)$$

Since $T \supseteq F^2$, T' satisfies condition (a). To check (b), we shall prove a stronger fact, namely $T' \cap U = T \cap U$ (this will imply that $\overline{T}' = \overline{T} \subseteq Q$). Let $u \in T' \cap U$ and write $u = t\varepsilon a_{i_1}...a_{i_n}$ in the notation of (*). Then n must be zero since the a_i's are $\mathbb{Z}_2$-independent in $\dot{F}/U \cdot \dot{T}$. Therefore $\varepsilon = \chi(a_{i_1}...a_{i_n}) = 1$ and so $u = t \in T \cap U$, as desired.

To complete the proof, let P be the wedge product $T' \wedge Q$, which is a preordering in F. From (*), we have

$$P = \{tua_{i_1}...a_{i_n} : t \in T,\ u \in U,\ i_1, ..., i_n \text{ are distinct } (n \geq 0) \text{ and } \chi(a_{i_1}...a_{i_n}) = \mathrm{sgn}_Q\overline{u}\}.$$

From this equation, we see that $[\dot{F} : \dot{P}] = 2$, so P is an ordering on F. Since $P \supseteq T$ and by 2.5.3, $\overline{P} = \overline{T' \wedge Q} = Q$; therefore $P \in X_T^v$. Finally, to see that $P^* = \chi$, it suffices to check that $P^*(v'(a_i)) = \chi(a_i)$. If $\chi(a_i) = 1$, then $a_i \in T' \subseteq P$, so $P^*(v'(a_i)) = \mathrm{sgn}_P(a_i) = 1$. On the other hand, if $\chi(a_i) = -1$, then $-a_i \in T' \subseteq P$ instead and $P^*(v'(a_i)) = \mathrm{sgn}_P(a_i) = -1$. □

As a special case of the theorem, consider the weak preordering $T_0 = \sum F^2$ in a formally real field F, and let $v : \dot{F} \to \Gamma$ be any real valuation. We shall denote $X_{T_0}^v$ more simply by X_F^v: this is the set of all orderings on F which are compatible with v. We have seen before (conform 2.5.7) that $v(\dot{T}_0) = 2\Gamma$, so the group G is simply $\Gamma/2\Gamma$; also recall that $\overline{T}_0 = \sum \overline{F}^2$. Therefore 2.5.10 yields the following

Corollary 2.5.11. *There is a one-one correspondence g_0 between X_F^v and $(\Gamma/2\Gamma)^* \times X_{\overline{F}}$ (this is however, not a natural one-one correspondence).*

We can also state 2.5.11 in the following less precise form: given any ordering Q on $\overline{F}$, the various ways of "lifting" Q to an ordering F correspond one-to-one (though not in natural way) to the characters on $\Gamma/2\Gamma$. In particular, Q will lift uniquely iff Γ is 2-divisible.

2.6 T-forms under a compatible valuation

In this section, we consider a preordering $T \subseteq F$, and a valuation v on F compatible with T. The general notations associated with the valuation v, namely $(v, \Gamma, A, \mathfrak{m}, U, \overline{F}, ...)$ will remain in force. For convenience of this section, we shall view Γ as a multiplicative group.

Our main goal is to study how T-forms behave under the compatible valuation v. As in section 2.5, the quotient group $\Gamma/v(\dot{T})$ turns out to play a crucial role in this analysis. Continuing the notations used in section 2.5, we shall again denote the group $\Gamma/v(\dot{T})$ by G and write v' for the composition $\dot{F} \xrightarrow{v} \Gamma \to G$.

Note that we have a natural short exact sequence

$$1 \longrightarrow U\dot{T}/\dot{T} \longrightarrow \dot{F}/\dot{T} \xrightarrow{v'} G \longrightarrow 1 \tag{2.6}$$

Since the three groups involved are all elementary 2-groups, this is a split exact sequence. For the rest of this section, we shall choose (and fix) a splitting

$$\lambda : \dot{F}/\dot{T} \to U\dot{T}/\dot{T}$$

for the inclusion map in the sequence 2.6. Composing λ with the natural maps

$$U\dot{T}/\dot{T} \cong U/U \cap \dot{T} \to \overline{\dot{F}}/\overline{\dot{T}},$$

we get a surjective homomorphism

$$\lambda' : \dot{F}/\dot{T} \to \overline{\dot{F}}/\overline{\dot{T}}.$$

Thus we have a surjection $(\lambda', v') : \dot{F}/\dot{T} \to \overline{\dot{F}}/\overline{\dot{T}} \times G$. By abuse of notation, the composition of this map with $\dot{F} \to \dot{F}/\dot{T}$ will again be denoted by (λ', v').

We shall consider the group ring of the group G over the Witt ring $W_{\overline{T}}(\overline{F})$, denoted by $W_{\overline{T}}(\overline{F})[G]$; a typical element of this ring will be written in the form $\sum \varphi_i[g_i]$, where $\varphi_i \in W_{\overline{T}}(\overline{F})$ and $g_i \in G$.

Under the map (λ', v') defined above, an arbitrary field element $a \in \dot{F}$ gives rise to a unary $\overline{T}$-form $\langle\lambda'(a)\rangle \in W_{\overline{T}}(\overline{F})$ and a group element $v'(a) \in G$. Thus, $a \in \dot{F}$ gives rise to a group ring element $\langle\lambda'(a)\rangle[v'(a)] \in W_{\overline{T}}(\overline{F})[G]$. We shall now prove the following result, which establishes the connection between $W_T F$ and $W_{\overline{T}}(\overline{F})[G]$:

Theorem 2.6.1. *The rule*

$$a \mapsto \langle\lambda'(a)\rangle[v'(a)] \in W_{\overline{T}}(\overline{F})[G]$$

induces a well-defined surjective ring homomorphism f from $W_T F$ to $W_{\overline{T}}(\overline{F})[G]$ (this homomorphisms does depend on the choice of the splitting λ).

Proof. For $a \in \dot{F}$, let us write

$$f'(a) = \langle\lambda'(a)\rangle[v'(a)] \in W_{\overline{T}}(\overline{F})[G].$$

To see that f' gives a well-defined ring homomorphism f from $W_F(F)$ to $W_{\overline{T}}(\overline{F})[G]$, we need to check the following relations (see 2.2.12):

a - $f'(1) + f'(-1) = 0$.

b - $f'(at) = f'(a)$ for $a \in \dot{F}$ and $t \in T$.

c - $f'(ab) = f'(a)f'(b)$ for $a, b \in \dot{F}$.

d - $f'(a) + f'(b) = f'(a+b) + f'(ab(a+b))$ for $a, b, a+b \in \dot{F}$.

Among these, (a) follow by $f'(1) = [1]$ and $f'(-1) = \langle -1\rangle[1] = -[1]$; (b) follows since both $\lambda'(a)$ and $v'(a)$ depends only on a mod T. (c) follows from the fact that λ' and v' are both homomorphisms. Now, we only need to check (d).

In view of (c), it suffices to check (d) in the special case $b = 1$, i.e, to check that

$$f'(1) + f'(a) = f'(1 + a)(f'(1) + f'(a)) \text{ if } a \in F,\ a \neq 0, -1. \tag{2.7}$$

For this purpose, we may assume that a lies in the valuation ring A of v (for otherwise, replace a by $1/a$ which is also $\neq 0, -1$). There are three possible cases:

Case 1 - $a \in \mathfrak{m}$. In this case $1 + a$ is a valuation unit. Thus

$$f'(1 + a) = \langle \lambda'(1 + a)\rangle[v'(1 + a)] = \langle 1\rangle[1] = [1],$$

so 2.7 follows.

Case 2 - $a \in U$ but $1 + a \in \mathfrak{m}$. In this case, $\lambda'(a) = -1$ and $v'(a) = 1$. Thus $f'(1) + f'(a) = [1] + \langle -1\rangle[1] = 0$, so 2.7 follows again.

Case 3 - $a \in U$ but $1 + a \in U$. In this case,

$$\begin{aligned} f'(1) + f'(a) &= [1] + \langle \lambda'(a)\rangle[v'(a)] = [1] + \langle \overline{a}\rangle[1] = \langle 1, \overline{a}\rangle[1], \\ f'(1 + a) &= \langle \lambda'(1 + a)\rangle[v'(1 + a)] = \langle \overline{1 + a}\rangle[1], \end{aligned}$$

so

$$\begin{aligned} f'(1 + a)(f'(1) + f'(a)) &= \langle \overline{1 + a}\rangle[1] \cdot \langle 1, \overline{a}\rangle[1] = \langle \overline{1 + a}\rangle \cdot \langle 1, \overline{a}\rangle[1] \\ &= \langle 1, \overline{1, a}\rangle[1] = f'(1) + f'(a) \end{aligned}$$

again, checking 2.7.

We have now proved that the rule $f'(a) = \langle \lambda'(a)\rangle[v'(a)]$ induces a well-defined ring homomorphism $f : W_T(F) \to W_{\overline{T}}(\overline{F})[G]$. Since $(\lambda', v') : \dot{F} \to \dot{\overline{F}}/\dot{\overline{T}} \times G$ is surjective, we conclude that f is also surjective. □

Take any T-form φ, and consider any diagonalization of it. We can "sort out" the diagonal entries into different "blocks", putting two entries $\langle a\rangle$ and $\langle b\rangle$ in the same block if and only if $v'(a) = v'(b) \in G$. Thus, we have a representation

$$\varphi \cong \perp_{g \in G} \langle a_{g1}, ..., a_{gn(g)}\rangle \tag{2.8}$$

where $v'(a_{g,i}) = g \in G$ for every i. For each $g \in G$, consider the $\overline{T}$-form $\langle \lambda'(a_{g1}), ..., \lambda'(a_{gn(g)})\rangle$. This is called the **$g$-residue form** of φ (with respect to the given diagonalization). By definition, we have

$$f(\varphi) = \sum_{g \in G} \langle \lambda'(a_{g1}), ..., \lambda'(a_{gn(g)})\rangle[g].$$

Therefore, by theorem 2.6.1, for each $g \in G$ the Witt class of the g-residue form $\langle \lambda'(a_{g1}), ..., \lambda'(a_{gn(g)})\rangle$ in $W_{\overline{T}}(\overline{F})$ is uniquely determined, i.e, it is independent of the particular diagonalization of φ which we have chosen (though still depending on the choice of the splitting λ). We shall write

$$\partial_g(\varphi) = \langle \lambda'(a_{g1}), ..., \lambda'(a_{gn(g)})\rangle \in W_{\overline{T}}(\overline{F})$$

so

$$f(\varphi) = \sum_{g \in G} \partial_g(\varphi)[g] \in W_{\overline{T}}(\overline{F})[G].$$

Thus, the group homomorphism $\partial_g : W_T F \to W_{\overline{T}}(\overline{F})$ $(g \in G)$ may be viewed as the "coordinate projections" of the ring homomorphism $f : W_T F \to W_{\overline{T}}(\overline{F})[G]$.

The case $g = 1 \in G$ is particular noteworthy. In this case, since $v'(a_{1,i}) = 1$, we can write $a_{1,i} = u_i t_i$ where $u_i \in U$ and $t_i \in \dot{T}$ (keep in mind that $G = \Gamma/v(\dot{T})$). Thus, the "1-residue form"

$$\langle \lambda'(a_{11}), ..., \lambda'(a_{1n(1)}) \rangle \cong_T \langle \overline{u}_1, ..., \overline{u}_{n(1)} \rangle$$

does not even depend on the choice of λ. This will be called the **principal residue form** of φ, with respect to the diagonalization. Its Witt class $\partial_1(\varphi) \in W_{\overline{T}}(\overline{F})$ depends only on the Witt class of $\varphi \in W_T F$ and not on the choice of the splitting λ.

We shall now prove two theorems relating the T-isotropy of a T-form φ to the $\overline{T}$-isotropy of its various residue forms.

Theorem 2.6.2. *Let v be a valuation compatible with T. If a T-form φ diagonal as in 2.8 is T-isotropic, then there exists an $h \in G$ such that the h-residue form $\langle \lambda'(a_{h,1}, ..., \lambda'(a_{h,n(h)} \rangle$ is $\overline{T}$-isotropic.*

Proof. If φ is T-isotropic, then its T-anisotropic part φ' has a smaller dimension. Comparing residue forms of φ and φ', we have $\partial_g(\varphi) = \partial_g(\varphi') \in W_{\overline{T}}(\overline{F})$ for every $g \in G$, from which the conclusion follows. □

Theorem 2.6.3. *Assume v is fully compatible with T. Then a T-form φ as in 2.8 is T-anisotropic iff all its residue forms (with respect to the diagonalization 2.8) are $\overline{T}$-anisotropic.*

Proof. ($\Rightarrow$) Assume v is fully compatible with T, and suppose some residue form, say $\perp_i \langle \lambda'(a_{hi} \rangle$ is $\overline{T}$-isotropic. Since $v(a_{hi}/a_{h1}) \in v(\dot{T})$, we can write $a_{hi}/a_{h1} = t_i^{-1} u_i$ where $t_i \in \dot{T}$ and $u_i \in U$. Then $\lambda'(a_{hi})/\lambda'(a_{h1}) = \overline{u}_i \dot{\overline{T}}$ and so (by assumption), $\langle \overline{u}_1, ..., \overline{u}_n \rangle$ is $\overline{T}$-isotropic. Write down an equation, say

$$0 = \sum_{i=1}^{r} \overline{u}_i \overline{s}_i \; (2 \leq r \leq n(h)),$$

where $s_i \in T \cap U$, and let $m = \sum_{i=1}^{r} u_i s_i \in \mathfrak{m}$. Plugging in $u_i = t_i a_{hi}/a_{h1}$, this becomes

$$0 = (s_1 t_1 - m) - \sum_{i=2}^{r} s_i t_i a_{hi}/a_{h1}.$$

Since v is fully compatible with T, and $t_1 = u_1 \in T \cap U$, we have $s_1 t_1 - m \in T \cdot (1 + \mathfrak{m}) \subseteq T$. Multiplying the equation above by a_{hi}, we see that $\langle a_{h1}, ..., a_{hr} \rangle$ is T-isotropic. In particular, so is φ.

($\Leftarrow$) Is just the preceding theorem which holds already under the weaker assumption that v is compatible with T. □

Corollary 2.6.4. *The ring homomorphism $f : W_T F \to W_{\overline{T}}(\overline{F})[G]$ defined in Theorem 2.6.1 is an isomorphism iff v is fully compatible with T.*

Proof. ($\Rightarrow$) Assume that f is an isomorphism, and consider $a = 1 + m$, where $m \in \mathfrak{m}$. Then $\varphi := \langle 1, -a \rangle_T$ has principal residue form $\langle 1, -1 \rangle_{\overline{T}}$ over $\overline{F}$ (and no other residue forms). Since f is an isomorphism, it follows that φ is T-hyperbolic, i.e, $a \in T$. Thus, $1 + \mathfrak{m} \subseteq T$, so v is fully compatible with T.

($\Leftarrow$) Follow by theorem above. □

2.7 Fans I

In this section, we shall introduce and study a very important class of preorderings called *fans*:

Definition 2.7.1. *A preordering $T \subseteq F$ is called a fan if it satisfies the following property: for any set $S \supseteq T$ such that $-1 \notin S$, if $\dot{S} = S \setminus \{0\}$ is a subgroup of index 2 in $\dot{F}$, then S is an ordering (i.e, S is automatically closed under addition).*

Roughly speaking, T is a fan iff X_T is as big a set as it could possibly be. Consider, for instance, the case when T has finite index, say $[\dot{F} : \dot{T}] = 2^n$. There are exactly 2^{n-1} sets $S \supseteq T$ with the property that $-1 \notin S$ and $\dot{S}$ is a subgroup of index 2 in $\dot{F}$. For T to be a fan, each such S must be an ordering. Thus, we have $|X_T| \leq 2^{n-1}$ in general, with equality iff T is a fan. Of course, from definition, if T is a fan, then so is every preordering containing T.

Proposition 2.7.2. *Let T be a preordering with $[\dot{F} : \dot{T}] \leq 4$. Then T is a fan (we shall say that such a T is a trivial fan).*

Proof. If $[\dot{F} : \dot{T}] = 2$, then T is an ordering, so is a fan. If $[\dot{F} : \dot{T}] = 4$, there are at least two (and therefore exactly two) orderings in X_T, so again T is a fan. □

The first nontrivial case to consider is when the index $[\dot{F} : \dot{T}] = 8$. In this case, we have $3 \leq |X_T| \leq 4$. Fix $P_1, P_2, P_3 \in X_T$, and let χ_i be the character on $\dot{F}/\dot{T}$ (into $\{\pm 1\}$) associated to the ordering P_i. Then χ_1, χ_2, χ_3 must be $\mathbb{Z}_2$-linearly independent in the $\mathbb{Z}_2$-dual $(\dot{F}/\dot{T})^*$ so they form a basis in this dual. There is exaclty one more character which takes $-\dot{T}$ to -1, namely, the product χ_1, χ_2, χ_3. In general, this may not be the character of an ordering. It will be the character of an ordering iff there is a fourth ordering $P_4 \in X_T$ iff T is a fan. If this is the case, we shall say that T is a "4-element fan" (the terminology refers to the fact that the set of orderings X_T consists of 4 elements). In this case, if χ_4 denotes the character of P_4, we have $\chi_1\chi_2\chi_3\chi_4 = 1$.

We shall now construct an explicit example of a 4-element fan. In the following, for a field K, $K((x))$ denote the power serie field in one variable over K. If K is formally real pythagorean field, then so is $K((x))$.

Example 2.7.3. *Let $F = \mathbb{R}((x))((y))$ and $T = F^2$. Since F is formally real and pythagorean, T is just the weak preordering on F. $\dot{F}/\dot{T}$ has a $\mathbb{Z}_2$-basis $\{-1, x, y\}$; moreover, $X_T = X_F$ consists of four orderings $\{P_1, P_2, P_3, P_4\}$, under which x, y have the four different combination of signs: $(+.+), (+,-), (-,+), (-,)$. Therefore, T is a 4-element fan. Writting again χ_i for the character of P_i on $\dot{F}/\dot{T}$, we have*

	P_1	P_2	P_3	P_4	$\chi_1\chi_2\chi_3\chi_4$
x	$+$	$+$	$-$	$-$	1
y	$+$	$-$	$+$	$-$	1
-1	$-$	$-$	$-$	$-$	1

Theorem 2.7.4. *For any preordering $T \subseteq F$, the following statements are equivalent:*

1 - *T is a fan;*

2 - *for any set $S \supseteq T$, if $-1 \notin S$ and $\dot{S}$ is a subgroup of $\dot{F}$, then S is a preordering;*

3 - *for any $b \in \dot{F} \setminus (-\dot{T})$, $T + Tb = T \cup T \cdot b$ (or, in the terminology of 2.1.8 every $b \notin -T$ is T-rigid);*

3′ - *for any $a, b \in \dot{F}$ such that $ab \notin -\dot{T}$, $T \cdot a + T \cdot b = T \cdot a \cup T \cdot b$;*

4 - *there exists an ordering $P \in X_T$ such that, for any $b \in \dot{P}$, $T + T \cdot b = T \cup T \cdot b$ (i.e, P consists of T-rigid elements);*

4′ - *there exist an ordering $P \in X_T$ such that, for any $a, b \in \dot{P}$, $T \cdot a + T \cdot b = T \cdot a \cup T \cdot b$;*

5 - *every preordering $T' \supseteq T$ of index 8 in F is a (4-element) fan.*

Proof. The equivalences (3) $\Leftrightarrow$ (3′) and (4) $\Leftrightarrow$ (4′) follow by scaling, so in the following we shall identify (3) with (3′) and (4) with (4′).

(1) $\Leftrightarrow$ (2) Let S be as in (2).By elementary group theory, we know that $\dot{S} = \bigcap V$ where V ranges over all subgroup of index 2 in $\dot{F}$ containing S but not containing -1. By the definition of a fan, each such V is additively closed. Hence so is $\dot{S}$ and so S is a preordering.

(2) $\Leftrightarrow$ (3) Consider $(T \cup T \cdot b) \setminus \{0\}$. This is a multiplicative subgroup of $\dot{F}$ containing $\dot{T}$ but not containing -1. By (2), $T \cup T \cdot b$ is a preordering. Therefore $T + T \cdot b \subseteq T \cup T \cdot b$. Since the reverse inclusion is immediate b is T-rigid.

(3) $\Leftrightarrow$ (4) Follows by the fact that $\dot{P}$ is disjoint from $-T$.

(4′) $\Leftrightarrow$ (1) Let $S \supseteq T$ be a set such that $-1 \notin S$ and $\dot{S}$ is a subgroup of index 2 in $\dot{F}$. We need to show that S is an ordering. Let P be as in (4′) and consider $S' := S \cap P$. Let $a, b \in \dot{S}'$. Using the hypothesis on P, we have $a + b \in T \cdot a \cup T \cdot b \subseteq P \cap S = S'$, so S' is a preordering, and the index of S' is 2 or 4. If S' has index 2, then $S = P$ and we are done, so we may assume that S' has index 4. There are three multiplicative groups containing $\dot{S}'$ of index 2 in $\dot{F}$, namely, $\dot{S}$, $\dot{P}$, and another one containing -1. But there are two orderings containing S', so S must be one of them (and P another).

(1) $\Leftrightarrow$ (5) Immediate from the fact that if T is a fan, then so is every preordering containing T.

(5) $\Leftrightarrow$ (3) For $b \in \dot{F} \setminus (-\dot{T})$, it is sufficient to show that $1 + b \in T \cup T \cdot b$. Assume this is false. Then $1 + b, b^{-1} + 1$ as well as b are not in T. By Artin's Theorem 2.1.6, there exist orderings $P_1, P_2, P_3 \in X_T$ which exclude these elements, respectively. Let $T' = P_1 \cap P_2 \cap P_3$. Then $b \notin -T'$ and $1 + b \notin T' \cup T' \cdot b$. Thus, T' is not a fan (by (1) $\Rightarrow$ (3), which is already proved). By 2.7.2 T' cannot have index ≤ 4, so necessarily $[\dot{F} : \dot{T}'] = 8$. This contradicts (5). □

We shall now record a few consequences of the theorem above:

Corollary 2.7.5. *Let $F \subseteq K$ be two fields. If T' is a fan in K, then $T = T' \cap F$ is a fan in F.*

Proof. Let $S \supseteq T$ be as in 2.7.4(2). Then $S \cdot T' \cap F = S$, so $-1 \notin S \cdot T'$. Since $S \cdot T' \setminus \{0\} \supseteq T'$ is a multiplicative group, $S \cdot T'$ is a preordering in K. Therefore S is a preordering in F, and so T is a fan in F. □

Another proof of 2.7.5 may also be obtained by checking condition (3) or (3′) in 2.7.4. Note that these conditions have a natural quadratic form-theoretic interpretation. In fact, let φ be the binary T-form $\langle a, b\rangle$; then $(T \cdot a + T \cdot b) \setminus \{0\}$ is just $D_T(\varphi)$, the set of values represented by φ over T. Thus, in form-theoretic terms, (3′) says that for any T-anisotropic binary form $\varphi = \langle a, b\rangle_T$, φ represents only the obvious $\dot{T}$-cosets $\dot{T} \cdot a$, $\dot{T} \cdot b$ and nothing more. By repeated application of this property, we obtain the following self-strenghened version of 2.7.4(3′):

Corollary 2.7.6. *Let T be a fan and φ be the T-form $\langle a_1, ..., a_n\rangle$ with the property that $a_i a_j \notin -T$ for all $i \neq j$. Then $D_T(\varphi) = \bigcup_i \dot{T} \cdot a_i$.*

Expressed informally, the condition on φ in 2.7.6 says that there is no T-hyperbolic plane "in the diagonalization" $\langle a_1, ..., a_n\rangle$ of φ. If φ is T-anisotropic, this condition on φ is surely satisfied.

Therefore, 2.7.6 gives the complete computation of values for all T-anisotropic forms over a fan T (of course, we need not worry about T-isotropic forms since they are universal).

Since the condition on φ in 2.7.6 is a necessary condition for φ to be T-anisotropic (for any preordering T), one may naturally ask: is it also a sufficient condition? The answer is provided in 2.7.7 below: it is iff T is a fan!

Corollary 2.7.7. *For any preordering T, the following are equivalent:*

1. *T is a fan;*
2. *for any T-form $\varphi = \langle a_1, ..., a_n\rangle$, φ is T-isotropic iff there exist $i \neq j$ such that $a_i a_j \in -T$;*
3. *if $\langle a_1, ..., a_n\rangle \cong_T \langle b_1, ..., b_n\rangle$ are T-anisotropic, then there is a permutation α of $\{1, ..., n\}$ such that $\dot{T} \cdot a_i = \dot{T} \cdot b_{\alpha(i)}$ for all i.*

Proof. (1)⇒(2) We only need to prove (⇒) part in (2). Assume φ is T-isotropic, but $a_i a_j \neq T$ for all $i \neq j$. Then, by 2.7.6, $D_T(\varphi) = \cup_i \dot{T} \cdot a_i$. But since φ is T-isotropic, we have $\pm 1 \in D_T(\varphi)$. Thus, we can write $1 = ta_i$ and $-1 = t'a_j$ for some $t, t' \in \dot{T}$, and some i, j. But then $a_i \in \dot{T}$ and $a_j \in -\dot{T}$, these imply that $i \neq j$ and $a_i a_j \in \dot{T}$, a contradiction.

(2)⇒(1) To show that T is a fan, we shall check that every element $b \notin -T$ is T-rigid (conform 2.7.4(3)). Let $\neq c \in T + T \cdot b$; then $\langle 1, b, -c\rangle$ is T-isotropic. By (2), we have either $-c \in -\dot{T}$ or $-bc \in -\dot{T}$, so $c \in \dot{T} \cup \dot{T} \cdot b$. This shows that b is T-rigid.

(1)⇒(3) Let b, c be as above. Then $\langle 1, b\rangle \cong_T \langle c, bc\rangle$ are T-anisotropic forms, and by (3), $c \in \dot{T} \cup \dot{T} \cdot b$.

(3)⇒(1) From $\langle a_1, ..., a_n\rangle \cong_T \langle b_1, ..., b_n\rangle$, we have $b_1 \in D_T(a_1, ..., a_n)$. Since $\langle a_1, ..., a_n\rangle$ is T-anisotropic and T is a fan,

$$D_T(a_1, ..., a_n) = \cup_i \dot{T} \cdot a_i,$$

as we have already observed. Thus, we may assume (after reindexing) that $b_i \in \dot{T} \cdot a_i$. Now cancel and induct. □

So far the only example of fans we have given are the "trivial fans" and "4-element fans". After the following discussion, we shall be able to construct (using valuations) many example of fans of index ≥ 16. In fact, by a result of Bröcker, we shall be able to explain precisely, in valuation-theoretic terms, how all fans can arise. We first make some basic observations relating valuations and fans.

Proposition 2.7.8. *Let $(v, A, \mathfrak{m}, U, ...)$ be a valuation on F, and $T \subseteq F$ be a preordering.*

a - If v is compatible with T, then T is a fan imply $\overline{T}$ is a fan.

b - If v is fully compatible with T, then T is a fan iff $\overline{T}$ is a fan.

Proof.

a - Let $b \in U$ be such that $\bar{b} \notin -\overline{T}$ (in particular, $b \notin T$). Let $t_1, t_2 \in T \cap A$, and consider $\bar{t}_1 + \bar{t}_2\bar{b}$. Since T is a fan, $t_1 + t_2 b$ has the form t_3 or $t_4 b$, where $t_3, t_4 \in T$. Going down to the residue field, we have $\bar{t}_1 + \bar{t}_2\bar{b} \in \overline{T} \cup \overline{T} \cdot \bar{b}$. This shows that every $\bar{b} \notin -\overline{T}$ is $\overline{T}$-rigid, so by 2.7.4(3) $\overline{T}$ is a fan.

b - (⇒) Is already proven in item (a).

(⇐) Assume that v is fully compatible with T (so $1 + \mathfrak{m} \subseteq T$), and that $\overline{T}$ is a fan. Let $W \supseteq T$ be a set in F such that $-1 \notin W$ and $\dot{W}$ is a subgroup (of index 2) in $\dot{F}$. We claim that

$-1 \notin \overline{W}$. For, if $-1 = \overline{w}$ for some $w \in W \cap A$, then $-1 = w + m$ for some $m \in \mathfrak{m}$ and so $-w = 1 + m \in 1 + \mathfrak{m} \subseteq T \subseteq W$, which is not the case. Since $\overline{T}$ is a fan, and $\dot{\overline{W}}$ is a subgroup (of index 2) in $\dot{\overline{F}}$, $\overline{W}$ is a preordering (ordering) of $\overline{F}$. In view of what we said in 2.5.4, we can form the wedge product $W \wedge \overline{W}$, which is a preordering in F. But

$$W \wedge \overline{W} = W \cdot (1 + \mathfrak{m}) \subseteq W \cdot T \subseteq W,$$

so $W = W \wedge \overline{W}$ is a preordering (ordering) in F as desired.

□

Corollary 2.7.9. *Let v be a valuation on F and $T_0 \subseteq F$ be such that $\dot{T}_0$ is a subgroup of $\dot{F}$ containing $\dot{F}^2$. Let S be a preordering in $\overline{F}$ containig $\overline{T}_0$. The S is a fan (in $\overline{F}$) imply $T_0 \wedge S$ is a fan (in F). In particular, the "pullback" $\hat{S} := F^2 \wedge S$ of a fan $S \subseteq \overline{F}$ is always a fan in F.*

Proof. We have observed in 2.5.4 that the wedge product $T_0 \wedge S$ is fully compatible with v, with $\overline{T \wedge S} = S$. Hence, the proposition 2.7.8 applies. The "pullback" case follows by taking $T_0 = F^2$. □

The corollary above enable us to construct a lot of fans by exploiting (real) valuations. For instance, fix a real valuation $(v, A, \mathfrak{m}, ...)$ on a field F, and take any trivial fan S on $\overline{F}$. Then the pullback $\hat{S} = F^2 \wedge S$ is a fan, and therefore any preordering $T \supseteq \hat{S}$ is also a fan. Quite remarkably, this turns out to be the way to account for all fans, namely, any fan T in fact arises in this way! This is a consequence of the following beautiful result:

Theorem 2.7.10 (Bröcker's Trivialization of Fans)**.** *Let T be a fan on F. Then there exists a valuation v on F fully compatible with T with respect to which the pushdown $\overline{T}$ is a trivial fan.*

Note that since v is fully compatible with T, the pullback $\hat{\overline{T}} = F^2 \wedge \overline{T}$ lies in $T \wedge \overline{T} = T \cdot (1 + \mathfrak{m}) = T$ (conform 2.5.5), so T contains the pullback of the trivial fan $\overline{T}$, we have stated in the paragraph preceding the theorem.

Since any preordering containing a fan is also a fan, it is particularly important to understand the structure of "minimal" fans: a fan T_0 is called minimal if no smaller preordering $T_1 \subsetneq T_0$ is a fan. By what we have said above, we know that any minimal fan in F is the pullback of a trivial fan (with respect to some valuation on F).

Unfortunately, we do not prove theorem 2.7.10. We should need to develop much more techinicalities and go away of our main goal, that is the abstract theories of quadratic forms.

2.8 The Representation Problem I

Recall that, for any preordering $T \subseteq F$, we have a (injective) ring homomorphism

$$c : c_T : W_T F \to C(X_T, \mathbb{Z}),$$

where $W_T F$ is the Witt ring over T, and $C(X_T, \mathbb{Z})$ is the ring of continuous functions from X_T to $\mathbb{Z}$ (the latter given the discrete topology). For any T-form φ, we have, by definition, $c(\varphi) = \hat{\varphi}$, where $\hat{\varphi}(P) = \mathrm{sgn}_P(\varphi)$ for any $P \in X_T$.

A very natural question to ask in this context is: *what is the image of c? In other words, what is the criterion for a continuous function $X_T \to \mathbb{Z}$ to be "represented" by a T-form?* We shall refer to this as the "Representation Problem" for such continuous functions. In this section, a full

solution of this Representation Problem will be presented. Our strategy will be as follows: we shall first solve the problem in the case when T is a fan. Then in the sequel, we shall solve the problem in general by making a reduction to fans.

First let us set up some notational and terminological conventions. To differentiate between forms and functions, we shall denote T-forms by Greek letters $\alpha, \beta, \varphi, \psi, ...$ and functions from X_T to $\mathbb{Z}$ by Latin letters $f, g, f', g', ...$ If $T' \supseteq T$ is another preordering, then $X_{T'} \subseteq X_T$, so any function $f : X_T \to \mathbb{Z}$ induces a function $X_{T'} \to \mathbb{Z}$ by restriction. By abuse of notation, we shall denote the latter function again by f. A function $f : X_T \to \mathbb{Z}$ is said to be **represented** over T (by a form) if $f = \hat{\varphi}$ for some T-form φ. If f is represented over T, then it will also be represented over any bigger preordering $T' \supseteq T$.

Two necessary conditions for a function $f : X_T \to \mathbb{Z}$ to be represented over T are as follows:

a - f must be continuous;

b - f is a function of constant parity, i.e, its values must be either all even or all odd. This is because if $f = \hat{\varphi}$ for a T-form φ, then

$$f(P) = \hat{\varphi}(P) = \mathrm{sgn}_P(\varphi) \equiv \dim \varphi \,(\mathrm{mod}\ 2).$$

Let $f : X_T \to \mathbb{Z}$ be a function satisfying (a) and (b). If f is an even-valued function, then $f \in 2C(X_T, \mathbb{Z})$; if f is an odd-valued function, then $f \in 1 + 2C(X_T, \mathbb{Z})$. Therefore, the set of functions f satisfying (a),(b) coincides with the subring $\mathbb{Z} + 2C(X_T, \mathbb{Z})$ of $C(X_T, \mathbb{Z})$, and we have

$$\mathrm{Im}(c) \subseteq \mathbb{Z} + 2C(X_T, \mathbb{Z}).$$

In general, this is not an equality.

We shall now introduce some of the key techniques for studying the Representation Problem. First we make a crucial definition:

Definition 2.8.1. *Let T be a given preordering in F, and let $\mathcal{F}$ be a family of preorderings in F containing T. We shall say that $\mathcal{F}$ is a Hasse-Minkowski family (or more briefly, an HM-family) for T if, for any T-form φ, φ is T-isotropic iff φ is S-isotropic for all $S \in \mathcal{F}$.*

Given a preordering T, it is an important task to try to identify good families $\mathcal{F}$ which are HM-families for T. If we can find an HM-family $\mathcal{F}$ such that for every $S \in \mathcal{F}$, we have a criterion for deciding the S-isotropy of S-forms, then we will also get a criterion for deciding the T-isotropy of T-forms. This situation reminds us of the usual Hasse-Minkowski Principle for quadratic forms over number fields, hence the present terminology.

The importance of definition 2.8.1 for the study of the Representation Problem lies in the fact that, once we identify an HM-family $\mathcal{F}$ for a preordering T, we can make a reduction of the Representation Problem from T to the preorderings S in $\mathcal{F}$. More precisely, we shall now prove the following result of Becker and Bröcker:

Proposition 2.8.2. *Let $\mathcal{F}$ be an HM-family for a preordering $T \subseteq F$, and let $f \in \mathbb{Z} + 2C(X_T, \mathbb{Z})$. Assume that f is represented over every $S \in \mathcal{F}$. Then f is also represented over T.*

First, let us rewrite Theorem 1.6.4 in the reduced theory context:

Theorem 2.8.3. *For any continuous function $f \in C(X_T, \mathbb{Z})$, there exists a natural number n such that $2^n f \in c_T(I_T^n F)$. In particular, coker(c_T) is a 2-primary torsion group.*

Now, we proceed with the proof.

Proof of Theorem 2.8.2. By 2.8.3, there exists a natural number k such that $2^k f$ is represented over T. Using induction, it is enough to deal with the case $k = 1$. Say $2f = \hat{\varphi}$, where $\varphi = \langle a_1, ..., a_m \rangle_T$. We may assume φ is T-anisotropic and of course, m is an even integer; say $m = 2n$. To prove that f is represented over T, we make the following claim:

$$\text{There exists a } T\text{-form } \varphi'' \text{ such that } \varphi \cong_T \langle a_1, a_1 \rangle \perp \varphi''. \tag{2.9}$$

If we can verify this, then $2(f - \widehat{\langle a_1 \rangle}) = \widehat{\varphi''}$. Repeating this process, we will eventually get $2(f - \widehat{\langle a_1, a_2, ... \rangle}) = 0$, so $f = \widehat{\langle a_1, a_2, ... \rangle} \in \mathrm{Im}(C_T)$ as desired.

To prove claim 2.9, we fix one preordering $S \in \mathcal{F}$. By the hypothesis (and the injectivity of c_S), we have $\varphi = 2\alpha_S \in W_S F$ for some S-anisotropic form α_S. Note that $2\alpha_S$ remains S-anisotropic, but φ might become isotropic over S. Write down a Witt decomposition (in the context of S-forms)

$$\varphi \cong_S 2\alpha_S \perp i_S\langle 1, -1 \rangle \, (i_s \geq 0) \tag{2.10}$$

We shall prove that $i_S \in 2\mathbb{Z}$. Once this is proved (for all $S \in \mathcal{F}$), then 2.9 can be deduced as follows. From 2.10, we have $\varphi \cong_S 2\beta_S$ for some S-form β_S. Writting $\varphi \cong_T \langle a_1 \rangle \perp \varphi'$, we have $a_1 \in D_S(2\beta_S) = D_S(\beta_S)$, so $\beta_S \cong_S \langle a_1 \rangle \perp \gamma_S$ for some γ_S. But then $\langle a_1 \rangle \perp \varphi' \cong_S \langle a_1, a_1 \rangle \perp \gamma_S \perp \gamma_S$, so, after cancellation, we get $a_1 \in D_S(\varphi')$. This says that $\varphi' \perp \langle -a_1 \rangle$ is S-isotropic, for every $S \in \mathcal{F}$, so $\varphi' \perp \langle -a_1 \rangle$ is, in fact, T-isotropic. Therefore $\varphi' \cong_T \langle a_1 \rangle \perp \varphi''$ for some T-form φ'', and 2.9 follows.

Our remaining task is, therefore, to prove that for any given $S \in \mathcal{F}$, the Witt index i_S in 2.10 is even. For this purpose, fix an ordering $P \in X_S$. Among the diagonal entries in $\varphi \cong_T \langle a_1, ..., a_{2n} \rangle$, suppose r elements are in P, and t elements are in $-P$. Then $2n = r + t$ and $\mathrm{sgn}_P(\varphi) = r - t$. Upon subtraction, we get

$$2t = 2n - \mathrm{sgn}_P(\varphi) = 2n - 2f(P),$$

so $t = n - f(P)$. On the other hand, computing the P-signature of the discriminant of φ from 2.10, we get

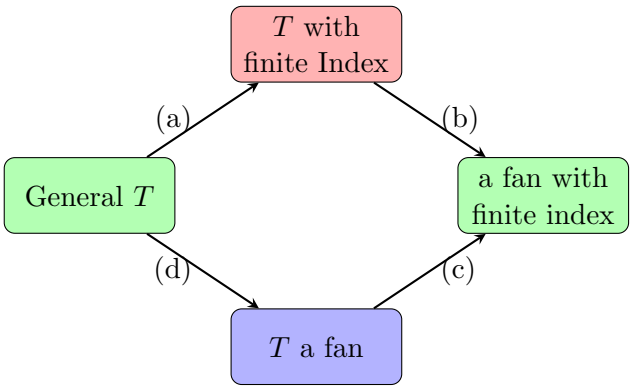
$$(-1)^{i_S} = \mathrm{sgn}_P(\det \varphi) = (-1)^t = (-1)^{n - f(P)}.$$

Since $f(P)$ has constant parity (for $P \in X_S$ and $S \in \mathcal{F}$), this implies that i_S also has constant parity (for $S \in \mathcal{F}$). If all i_S's were odd, then 2.10 would say that φ is S-isotropic, for all $S \in \mathcal{F}$, and hence φ is T-isotropic, a contradiction. Therefore all i_S's must be even, as we had hoped to prove. □

Of course, how successfully we can apply the proposition above to solve the Representation Problem over T would depend on what kind of HM-families $\mathcal{F}$ we can find for T. The kind of HM-family used by Becker and Bröcker is described in the following theorem:

Theorem 2.8.4 (Becker and Bröcker)**.** *Let $T \subseteq \dot{F}$ be any preordering, and let $\mathcal{F}$ be the family of all preorderings containing T which have finite index in F. Then $\mathcal{F}$ is an HM-family for T.*

If we combine this result with 2.8.2, we see that, in order to solve the Representation Problem, it is sufficient to do it in the case when the preordering has finite index in F. For preorderings $T \subseteq F$ of finite index in F, Becker and Bröcker made a further reduction of the problem to the case when T is a fan (of finite index), in which case the problem had been solved earlier by R. Brown. To illustrate the situation, consider the following "flow chart" of reduction steps:



The upper route, with reduction (a) followed by reduction (b), is the route followed by Becker and Bröcker. This is, however, a difficult route: (a) would depend on 2.8.4, which is a rather deep result, and (b) is also a very complicated reduction. In these notes, we shall offer an alternative approach by trying to follow the lower route (marked (c) and (a)) in the "commutative diagram" above. This lower route is made possibly by the work of M. Marshall, who gave a very ingenuous proof for the reduction (d). Of course (d) would subsume (b), so if we assume Marshall's work, the upper route depend on (a), while the lower route would depend on (c) which is a special case of (a). In order to get (a), we would need to prove 2.8.4, but, in order to get (c), it will be enough to prove 2.8.4 in the special case when T is a fan (of course, these statements all assume 2.8.2). The latter turns out to be easier, and because this, we use the lower route "(c) and (d)" for solving the Representation Problem without to prove 2.8.4 in full.

Lemma 2.8.5 (Special case of 2.8.4)**.** *Let T be a fan, and let $\mathcal{F}$ be the family of preorderings $S \supseteq T$ which have finite index in F. Then $\mathcal{F}$ is an HM-family for T.*

Proof. Let $\varphi = \langle a_1, ..., a_n \rangle$ be a T-form, and assume φ is T-anisotropic. Then for all $i \neq j$, we have $a_i a_j \notin -T$. By Artin's Theorem 2.1.6, there exists an ordering $P_{ij} \in X_T$ such that $a_i a_j \in P_{ij}$. Now let $S = \bigcap_{i<j} P_{ij}$. Then whenever $i \neq j$, we have $a_i a_j \notin -S$. But S is also a fan since T is, so by 2.7.7, φ is S-anisotropic. Since $S \in \mathcal{F}$, this completes the proof of the lemma. □

Now we shall give the solution of the Representation Problem in the special case of fans of finite index. This steps is, of course, necessary no matter which route we want to follow. Note that, once we solve the Representation Problem for fans of finite index, we will have solved the Representation Problem for all fans, in view of 2.8.5 and 2.8.2.

Theorem 2.8.6 (R. Brown)**.** *Let T be a fan of finite index in F, and let $f \in C(X_T, \mathbb{Z})$. Then f is represented over T iff, for any preordering $S \supseteq T$, we have a congruence*

$$\sum_{P \in X_S} f(P) \equiv 0 \, (mod \, |X_S|). \tag{2.11}$$

Thus, the representability of a continuous function f (by a quadratic form) depends on a whole bunch of arithmetic conditions, in case T is a fan. Before we proceed to the proof of 2.8.6, let us take a closer look at some special cases of the congruence above. Of course, if S has index 2, then S is an ordering and $|X_S| = 1$; in this case the congruence is a tautology. Next consider an S which has index 4, say $S = P_1 \cap P_2$, where P_1, P_2 are distinct orderings in X_T. In this case, the congruence says $f(P_1) + f(P_2) \equiv 0 \, (\text{mod } 2)$. Since P_1, P_2 are arbitrary, this amounts to the condition that f has constant parity on X_T, which, as we have observed before, is a necessary condition for representability. In this light, the congruence 2.11 for S with bigger indices may be

construed as generalizations of the constant parity condition – and according to the theorem, these will be necessary and sufficient conditions for the representability of f.

After making these miscellaneous remarks, we shall now proceed to the

Proof of Theorem 2.8.6. ($\Rightarrow$) We need only consider the case $S = T$, and, by additivity, we may assume that f is represented over T by a unary form $\langle a \rangle_T$. If $a \in \pm\dot{T}$, then

$$\sum_{P \in X_T} f(P) = \sum_{P \in X_T} \mathrm{sgn}_P\langle a \rangle = \pm |X_T|,$$

so we are reduced to checking the case when $a \notin \pm T$. In this case

$$T[a] = T + T \cdot a = T \cup T \cdot a \text{ and } T[-a] = T + T \cdot (-a) = T \cup T \cdot (-a)$$

both exclude -1 and hence are preorderings in F. If $[\dot{F} : \dot{T}] = 2^n$, then these preorderings both have index 2^{n-1}. Since they are also fans, we have

$$|X_{T[a]}| = |X_{T[-a]}| = 2^{n-2}.$$

Observing finally that X_T is the disjoint union of $X_{T[a]}$ and $X_{T[-a]}$, we get

$$\sum_{P \in X_T} f(P) = \sum_{P \in X_T} \mathrm{sgn}_P\langle a \rangle = 2^{n-2} - 2^{n-2} = 0,$$

in particular proving 2.11.

($\Leftarrow$) To prove the converse, we shall imbed $C(X_T, \mathbb{Z})$ into the larger ring $C(X_T, \mathbb{Q})$ of continuous functions on X_T to $\mathbb{Q}$. Here $\mathbb{Q}$ is again given the discrete topology (not the funny topology that it inherits from the reals). In the ring $C(X_T, \mathbb{Q})$, we introduce the following inner product $\langle \_, \_ \rangle$:

$$\langle f, g \rangle = \frac{1}{|X_T|} \sum_{P \in X_T} f(P)g(P) \in \mathbb{Q}. \tag{2.12}$$

Fix an ordering $P_0 \in X_T$, and let G denote the group $\dot{P}_0/\dot{T}$ with cardinality $m = [\dot{F} : \dot{T}]/2 = |X_T|$. We claim that the functions $\{\hat{a} : a \in G\}$ form an orthonormal basis for $C(X_T, \mathbb{Q})$ under the inner product defined in 2.12.

Here (and in the following), we shall identify each $a \in G$ with a coset representative $a \in \dot{P}_0$. For each such a, we have

$$\langle \hat{a}, \hat{a} \rangle = \frac{1}{m} \sum_{P \in X_T} (\mathrm{sgn}_P(a))^2 = \frac{1}{m}|X_T| = 1,$$

and, for distinct $a, b \in G$, we have

$$\langle \hat{a}, \hat{b} \rangle = \frac{1}{m} \sum_{P \in X_T} \mathrm{sgn}_P(a)\mathrm{sgn}_P(b) = \sum_{P \in X_T} \mathrm{sgn}_P(c)$$

where $c := ab$. Since $c \notin \pm T$, by the proof of ($\Rightarrow$) the summation above is zero. Thus $\{\hat{a} : a \in G\}$ is an orthonormal set, and since $C(X_T, \mathbb{Q})$ has $\mathbb{Q}$-dimension $|X_T| = |G| = m$, this proves the claim.

Now let $f \in C(X_T, \mathbb{Z}) \subseteq C(X_T, \mathbb{Q})$ be such that the congruence 2.11 are satisfied for any

preordering $S \supseteq T$ such that $[\dot{S} : \dot{T}] \leq 2$. We have a "Fourier expansion"

$$f = \sum_{a \in G} \langle f, \hat{a} \rangle \hat{a}$$

with respect to the orthonormal basis that we found. To check that $f \in \mathrm{Im}(c_T)$, it suffices to show that $\langle f, \hat{a} \rangle \in \mathbb{Z}$ for all $a \in G$. This inner product can be computed as follows:

$$\begin{aligned}
\langle f, \hat{a} \rangle &= \frac{1}{m} \sum_{P \in X_T} \mathrm{sgn}_P(a) f(P) \\
&= \frac{1}{m} \left\{ \sum_{P \in X_{T[a]}} f(P) - \sum_{P \in X_{T[-a]}} f(P) \right\} \\
&= \frac{1}{m} \left\{ \sum_{P \in X_T} f(P) - 2 \sum_{P \in X_{T[-a]}} f(P) \right\} \\
&= \frac{1}{m} \sum_{P \in X_T} f(P) - \frac{1}{m/2} \sum_{P \in X_{T[-a]}} f(P).
\end{aligned}$$

By 2.11 for $S = T$, the first term is an integer, so we need only worry about the second term. If $a \in \dot{T}$ the second summation is empty, so assume $a \notin \dot{T}$. Then $S := T[-a] = T \cup T \cdot (-a)$ is a preordering. Since $a \in \dot{P}_0$, we have $-a \notin \dot{T}$, so

$$[\dot{S} : \dot{T}] = 2,\ [\dot{F} : \dot{S}] = 1/2[\dot{F} : \dot{T}] = m \text{ and } |X_S| = m/2.$$

Applying 2.11 to this S, we get the desired conclusion that $\langle f, \hat{a} \rangle \in \mathbb{Z}$. □

We are now in a good strategic position to follow through the "lower route" approach. The only missing link is Step (d), which is reduction of the Representation Problem from the case of general preorderings to the case of fans. The following result will, therefore, be our main goal:

Theorem 2.8.7. *Let $T_0 \subseteq F$ be a preordering, and $f \in C(X_{T_0}, \mathbb{Z})$. Then f is represented over T_0 iff f is represented over any fan containing T_0.*

Once we have proved 2.8.7, we can combine it with 2.8.2, 2.8.5 and 2.8.6 to get the following ultimate result:

Theorem 2.8.8 (Representation Theorem)**.** *Let $T_0 \subseteq F$ be a preordering, and $f \in C(X_{T_0}, \mathbb{Z})$. Then f is represented over T_0 iff, for any fan $T \supseteq T_0$ of finite index in F, we have a congruence*

$$\sum_{P \in X_T} f(P) \cong 0 \,(mod\ |X_T|).$$

Our proof of 2.8.7 follows after three lemmas:

Lemma 2.8.9. *Let $T \subseteq F$ be any preordering, and $x_1, x_2 \in \dot{F}$. Suppose φ_1, φ_2 are T-forms such that $\varphi_1\langle 1, x_1 \rangle \cong_T \varphi_2\langle 1, x_2 \rangle$. Then there exists a T-form φ such that $\varphi\langle 1, x_i \rangle \cong_T \varphi_i\langle 1, x_i \rangle$ for $i = 1, 2$.*

Proof. If $x_1 \in -\dot{T}$ (resp. $x_2 \in -\dot{T}$), the lemma is immediate as we can take $\varphi = \varphi_2$ (resp. $\varphi = \varphi_1$). Therefore, in the following, we shall assume $x_1, x_2 \notin \dot{T}$, so $T[x_i]$ $(i = 1, 2)$ are both preorderings.

To prove the lemma, we shall work with both T-forms and $T[x_i]$-forms. For this purpose, the following three observations will be useful:

$$\varphi\langle 1, x_i\rangle \cong_T \varphi_i\langle 1, x_i\rangle \Leftrightarrow \varphi \cong_{T[x_i]} \varphi_i. \tag{2.13}$$

This is checked by signature considerations.

$$\text{For any } T\text{-form, we have } D_T(\varphi\langle 1, x_i\rangle) = D_{T[x_i]}(\varphi). \tag{2.14}$$

This follows by a straightforward calculation of values.

$$\text{For any } T\text{-form } \varphi,\ \varphi\langle 1, x_i\rangle \text{ is } T\text{-isotropic iff } \varphi \text{ is } T[x_i]\text{-isotropic.} \tag{2.15}$$

This is proved by the same calculation used to prove 2.14.

To prove 2.8.9, we proceed by induction on $n = \dim \varphi_1 = \dim \varphi_2$. If $n = 1$, the hypothesis implies that $x_1\dot{T} = x_2\dot{T}$, so we are done by choosing $\varphi = \varphi_1$ or $\varphi = \varphi_2$. Now assume $n \geq 2$. From the hypothesis and 2.14, we have

$$D_{T[x_1]}(\varphi_1) = D_{T[x_1]}(\varphi_2).$$

Fix an element y in this set and write $\varphi_i \cong \langle y\rangle \perp \varphi'$ over $T[x_i]$ $(i = 1, 2)$. Then, by 2.13,

$$\varphi_1\langle 1, x_i\rangle \cong_T \langle y, yx_i\rangle \perp \varphi'\langle 1, x_i\rangle.$$

Using this for $i = 1, 2$ and cancelling $\langle y\rangle$, we get

$$\langle yx_1\rangle \perp \varphi_1'\langle 1, x_1\rangle \cong_T \langle yx_2\rangle \perp \langle\varphi_2'\langle 1, x_2\rangle. \tag{A}$$

Since yx_2 is T-represented by the left hand side, there exists $c \in D_T(\varphi_1'\langle 1, x_1\rangle) = D_{T[x_1]}(\varphi_1')$ sicj that yx_2 is T-represented by $\langle yx_1, c\rangle$, i.e,

$$\langle yx_1, c\rangle \cong_T \langle yx_2, x_1x_2c\rangle.$$

Writing $\varphi_1' \cong_{T[x_1]} \langle c\rangle \perp \varphi_1''$, (A) becomes

$$\langle yx_1\rangle \perp cx_1\langle 1, x_2\rangle \perp \varphi_1''\langle 1, x_1\rangle \cong_T \langle yx_2\rangle \perp \langle\varphi_2'\langle 1, x_2\rangle. \tag{B}$$

After cancelling $\langle yx_2\rangle$, we have $cx_1 \in D_T(\varphi_2'\langle 1, x_2\rangle)$, so as before, we can write $\varphi_2' \cong_{T[x_2]} \langle cx_1\rangle \perp \varphi_2''$. Then (B) becomes

$$cx_1\langle 1, x)2\rangle \perp \varphi_1''\langle 1, x_1\rangle \cong_T cx_1\langle 1, x_2\rangle \perp \varphi_2''\langle 1, x_2\rangle, \tag{C}$$

so $\varphi_1''\langle 1, x_1\rangle \cong_T \varphi_2''\langle 1, x_2\rangle$. We have now

$$\varphi_2 \cong_{T[x_2]} \langle y, cx_1\rangle \perp \varphi_2''$$

and

$$\varphi_1 \cong T[x_1]\langle y, c\rangle \perp \varphi_1'' \cong_{T[x_1]} \langle y, cx_1\rangle \perp \varphi_1''.$$

Hence we can let $\varphi_T\langle y, cx_1\rangle \perp \varphi''$, and find φ'' by the inductive hypothesis for the dimension $n - 2$. □

Lemma 2.8.10. *Let $T \subseteq F$ be a preordering, and let $x_1, x_2 \in \dot{F}$ be such that $x_3 : -x_1x_2 \notin \pm T$, and $\langle x_1, x_2\rangle \cong_T \langle 1, -x_3\rangle$. Let $f : X_T \to \mathbb{Z}$ be any (not necessarily continuous) function on X_T. If f is represented by a form φ_i over $T[x_i]$ $(i = 1, 2, 3)$, then f is represented by a form φ over T.*

Note that each $T[x_i]$ $(i = 1, 2, 3)$ is a preordering in this lemma. For $i = 3$, this follows from the assumption that $x_3 \notin -T$. Since we also assume $x_3 \notin T$, $\langle 1, -x_3\rangle$ is not the T-hyperbolic plane. By 2.2.7, its T-values x_1, x_2 cannot be in $-T$, so $T[x_1], T[x_2]$ are also preorderings.

Proof of lemma 2.8.10. We may assume that $\varphi_3 = 0$ (after replacing f by $f - \hat{\varphi}_3$). Also, we may assume that φ_i is anisotropic over $T[x_i]$, for $i = 1, 2$. Since $x_3 = -x_1x_2$, this means that $\varphi_i\langle 1, x_i\rangle$ is anisotropic over T, for $i = 1, 2$. Since $x_3 = -x_1x_2$, the symmetric difference of $X_{T[x_1]}$ and $X_{T[x_2]}$ is $X_{T[x_3]}$, and, since $\langle x_1, x_2\rangle \cong_T \langle 1, -x_3\rangle$, the union of these two sets is X_T.

By checking signatures, we see that $\varphi_1\langle 1, x_1\rangle = \varphi_2\langle 1, x_2\rangle$ in W_TF. Therefore, we have

$$\varphi_1\langle 1, x_1\rangle \cong_T \varphi_2\langle 1, x_2\rangle,$$

since these forms are both T-anisotropic.

By 2.8.9 (and 2.13), there exists a T-form φ such that $\varphi \cong \varphi_i$ over $T[x_i]$, for $i = 1, 2$. Hence φ will represent f over $X_{T[x_1]} \cup X_{T[x_2]} = X_T$. □

The last lemma we need for the proof of 2.8.7 shows in an interesting way how naturally fans can arise in dealing with the Representation Problem:

Lemma 2.8.11. *Let f be a function from X_T to $\mathbb{Z}$ (which is not necessarily continuous). Suppose f is not represented over T, but is represented over any preordering $T' \supsetneq T$. Then T must be a fan.*

Proof. Assume T is not a fan. Then by 2.7.4 there exists a nonzero $x \notin_T$ such that $\langle 1, x\rangle \cong_T \langle y, x/y\rangle$ for some $y \notin T \cup T \cdot x$. We also have $x \notin T$ (since the T-form $\langle 1, 1\rangle$ can represent only elements in $\dot{T}$). Now let $x_1 = y$, $x_2 = x/y$ and $x_3 = -x_1x_2 = -x$. Then $x_3 \notin \pm T$ and $\langle x_1, x_2\rangle \cong_T \langle 1, -x_3\rangle$, as in 2.8.10. As noted after the statement of 2.8.10, each $T[x_i]$ $(i = 1, 2, 3)$ is a preordering; also we have each $x_i \notin T$, so $T[x_i] \supsetneq T$. By the hypothesis, f is not represented over each $T[x_i]$ $(i = 1, 2, 3)$. But the, by 2.8.10, f is represented over T, a contradiction. □

We have now developed all the necessary machinery to prove 2.8.7:

Proof of Theorem 2.8.7. Returning to the notations there, we deal with a function $f \in C(X_{T_0}, \mathbb{Z})$ which we assume is represented over any fan $\supseteq T_0$. Assume that f is not represented over T_0. Let $\mathcal{F}$ be the (nonempty) family of preorderings $T \supseteq T_0$ such that f is not represented over T. If $\mathcal{F}$ has a maximal element T_1 (with respect to inclusion), then by 2.8.11 T_1 must be a fan, and we get a contradiction.

To see that $\mathcal{F}$ does have a maximal element, we need only check that Zorn's lemma applies. Consider, therefore, a family of preorderings $\{T_i : i \in I\}$ which form a chain in $\mathcal{F}$ (with respect to inclusion). We are done if we can show that the preordering $T := \bigcup_{i\in I} T_i$ belongs to $\mathcal{F}$. Let φ be any T_0-form, and let

$$V = \{P \in X_{T_0} : f(P) = \hat{\varphi}(P)\}.$$

This is an open (and closed) set in X_{T_0}, by continuity of f and $\hat{\varphi}$. Since f cannot be represented over φ over T_i, we have $(X_{T_i}) \setminus V \neq \emptyset$. These closed sets form a chain in X_{T_0}, so by compactness of X_{T_0}, we have

$$\emptyset = \bigcap_{i\in I}((X_{T_i}) \setminus V) = \left(\bigcap_{i\in I} X_{T_i}\right) \setminus V = (X_T) \setminus V.$$

Therefore, f cannot be represented by φ over T. Since this holds for any form φ, we have $T \in \mathcal{F}$. This completes the proof of 2.8.7. $\square$

Chapter 3

First Abstract Theories

The first abstract theories appears in 70's, by the hands of M. Marshall and C. M. Cordes. These theories appears for a reason: they are interested in the existence (or not) of fields with prescribed properties relating to quadratic forms. Questions like

There is a field with finite number of square classes and non-trivial Kaplansky's radical (see for example, [Cor75])? [1]

are the guide to their journey.

The very first step in abstracting the theory of quadratic forms is decide

What we take as primitive notions?

There is a reasonable list to take acount: representability, Witt ring, orderings, Pfister forms, quaternionic structures and so on. And the privilegy of one in relation to the others is none! Because this, the first theories are not necessarily the most elegant and efficient ones. But they are important, because they answer some questions about Witt rings and reveal a roadmap to construct more sophisticate tools to attack difficult questions, like Marshall's signature conjecture (see theorem 1.6.7).

In this chapter we expose the quaternionic structures, the abstract witt rings and the Cordes schemes. This is not the historical order (Cordes schemes are the first and quaternionic structures the last) but for didatical reasons we choose as well. Chapters 1 and 2 is the basic set of properties that we want to proof in all abstract theories, so we strongly recommend to keep it in mind and compare the results in the next chapters with the same ones in chapters 1 and 2 whenever is possible.

[1] A quick digression about the Kaplansky's radical: a **central simple algebra** over a field F is an algebra A over F whose center is F, and whose only two-sided ideals are 0 and A. As we will see later in this chapter, each quaternion algebra over F is such an algebra. By Wedderburn's structure theorem, every central simple algebra over F is uniquely of the form $A \cong M_n(D) \cong D \otimes M_n(F)$ for some $n \geq 1$ and some central division algebra D over F. D is referred to as the **division algebra component** of A. Two central simple algebras A, B over F are said to be **equivalent**, denoted $A \sim B$ if their associated division algebra components are isomorphic as algebras. This defines an equivalence relation on the class of all central simple algebras over F. Let us denote by $Br(F)$ the associated set of equivalence classes. The tensor product induces a binary operation on $Br(F)$, and with respect to this operation, $Br(F)$ is an abelian group. This is known as the **Brauer group** of F. So, given $a, b \in \dot{F}/\dot{F}^2$, we can define a quaternion algebra $\left(\frac{a,b}{F}\right)$, and therefore, a map $(.,.) : \dot{F}/\dot{F}^2 \times \dot{F}/\dot{F}^2 \to Br(F)$, given by $(a, b) \mapsto \left(\frac{a,b}{F}\right)$. The **Kaplansky's radical** of F is the kernel of this map $(.,.)$.

3.1 Quaternionic Structure

First of all, we show how the theory of quadratic forms over a field F os characteristic not 2, is describable in terms of the quaternionic structure associated to F, and then, the axioms for abstract quaternionic structures appears naturally. Here, we follow chapters 1 and 2 of [Mar80]. Of course, we admit that all fields have characteristic not 2.

3.1.1 The Field case

In this section we define the quaternionic structure $(G(F), Q(F), q)$ associated to F, prove its basic properties, and show how the study of quadratic forms over F is reduced to the study of the quaternionic structure of F.

We define $G(F)$ to be the quotient group $\dot{F}/\dot{F}^2$. This is a group of exponent 2 in the sense that $x^2 = 1$ for all $x \in G(F)$. In view of theorem 1.1.25(c) we can view quadratic forms over F to be n-tuples $\langle a_1, ..., a_n\rangle$ with $a_1, ..., a_n \in G(F)$. We define $Q(F)$ to be the set of all isometry classes of quadratic forms of the type $\langle 1, -a, -b, ab\rangle$, with $a, b \in G(F)$. We consider $Q(F)$ to be a "pointed set" with point 0 equal to the isometry class of $\langle 1, -1, 1, -1\rangle$. Finally, we define $q : G(F) \times G(F) \to Q(F)$ to be the map sending (a, b) to the isometry class of $\langle 1, -a, -b, ab\rangle$. The triple $(G(F), Q(F), q)$ will be referred to as the *quaternionic structure associated to* F.

The reader could be note these facts: the isometry class of $\langle 1, -a, -b, ab\rangle$ is nothing else that the isometry class of the Pfister form $\langle\langle a, b\rangle\rangle$ and with the proper identification, we have $Q(F) \subseteq W(F)$, the Witt Ring of F. These facts will be useful later.

Theorem 3.1.1. *For all $a, b, c, d \in G(F)$ we have:*

i - $q(a, b) = q(b, a)$.

ii - $q(a, -a) = 0$.

iii - $q(a, b) = q(a, c) \Leftrightarrow q(a, bc) = 0$.

iv - $q(a, b) = q(c, d) \Rightarrow$ *there exist* $x \in G(F)$ *with* $q(a, b) = q(a, x)$, *and* $q(c, d) = q(c, x)$.

Proof. With the identification $Q(F) \subseteq W(F)$, theorem 1.1.25(d) and their corollaries, operating on the Witt ring we obtain (i), (ii) and (iii). To prove (iv), suppose $q(a, b) = q(c, d)$, i.e, the isometry class of $\langle 1, -a, -b, ab\rangle$ is equal to the isometry class of $\langle 1, -c, -d, cd\rangle$. By Witt's Cancellation, $\langle -a, -b, -ab\rangle \cong \langle -c, -d, cd\rangle$. There exist $e, f, g \in G(F)$ with $\langle -b, ab\rangle \cong \langle e, f\rangle$, $\langle -d, cd\rangle \cong \langle g, f\rangle$ and $\langle -a, e\rangle \cong \langle -c, g\rangle$. Comparing discriminants we get $ef = -a$, $gf = -c$, so $e = -af$ and $g = -cf$. Taking $x = -f$, we have $e = ax$, $g = cx$, so $\langle -b, ab\rangle \cong \langle -x, ax\rangle$ and $\langle -d, cd\rangle \cong \langle -x, cx\rangle$. Adding $\langle 1, -a\rangle$ and $\langle 1, -c\rangle$ respectively we obtain $q(a, b) = q(a, x)$ and $q(c, d) = q(c, x)$, proving (iv). □

We now give a result which shows how the isometry relation on quadratic forms over F is determined by the quaternionic structure:

Theorem 3.1.2.

i - $\langle a\rangle \cong \langle b\rangle \Leftrightarrow a = b$.

ii - $\langle a, b\rangle \cong \langle c, d\rangle \Leftrightarrow ab = cd$ *and* $q(a, b) = q(c, d)$.

iii - *For* $n \geq 3$, $\langle a_1, ..., a_n\rangle \cong \langle b_1, ..., b_n\rangle \Leftrightarrow$ *there exist* $a, b, c_3, ..., c_n \in G(F)$ *with* $\langle a_2, ..., a_n\rangle \cong \langle a, c_3, ..., c_n\rangle$, $\langle b_2, ..., b_n\rangle \cong \langle b, c_3, ..., c_n\rangle$, *and* $\langle a_1, a\rangle \cong \langle b_1, b\rangle$.

Proof. Here, we just need to combine the theorems (and corollaries) 1.1.26,1.1.27, 1.1.28 with the operations on the Witt ring (remember that $Q(F) \subseteq W(F)$!). □

Now, we devote some time to describe the relationship between the elements of $Q(F)$ and quaternion algebras over F. This is not a necessary knowledge for the rest of the content of this work, but quaternion algebras is the classical treatment for the abstract quaternionic structure that will be presented in the next section.

For fixed $a, b \in \dot{F}$, the *quaternion algebra* $\left(\frac{a,b}{F}\right)$ is defined to be the unitary algebra over F generated by symbols i, j subject to $i^2 = a$, $j^2 = b$, $ij = -ji$. It is a 4-dimensional algebra over F with basis $1, i, j$ and $k = ij$. On this so called "standard" basis, the multiplication is given by $i^2 = a$, $j^2 = b$, $k^2 = -ab$, $ij = -ji = k$, $kj = -jk = bi$, and $ik = -ki = aj$.

Theorem 3.1.3. *Let $a, b \in \dot{F}$, and let $A = \left(\frac{a,b}{F}\right)$. Then the center of A is $F = F \cdot 1$, and A has only the trivial 2-sided ideals.*

Proof. Let $x = x_0 + x_1 i + x_2 j + x_3 k$ lie in the center of A. Thus, by definition, $xy = yx$ for all $y \in A$. In particular,

$$0 = ix - xi = 2x_3 j + 2x_2 k$$

so $x_2 = x_3 = 0$. Using the same argument with j instead of i, we obtain $x_1 = 0$. Thus $x = x_0 \in F$.

Now suppose $J \subseteq A$ be a 2-sided ideal and $x \in J$, $x \neq 0$. We wish to show that $J = A$. Suppose $x = x_0 + x_1 i + x_2 j + x_3 k$. Multiplying x by a suitable element of $\{1, i, j, k\}$, we can assume $x_3 \neq 0$. Let $y = ix - xi$. Thus $y \in J$, and, as above, $y_2 j + y_3 k$, where $y_2 = 2x_3 a \neq 0$, and $y_3 = 2x_2$. Now let $z = yj - jy$. Thus $z \in J$, and $z = 2y_2 b \in \dot{F}$. Thus z is a unit in A, so $J = A$. □

Corollary 3.1.4. *For $a, b \in \dot{F}$, $\left(\frac{a,b}{F}\right)$ is either a division algebra over F or it is isomorphic to $M_2(F)$ (the algebra of all 2×2 matrices over F).*

Proof. By theorem 3.1.3, $A = \left(\frac{a,b}{F}\right)$ is a simple algebra over F, so by Wedderburn's theorem on simple algebras, $A \cong M_n(D)$, the algebra of all $n \times n$ matrices over D, for some division algebra D over F. Comparing dimensions, $4 = n^2 k$, where k denote the dimension of D over F. Thus either $n = 2$, $k = 1$, in which case $A \cong M_2(F)$, or $n = 1$, $k = 4$, in which case $A \cong D$. □

We now establish the connection between quaternion algebras and elements of $Q(F)$. Suppose $A = \left(\frac{a,b}{F}\right)$ for some $a, b \in \dot{F}$. Let us say an element $x = x_0 + x_1 i + x_2 j + x_3 k$ in A is a **pure quaternion** if $x_0 = 0$. We denote $A_0 = \{v \in A : v \text{ is pure}\}$.

Lemma 3.1.5. *Suppose $x \in A$, $x \neq 0$. Then x is pure if and only if $x^2 \in F$, $x \notin F$.*

Proof. One sees by "long-hand" computation that

$$x^2 = x_0^2 + a x_1^2 + b x_2^2 - ab x_3^2 + 2x_0(x_1 i + x_2 j + x_3 k).$$

Thus, if x is pure, then $x^2 = a x_1^2 + b x_2^2 - ab x_3^2 \in F$. Conversely, suppose $x^2 \in F$, $x \notin F$. Thus $2x_0(x_1 i + x_2 j + x_3 k) = 0$. But not all of x_1, x_2, x_3 are zero. Since $x_0 x_1 = x_0 x_2 = x_0 x_3 = 0$, this implies $x_0 = 0$. Thus x is pure. □

It follows that the concept of "purity" is independent of the particular presentation of A. Another way of putting this is: any isomorphism $A \cong B$ of quaternion algebras must carry pure quaternions to pure quaternions.

Corollary 3.1.6. *If* $A = \left(\frac{a,b}{F}\right)$, $B = \left(\frac{c,d}{F}\right)$ *and* $\varphi : A \to B$ *is an* F*-algebra isomorphism, then* $\varphi(A_0) = B_0$.

For $x = x_0 + x_1 i + x_2 j + x_3 k$ in A, we define the **conjugate** of x to be $\overline{x} = x_0 - x_1 i - x_2 j - x_3 k$. Note that for $x \in F$, $\overline{x} = x$. One verifies for $x, y \in A$ and $c \in F$ that $\overline{x+y} = \overline{x} + \overline{y}$, $\overline{cx} = c\overline{x}$, $\overline{xy} = \overline{y}\,\overline{x}$, and $\overline{\overline{x}} = x$. Thus conjugation is an algebra anti-isomorphism of order 2.

Let us define the **trace** $tr : A \times A \to F$ by $tr(x, y) = 1/2(x\overline{y} + y\overline{x})$. The trace is in fact, well-defined, since $\overline{tr(x,y)} = tr(x, y)$, then $tr(x, y) \in F$. One observe that tr is a symmetric bilinear mapping on the underlying vector space of A. Thus, as well as being an algebra, A can also be viewed as a quadratic space. The associated quadratic mapping is referred to as the **norm** of A. It is given by

$$N(x) = tr(x, x) = \frac{1}{2}(x\overline{x} + x\overline{x}) = x\overline{x}.$$

It is important to note that, the conjugation mapping (and hence the quadratic space structure) on A is independent of the particular presentation of A. Let $A = \left(\frac{a,b}{F}\right)$, $B = \left(\frac{c,d}{F}\right)$ and suppose that $\varphi : A \to B$ is an algebra isomorphism. Then corollary 3.1.6 implies that $\varphi(A_0) = B_0$. If $x = \alpha + x_0$, where $\alpha \in F$ and $x_0 \in A_0$, then $\overline{x} = \alpha - x_0$, and hence $\varphi(x) = \alpha + \varphi(x_0)$ and $\varphi(\overline{x}) = \alpha - \varphi(x_0)$. Since $\varphi(x_0) \in B_0$, we have $\overline{\varphi(x)} = \varphi(\overline{x})$. Therefore,

$$N(\varphi(x)) = \varphi \cdot \overline{\varphi(x)} = \varphi(x) \cdot \varphi(\overline{x}) = \varphi(x\overline{x}) = \varphi(N(x)) = N(x),$$

so φ is an isometry. Thus any isomorphism $A \cong B$ of quaternion algebras is also an isometry of quadratic spaces.

Observe that if $x \in F$, $\overline{x} = x$, whereas if x is pure, $\overline{x} = -x$. Thus if $x \in F$ and y is pure then

$$tr(x, y) = \frac{1}{2}(-xy + yx) = 0.$$

Now suppose x, y are both pure. Then

$$tr(x, y) = 0 \Leftrightarrow \frac{1}{2}(-xy - yx) = 0 \Leftrightarrow xy = -yx.$$

It follows from these remarks, and the fact that i, j, k are pure and anti-comute, that the standard basis $1, i, j, k$ forms an orthogonal basis. Since $N(1) = 1$, $N(i) = -a$, $N(j) = -b$, and $N(k) = ab$, we see that the quadratic form of A with respect to this basis is $\langle 1, -a, -b, ab\rangle$. Note that

$$\left(\frac{ax^2, by^2}{F}\right) \cong \left(\frac{a, b}{F}\right)$$

holds for any $a, b, x, y \in \dot{F}$. We see this replacing the standard basis $\{1, i, j, k\}$ of $\left(\frac{a,b}{F}\right)$ by $\{1, i', j', k'\}$ where $i' = xi$, $j' = yj$, $k' = i'j'$. Then $i'^2 = x^2 a$, $j'^2 = y^2 b$. Since we are only interested in the isomorphism class of the quaternion algebra $\left(\frac{a,b}{F}\right)$, we are thus able to view a, b as elements of $G(F)$. We now prove the following:

Theorem 3.1.7. *Let* $a, b, c, d \in G(F)$. *Then* $q(a, b) = q(c, d)$ *iff the algebras* $\left(\frac{a,b}{F}\right)$ *and* $\left(\frac{c,d}{F}\right)$ *are isomorphic. Further,* $q(a, b) = 0$ *iff* $\left(\frac{a,b}{F}\right) \cong M_2(F)$.

Proof. Suppose $\alpha : \left(\frac{a,b}{F}\right) \cong \left(\frac{c,d}{F}\right)$ is an algebra isomorphism. In view of the criterion for purity

given in lemma 3.1.5, $\alpha(\overline{x}) = \overline{\alpha(x)}$ for all $x \in \left(\frac{a,b}{F}\right)$. It follows that

$$tr(\alpha(x), \alpha(y)) = tr(x, y) \text{ for all } x, y \in \left(\frac{a,b}{F}\right).$$

Thus α is an isometry of quadratic spaces. From the basic correspondence between quadratic forms and quadratic spaces, follows that the associated quadratic forms $\langle 1, -a, -b, ab\rangle$ and $\langle 1, -c, -d, cd\rangle$ are isometric.

Now, conversely, assume $\langle 1, -a, -b, ab\rangle \cong \langle 1, -c, -d, cd\rangle$. Then $\langle -a, -b, ab\rangle \cong \langle -c, -d, cd\rangle$ by Witt's cancellation. Let $1, i, j, k$ and $1, i', j', k'$ be the "standard" bases of $\left(\frac{a,b}{F}\right)$ and $\left(\frac{c,d}{F}\right)$ respectively. It follows that the 3-dimensional subspace $[i, j, k]$ of pure quaternions of $\left(\frac{a,b}{F}\right)$ is isometric to the corresponding subspace $[i, j', k']$ of $\left(\frac{c,d}{F}\right)$. Let $\alpha : [i, j, k] \cong [i', j', k']$ be any isometry. Then $\alpha(i)$ is pure so $\overline{\alpha(i)} = -\alpha(i)$. Thus

$$N(\alpha(i)) = \alpha(i)\overline{\alpha(i)} = -\alpha(i)^2.$$

But α is an isometry so $N(\alpha(i)) = N(i) = -a$. Thus $\alpha(i)^2 = a$. Similarly, $\alpha(j)^2 = b$. Since $tr(i, j) = 0$, we also have $tr(\alpha(i), \alpha(j)) = 0$. In view of an earlier remark, this implies $\alpha(i)$ and $\alpha(j)$ anti-comutes. Thus, by replacing the standard basis of $\left(\frac{c,d}{F}\right)$ by $\{1, \alpha(i), \alpha(j), \alpha(i)\alpha(j)\}$, we see that $\left(\frac{c,d}{F}\right) \cong \left(\frac{a,b}{F}\right)$.

Now consider $\left(\frac{1,-1}{F}\right)$. If $1, i, j, k$ is the "standard" basis of this algebra, then $i^2 = 1$, $j^2 = -1$, so

$$(i + j)^2 = i^2 + ij + ji + j^2 = i^2 + j^2 = 0.$$

It follows that $i + j$ is not invertible, so $\left(\frac{1,-1}{F}\right)$ is not a division algebra. Thus, by corollary 3.1.4, $\left(\frac{1,-1}{F}\right) \cong M_2(F)$. Thus by the first half of the theorem, and the fact that $q(1, -1) = 0$,

$$\left(\frac{a,b}{F}\right) \cong M_2(F) \Leftrightarrow \left(\frac{a,b}{F}\right) \cong \left(\frac{1,-1}{F}\right) \Leftrightarrow q(a, b) = q(1, -1) \Leftrightarrow q(a, b) = 0.$$

□

3.1.2 Quaternionic structures and the associated form theory

Definition 3.1.8. *A quaternionic structure (or Q-structure) is defined to be a triple (G, Q, q) where G is a group of exponent 2 (i.e, $x^2 = 1$ for all $x \in G$) with a distinguished element denoted -1, Q is a pointed set with distinguished point denoted 0, and $q : G \times G \to Q$ is a surjective mapping satisfying:*

Q1 (symmetry) - $q(a, b) = q(b, a)$.

Q2 - $q(a, -a) = 0$.

Q3 (weak bilinearity) - $q(a, b) = q(a, c) \Leftrightarrow q(a, bc) = 0$.

Q4 (linkage) - $q(a, b) = q(c, d) \Rightarrow$ *there exist* $x \in G$ *such that* $q(a, b) = q(a, x)$ *and* $q(c, d) = q(c, x)$.

If F is a field of characteristic $\neq 2$, then we have the associated Q-structure $(G(F), Q(F), q)$ (see theorem 3.1.1). We do not claim that every Q-structure is realized in this way, as the Q-structure associated to a field, but, on the other hand, is not known if there is a counter example.

Here are basic consequences of these definition:

Lemma 3.1.9. *Let (G, Q, q) be a quaternionic structure and $a, b \in G$. Then:*

i - $q(a, 1) = 0$.

ii - $q(a, a) = q(a, -1)$.

iii - $q(a, -ab) = q(a, b)$.

iv - $q(a, b) = q(c, d) \Leftrightarrow$ *there exist* $x \in G$ *with* $q(a, bx) = 0$, $q(c, dx) = 0$ *and* $q(ac, x) = 0$.

Proof.

i - Follow from Q3, since $q(a, 1) = q(a, 1)$.

ii - By Q2 $q(a, -a) = q(a, (-1)a) = 0$, so by Q3, $q(a, a) = q(a, -1)$.

iii - Since by Q2 $q(a, -ab^2) = q(a, -a) = 0$, Q3 provides $q(a, -ab) = q(a, b)$.

iv - ($\Rightarrow$) From $q(a, b) = q(c, d)$ by Q4 we obtain $x \in G$ such that $q(a, b) = q(a, x)$ and $q(c, d) = q(c, x)$. So using Q3, we have $q(a, bx) = q(c, dx) = 0$. From $q(a, x) = q(a, b) = q(c, d) = q(c, x)$, using Q3 again we obtain $q(ac, x) = 0$.

($\Leftarrow$) Using Q3 in the equalities $q(a, bx) = 0$, $q(c, dx) = 0$ and $q(ac, x) = 0$ we get $q(a, b) = q(a, x)$, $q(c, d) = q(c, x)$ and $q(a, x) = q(c, x)$. So $q(a, b) = q(c, d)$.

□

A *morphism* between Q-structures (G, Q, q) and (G', Q', q') is a group homomorphism $\alpha : G \to G'$ satisfying $\alpha(-1) = -1$ and

$$q(a, b) = 0 \Rightarrow q'(\alpha(a), \alpha(b)) = 0$$

for all $a, b \in G$. By 3.1.9(iv), the second requirement for a morphism of Q-structures implies the (apparently stronger) condition

$$q(a, b) = q(c, d) \Rightarrow q'(\alpha(a), \alpha(b)) = q'(\alpha(c), \alpha(d)).$$

We now show how to develop an abstract theory of quadratic forms associated to any abstract quaternionic structure. Of course, these abstract approach generalize the classical one, in the sense that on case the Q-structure we start with is the Q-structure of some field F, this is just the usual quadratic form theory over F.

Let (G, Q, q) be a Q-structure which will remain fixed throughout this section. A *form of dimension $n \geq 1$ over G* is just an n-tuple $f \cong \langle a_1, ..., a_n \rangle$ where $a_1, ..., a_n \in G$. The dimension of f is denoted by $\dim(f)$. The discriminant of f is defined to be $\text{disc}(f) := a_1 a_2 ... a_n \in G$. If $a \in G$, we can *scale* f by a to obtain the form $af := \langle aa_1, ..., aa_n \rangle$. The *sum* of f and a form $g \cong \langle b_1, ..., b_m \rangle$ is defined by $f \oplus g = \langle a_1, ..., a_n, b_1, ..., b_m \rangle$ and the *tensor product* of f and g is defined by $f \otimes g = \langle a_1 b_1, ..., a_i b_j, ..., a_n b_m \rangle$.

Isometry of one and two-dimensional forms is defined by $\langle a \rangle \cong \langle b \rangle \Leftrightarrow a = b$ and $\langle a, b \rangle \cong \langle c, d \rangle \Leftrightarrow ab = cd$ and $q(a, b) = q(c, d)$. For forms of dimension $n \geq 3$ isometry is defined inductively

by: $\langle a_1, ..., a_n\rangle \cong_n \langle b_1, ..., b_n\rangle$ if and only there are $x, y, z_3, ..., z_n \in A$ such that $\langle a_1, x\rangle \cong \langle b_1, y\rangle$, $\langle a_2, ..., a_n\rangle \cong_{n-1} \langle x, z_3, ..., z_n\rangle$ and $\langle b_2, ..., b_n\rangle \cong_{n-1} \langle y, z_3, ..., z_n\rangle$.

Note that these definitions in the field case is already know basic properties of the isometry. The next results is to establish another properties for our abstract isometry.

Proposition 3.1.10. *Let (G, Q, q) be a quaternionic structure. Then for all $a, b, c, d, x \in G$ and all forms φ, ψ:*

a - If π is a permutation of $\{1, ..., n\}$ and $\varphi = \langle a_1, ..., a_n\rangle$, $\psi = \langle a_{\pi(1)}, ..., a_{\pi(n)}\rangle$ then $\varphi \equiv \psi$.

b - $\varphi \cong \psi \Rightarrow dim(\varphi) = dim(\psi)$ and $disc(\varphi) = disc(\psi)$.

c - $\langle b, -bx\rangle \cong \langle c, -cx\rangle$ holds if and only if $q(bc, x) = 0$.

d - $\varphi \cong \psi \Rightarrow a\varphi \cong a\psi$. In particular, if $\langle a, b\rangle \cong \langle c, d\rangle$ then $\langle xa, xb\rangle \cong \langle xc, xd\rangle$ for all $x \in G$.

e - $\langle -a, -b, ab\rangle \cong \langle -c, -d, cd\rangle \Leftrightarrow q(a, b) = q(c, d)$.

f - $\langle a, -a\rangle \cong \langle 1, -1\rangle$.

Proof.

a - We may assume $n \geq 3$. If $\pi(1) = i \geq 2$, take $a = a_i$, $b = a_1$, and take $c_3, ..., c_n$ to be the elements left after a_1 and a_i are deleted from the list $a_1, ..., a_n$. Note that $a, c_3, ..., c_n$ is a permutation of $a_2, ..., a_n$; $b, c_3, ..., c_n$ a permutation of $b_2, ..., b_n$ and b_1, b is a permutation of a_1, a, so the result is true by induction on n. On the other hand, if $\pi(1) = 1$, take $a = b = a_2$, and $c_i = a_i$, $i \geq 3$.

b - The first assertion is immediate. Also, the assertion concerning discriminants is true for 1 and 2 dimensional forms. Now, suppose $\varphi = \langle a_1, ..., a_n\rangle$, $\psi = \langle b_1, ..., b_n\rangle$, $n \geq 3$. By assumption, there exists $a, b, c_3, ..., c_n$ the "witness of the isometry", i.e, with $\langle a_1, a\rangle \cong \langle b_1, b\rangle$, $\langle a_2, ..., a_n\rangle \cong_{n-1} \langle a, c_3, ..., c_n\rangle$ and $\langle b_2, ..., b_n\rangle \cong_{n-1} \langle b, c_3, ..., c_n\rangle$. By induction, we have $a_2...a_n = ac_3...c_n$, $a_1a = b_1b$ and $bc_3...c_n = b_2...b_n$. Thus

$$a_1a_2...a_n = a_1ac_3...c_n = b_1bc_3...c_n = b_1b_2...b_n.$$

c - $q(b, -bx) = q(b, x)$ and $-b^2x = -x = -c^2x$ so $\langle b, -bx\rangle$ and $\langle c, -cx\rangle$ have the same discriminants. Thus

$$\langle b, -bx\rangle \cong \langle c, -cx\rangle \Leftrightarrow q(b, -bx) = q(c, -cx) \overset{3.1.9(iii)}{\Leftrightarrow} q(b, x) = q(c, x) \Leftrightarrow q(bc, x) = 0.$$

d - Is immediate for 1-dimensional forms. Now suppose $\varphi = \langle b, d\rangle$, $\psi = \langle c, e\rangle$ and $\varphi \cong \psi$. Thus $bd = ce$, and setting $-x := bd = ce$, we get $d = -bx$ and $e = -cx$. Thus $\varphi \cong \langle b, -bx\rangle$, $\psi \cong \langle c, -cx\rangle$, $a\varphi \cong \langle ab, -abx\rangle$, $a\psi \cong \langle ac, -acx\rangle$. Thus, applying (c),

$$\varphi \cong \psi \Leftrightarrow q(bc, x) = 0 \Leftrightarrow q(abac, x) = 0 \Leftrightarrow a\varphi \cong a\psi.$$

The result for forms of dimension ≥ 3 follows by induction on n.

e - By definition, $\langle -a, -b, ab\rangle \cong \langle -c, -d, cd\rangle$ if exists $p, q, r \in G$ such that $\langle -b, ab\rangle \cong \langle p, r\rangle$, $\langle -d, cd\rangle \cong \langle q, r\rangle$ and $\langle -a, p\rangle \cong \langle -c, q\rangle$. Comparing discriminants this yields $-a = pr$, $-c = qr$.

Let $x = -r$. Thus $p = ax$, $q = cx$. Thus $\langle -a, -b, ab\rangle \cong \langle -c, -d, cd\rangle$ iff exists $x \in G$ such that $\langle -b, ab\rangle \cong \langle -x, ax\rangle$, $\langle -d, cd\rangle \cong \langle -x, cx\rangle$ and $\langle -a, ax\rangle \cong \langle -c, cx\rangle$. Using (d) and (c) we get

$$\langle -b, ab\rangle \cong \langle -x, ax\rangle \Leftrightarrow \langle b, -ab\rangle \cong \langle x, -ax\rangle \Leftrightarrow q(a, bx) = 0.$$

Similarly, $\langle -d, cd\rangle \cong \langle -x, cx\rangle \Leftrightarrow q(c, dx) = 0$ and $\langle -a, ax\rangle \cong \langle -c, cx\rangle \Leftrightarrow q(x, ac) = 0$. Summarizing, we have $\langle -a, -b, ab\rangle \cong \langle -c, -d, cd\rangle$ iff there exist $x \in G$ such that $q(a, bx) = 0$, $q(c, dx) = 0$ and $q(ac, x) = 0$. By 3.1.9(iv), we have $\langle -a, -b, ab\rangle \cong \langle -c, -d, cd\rangle$ iff $q(a, b) = q(c, d)$.

f - Is just Q2 and the definition of isometry.

□

Theorem 3.1.11. *Isometry is an equivalence relation (on forms of same dimension).*

Proof. Since reflexivity and symmetry follows by definition of $\cong$, we just need to worry with transitivity. Let φ, ψ, θ be n-dimensional forms over G with $\varphi \cong \psi$ and $\psi \cong \theta$. We show that $\varphi \cong \theta$ by induction on n. This is immediate if $n = 1$ or 2. If $n = 3$, scaling by discriminant we are reduced to the discriminant 1 case (see 3.1.10(d)). But any 3-dimensional form of discriminant 1 is of the shape $\langle -a, -b, ab\rangle$ for suitable $a, b \in G$. Thus, this case follows using 3.1.10(e).

Now assume $n \geq 4$. Let $\varphi \cong \langle a\rangle \oplus \varphi'$, $\psi \cong \langle b\rangle \oplus \psi'$ and $\theta \cong \langle c\rangle \oplus \theta'$. Thus, exists $a', b', b'', c' \in G$ and $n-2$-dimensional forms τ, σ such that

$$\varphi' \cong \langle a'\rangle \oplus \tau,\ \psi' \cong \langle b'\rangle \oplus \tau \text{ and } \langle a, a'\rangle \cong \langle b, b'\rangle.$$

and

$$\psi' \cong \langle b''\rangle \oplus \sigma,\ \theta' \cong \langle c'\rangle \oplus \sigma \text{ and } \langle b, b''\rangle \cong \langle c, c'\rangle.$$

Thus, by induction, $\langle b'\rangle \oplus \tau \cong \langle b''\rangle \oplus \sigma$, so exists b_1, b_2 and an $n-3$-dimensional form α satisfying

$$\tau \cong \langle b_1\rangle \oplus \alpha,\ \sigma \cong \langle b_2\rangle \oplus \alpha \text{ and } \langle b', b_1\rangle \cong \langle b'', b_2\rangle.$$

It follows (using transitivity for $n \leq 3$) that

$$\langle a, a', b_1\rangle \cong \langle b, b', b_1\rangle \cong \langle b, b'', b_2\rangle \cong \langle c, c', b_2\rangle,$$

so using transitivity for $n \leq 3$ (again!) exists a_1, c_1, x such that

$$\langle a', b_1\rangle \cong \langle a_1, x\rangle,\ \langle c', b_2\rangle \cong \langle c_1, x\rangle \text{ and } \langle a, a_1\rangle \cong \langle c, c_1\rangle.$$

Take $\beta = \langle x\rangle \oplus \alpha$. Then

$$\varphi' = \langle a'\rangle \oplus \tau \cong \langle a', b_1\rangle \oplus \alpha \cong \langle a_1, x\rangle \oplus \alpha = \langle a_1\rangle \oplus \beta$$

and

$$\theta' = \langle c'\rangle \oplus \sigma \cong \langle c', b_2\rangle \oplus \alpha \cong \langle c_1, x\rangle \oplus \alpha = \langle c_1\rangle \oplus \beta.$$

Thus by induction, $\varphi' \cong \langle a_1\rangle \oplus \alpha$ and $\theta' \cong \langle c_1\rangle \oplus \alpha$. Since $\langle a, a_1\rangle \cong \langle c, c_1\rangle$, this implies $\varphi \cong \theta$, as desired. □

Lemma 3.1.12. *For arbitrary forms φ, ψ, ψ' over G, $\psi \cong \psi' \Leftrightarrow \varphi \oplus \psi \cong \varphi \oplus \psi'$.*

Proof. By induction, we can assume φ is one dimensional, say $\varphi := \langle a_1 \rangle$.

($\Rightarrow$) let $\psi = \langle x, c_3, ..., c_n \rangle$ and $\psi' = \langle y, d_3, ..., d_n \rangle$. Then

$$\begin{aligned} \langle a_1, x \rangle &\cong \langle a_1, x \rangle \\ \langle x, c_3, ..., c_n \rangle &\cong \langle x, c_3, ..., c_n \rangle \\ \langle y, d_3, ..., d_n \rangle &\cong \langle x, c_3, ..., c_n \rangle. \end{aligned}$$

Therefore, $\langle a_1 \rangle \oplus \psi \cong \langle a_1 \rangle \oplus \psi'$ by definition of isometry (take $x = y$ and $z_j = c_j$, $j = 3, ..., n$).

($\Leftarrow$) By definition of isometry, exists $a, b, c_3, ..., c_n$ such that $\psi \cong \langle a, c_3, ..., c_n \rangle$, $\psi' \cong \langle b, c_3, ..., c_n \rangle$ and $\langle a_1, a \rangle \cong \langle a_1, b \rangle$ (remember the induction step!). Comparing discriminants, this yields $a = b$, so $\psi \cong \langle a, c_3, ..., c_n \rangle \cong \psi'$. Thus $\psi \cong \psi'$. □

Proposition 3.1.13 (Witt's Cancellation)**.** *Suppose $\varphi, \varphi', \psi, \psi'$ are forms over G satisfying $\varphi \cong \varphi'$. Then $\psi \cong \psi' \Leftrightarrow \varphi \oplus \psi \cong \varphi' \oplus \psi'$.*

Proof. Since $\varphi \cong \varphi'$, it follows from lemma 3.1.12 and 3.1.10(a) that $\varphi \oplus \varphi' \cong \psi \oplus \psi$. Thus

$$\varphi \oplus \psi \cong \varphi' \oplus \psi' \Leftrightarrow \varphi' \oplus \psi \cong \varphi' \oplus \psi' \Leftrightarrow \psi \cong \psi'$$

by lemma 3.1.12. □

Corollary 3.1.14. *If $\langle a, b \rangle \cong \langle c, d \rangle$ then $\langle a, -c \rangle \cong \langle -b, d \rangle$.*

Proof. From $\langle a, b \rangle \cong \langle c, d \rangle$, applying 3.1.12, 3.1.13 and 3.1.10 we get:

$$\begin{aligned} \langle a, b \rangle \cong \langle c, d \rangle &\Rightarrow \langle a, b \rangle \oplus \langle -b, -c \rangle \cong \langle c, d \rangle \oplus \langle -b, -c \rangle \\ &\Rightarrow \langle a, b, -b, -c \rangle \cong \langle c, d, -b, -c \rangle \\ &\Rightarrow \langle a, -c \rangle \oplus \langle b, -b \rangle \cong \langle -b, d \rangle \oplus \langle c, -c \rangle \\ &\Rightarrow \langle a, -c \rangle \oplus \langle 1, -1 \rangle \cong \langle -b, d \rangle \oplus \langle 1, -1 \rangle \\ &\Rightarrow \langle a, -c \rangle \cong \langle -b, d \rangle. \end{aligned}$$

□

Proposition 3.1.15. *If $\varphi, \psi, \varphi', \psi'$ are forms over G with $\varphi \cong \varphi'$ and $\psi \cong \psi'$, then $\varphi \otimes \psi \cong \varphi' \otimes \psi'$.*

Proof. If $\varphi = \langle a_1, ..., a_n \rangle$, then by 3.1.10(d) and 3.1.13

$$\varphi \otimes \psi \cong a_1\psi \oplus ... \oplus a_n\psi \cong a_1\psi' \oplus ... \oplus a_n\psi' \cong \varphi \otimes \psi'.$$

Similarly $\varphi \otimes \psi' \cong \varphi' \otimes \psi'$, so $\varphi \otimes \psi \cong \varphi' \otimes \psi'$. □

We say a form φ of dimension n *represents* $x \in G$ if there exist $x_2, ..., x_n \in G$ such that $\varphi \cong \langle x, x_2, ..., x_n \rangle$. We denote by $D(\varphi)$ the set of elements $x \in G$ represented by φ in this sense. In the field-theoretic case elements represented by $\varphi \cong \langle a_1, ..., a_n \rangle$ are also expressible in terms of $a_1, ..., a_n$ using the operations of F. The following result provide an analogous in the abstract situation:

Proposition 3.1.16. *If φ and ψ are arbitrary forms over G, then*

$$D(\varphi \oplus \psi) = \bigcup \{D\langle x, y \rangle : x \in D(\varphi),\ y \in D(\psi)\}.$$

Proof. Let $\varphi = \langle a_1, ..., a_k\rangle$, $\psi = \langle a_{k+1}, ..., a_n\rangle$. For the inclusion $\supseteq$, let

$$z \in \bigcup\{D\langle x, y\rangle : x \in D(\varphi),\, y \in D(\psi)\}.$$

Then, there exists $x \in D(\varphi)$, $y \in D(\psi)$ such that $z \in D(x, y)$. By definition of representation, there exists $w, x_2, ..., x_k, y_{k+2}, ..., y_n$ such that

$$\begin{aligned}\langle z, w\rangle &\cong \langle x, y\rangle\\ \varphi &\cong \langle x, x_2, ..., x_k\rangle\\ \psi &\cong \langle y, y_{k+2}, ..., y_n\rangle.\end{aligned}$$

By proposition 3.1.13 and the properties in proposition 3.1.10, we have

$$\begin{aligned}\varphi \oplus \psi &\cong \langle x, x_2, ..., x_k, y, y_{k+2}, ..., y_n\rangle\\ &\cong \langle x, y, x_2, ..., x_k, y_{k+2}, ..., y_n\rangle\\ &\cong \langle z, w, x_2, ..., x_k, y_{k+2}, ..., y_n\rangle.\end{aligned}$$

Then $z \in D(\varphi \oplus \psi)$.

To prove $\subseteq$, let $b_1 \in D(\varphi \oplus \psi)$. Thus, exists $b_2, ..., b_n \in G$ such that $\varphi \oplus \psi \cong \langle b_1, b_2, ...b_n\rangle$. Choose $a, b, c_3, ..., c_n$ as witness of this isometry. Thus $b_1 \in D(a_1, a)$. This completes the proof if $k = 1$ (take $x = a_1$, $y = a$). If $k \geq 2$, by induction on k, exists $x' \in D(a_2, ..., a_k)$, $y \in D(\psi)$ such that $a \in D(x', y)$. Thus

$$b_1 \in D(a_1, a) \subseteq D(a_1, x', y) = D(y, a_1, x'),$$

so by the case $k = 1$, exists $x \in D(a_1, x')$ such that $b_1 \in D(y, x) = D(x, y)$. Since $D(a_1, x) \subseteq D(\varphi)$, this completes the proof. □

Corollary 3.1.17. *Suppose $\varphi_1, ..., \varphi_n$ are forms over G. Then*

$$D(\varphi_1 \oplus ... \oplus \varphi_n) = \bigcup\{D\langle x_1, ..., x_n\rangle : x_1 \in D(\varphi),\, \forall\, i = 1, ..., n\}.$$

Proof. Is just an application of induction on proposition 3.1.16. □

Note that $\langle a, -a\rangle \cong \langle 1, -1\rangle$ for all $a \in G$, since $q(a, -a) = 0 = q(1, -1)$. Any form $\langle a, -a\rangle$, $a \in G$ will be called a *hyperbolic form*. A form φ will be called *isotropic* if there exist a form ψ such that $\varphi \cong \langle 1, -1\rangle \oplus \psi$. Otherwise f will be called *anisotropic*. A form is said to be *universal* if $D(\varphi) = G$.

Corollary 3.1.18. *Let φ, ψ be forms over G. Then $\varphi \oplus \psi$ is isotropic iff there exist $x \in D(\varphi)$ such that $-x \in D(\psi)$.*

Proof. ($\Rightarrow$) suppose $\varphi \oplus \psi \cong \langle 1, -1\rangle \oplus \theta$. Decompose $\varphi = \langle a\rangle \oplus \varphi'$. Then

$$\langle a\rangle \oplus \varphi' \oplus \psi \cong \varphi \oplus \psi \cong \langle 1, -1\rangle \oplus \theta \cong \langle a, -a\rangle \oplus \theta,$$

so by Witt's cancellation, $\varphi' \oplus \psi \cong \langle -a\rangle \oplus \theta$. Suppose $\dim(\varphi') \geq 1$. Then, by proposition 3.1.16, exists $b \in D(\psi)$, $c \in D(\varphi')$, $d \in G$ such that $\langle b, c\rangle \cong \langle -a, d\rangle$. Adding $\langle a, -b\rangle$ to both sides, and cancelling the hyperbolic forms yields $\langle a, c\rangle \cong \langle -b, d\rangle$. Thus $-b \in D(a, c) \subseteq D(\varphi)$, i.e, $x = -b$ satisfies the required conditions. If, on the other hand, $\dim(\varphi') = 0$, then $x = a$ works.

($\Leftarrow$) If $\varphi \cong \langle x \rangle \oplus \varphi'$ and $\psi \cong \langle -x \rangle \oplus \psi'$ then

$$\varphi \oplus \psi \cong \langle x, -x \rangle \oplus \varphi' \oplus \psi' \cong \langle 1, -1 \rangle \oplus \varphi' \oplus \psi'.$$

□

Can be useful keep in mind the following special subcase of the above corollary:

Corollary 3.1.19. *Let φ be a form over G and let $a \in G$. Then $a \in D(\varphi) \Leftrightarrow \langle -a \rangle \oplus \varphi$ is isotropic.*

3.1.3 The Witt Ring of a Q-structure

Here, we have the same situation of the chapter 1: the set of equivalence classes of forms over G with respect to the equivalence relation $\cong$ (isometry) with the operations of sum and product on forms induce binary operations on this set. The resulting structure is "almost" a ring, except for the fact that additive inverses fail to exist. To rectify this situation, we got to a slightly coarser equivalence relation called Witt equivalence. For φ a form over G, and an integer $n \geq 0$ we define $n\varphi = \varphi \otimes ... \otimes \varphi$ (n times) (with the convention $0\varphi = 0$, the 0-dimensional form). Now, we say two forms φ, ψ over G (not necessarily of the same dimension) are **Witt equivalent**, denote $\varphi \sim \psi$, if there exist non-negative integers k, l such that $\varphi \otimes k\langle 1, -1 \rangle \cong \psi \otimes l\langle 1, -1 \rangle$. Could be fruitful compare the Witt equivalence with the construction in section 1.3.

Of course, a direct consequence of the definition of Witt equivalence is that this relation is an equivalence relation. Another consequence is the follow: suppose $\varphi \sim \varphi'$, $\psi \sim \psi'$ and $a \in G$. Then $\varphi \oplus \psi \sim \varphi' \oplus \psi'$, $a\varphi \sim a\varphi'$ and $\varphi \otimes \psi \sim \varphi' \otimes \psi'$.

Let R be the set of equivalence classes of forms with respect to Witt equivalence. The sum and product of forms induces binary operations on R. Defining on R the prescriptions $0 := \langle 1, -1 \rangle$, $1 := \langle 1 \rangle$ and $-\langle a_1, ..., a_n \rangle := \langle -a_1, ..., -a_n \rangle$, we have that R is a commutative ring with unity. This ring is called *the Witt ring associated to the Q-structure* (G, Q, q). In the field case, this construction coincide with the Witt ring of a field. In fact, this provides an alternative way to define the Witt ring of a field.

The following proposition shows how to recover the concepts of isometry and isotropy from Witt equivalence:

Proposition 3.1.20.

a - $\varphi \cong \psi \Leftrightarrow \varphi \sim \psi$ *and* $dim(\varphi) = dim(\psi)$.

b - φ *is isotropic* $\Leftrightarrow$ *there exist a form* ψ *with* $\varphi \sim \psi$ *and* $dim(\varphi) > dim(\psi)$.

Proof.

a - ($\Rightarrow$) is just the definition of Witt equivalence. ($\Leftarrow$) suppose $\varphi \oplus k\langle 1, -1 \rangle \cong \psi \oplus l\langle 1, -1 \rangle$. Comparing dimensions and using $\dim(\varphi) = \dim(\psi)$, this yields $k = l$. Thus $\varphi \cong \psi$ by Witt's cancellation.

b - ($\Rightarrow$) is just the definition of isotropy. ($\Leftarrow$) suppose $\varphi \oplus k\langle 1, -1 \rangle \cong \psi \oplus l\langle 1, -1 \rangle$. Then comparing dimensions and using $\dim(\varphi) > \dim(\psi)$ yields $k < l$. Thus, by Witt's cancellation, $\varphi \cong \psi \oplus (l - k)\langle 1, -1 \rangle$ so φ is isotropic.

□

Observe that any form φ over G decomposes as $\varphi \cong \varphi_{an} \oplus k\langle 1, -1 \rangle$ with $k \geq 0$ and with φ_{an} a (possibly 0-dimensional) anisotropic form. To obtain such a decomposition, just keep extracting terms $\langle 1, -1 \rangle$ until it is no longer possible.

Corollary 3.1.21. *Suppose* $\varphi \cong \varphi_{an} \oplus k\langle 1,-1\rangle$ *and* $\psi \cong \psi_{an} \oplus l\langle 1,-1\rangle$ *with* $k,l \geq 0$ *and* φ_{an}, ψ_{an} *anisotropic. Then* $\varphi \sim \psi \Rightarrow \varphi_{an} \cong \psi_{an}$.

Proof. Observe that $\varphi \sim \varphi_{an}$, and $\psi \sim \psi_{an}$, so $\varphi \sim \psi \Leftrightarrow \varphi_{an} \sim \psi_{an}$.Thus, we must verify $\varphi_{an} \sim \psi_{an} \Leftrightarrow \varphi_{an} \cong \psi_{an}$. ($\Leftarrow$) is just the definition of Witt equivalence. For ($\Rightarrow$), suppose $\varphi_{an} \sim \psi_{an}$. Since φ_{an} is anisotropic, by 3.1.20(b) $\dim(\varphi_{an}) \leq \dim(\psi_{an})$. Similarly, $\dim(\psi_{an}) \leq \dim(\varphi_{an})$, since ψ_{an} is anisotropic. Thus $\dim(\varphi_{an}) = \dim(\psi_{an})$, so $\varphi_{an} \cong \psi_{an}$ by 3.1.20(a). □

We refer to φ_{an} (notation as above) as the **anisotropic part** of φ. The non-negative integer k is referred to as the **Witt index** of φ.

Note it follows from corollary 3.1.21 that if φ and ψ are already anisotropic, then $\varphi \sim \psi \Leftrightarrow \varphi \cong \psi$. Since each element of R is representable by an anisotropic form, R (as a set) can be identified with the set of isometry class of anisotropic forms. Some care must be taken in doing this, however, since the sum and product of anisotropic forms need not be anisotropic.

3.1.4 Pfister forms, fundamental ideal and Arason-Pfister property

We already know that Pfister forms are central for quadratic forms on the field case. Here, we will want to reproduce this concepts in the abstract case. Again, we will work on a fixed Q-structure (G,Q,q).

A k-folded *Pfister form* is a form of the type

$$\varphi : \langle\langle a_1,...,a_n\rangle\rangle := \otimes_{i=1}^{k}\langle 1,a_i\rangle \text{ with } a_1,...,a_k \in G \text{ and } k \geq 0.$$

A form φ over G is said to be *round* if the elements of G represented by φ are just the elements $a \in G$ satisfying $a\varphi \cong \varphi$ ($1\varphi = \varphi \Rightarrow 1 \in D(\varphi)$). Since $D(a\varphi) = aD(\varphi)$, one sees if φ is round then $aD(\varphi) = D(\varphi)$ for all $a \in D(\varphi)$, i.e, $D(\varphi)D(\varphi) = D(\varphi)$. This implies the set $D(\varphi)$ is a subgroup of G if φ is round.

Proposition 3.1.22. *Every Pfister form is round.*

Proof. Let $\varphi = \langle\langle a_1,...,a_k\rangle\rangle$, $a_1,...,a_k \in G$. Expanding the products that define φ, we see $1 \in D(\varphi)$. Now suppose $a \in D(\varphi)$. If $k=0$, $\varphi = \langle 1\rangle$ so $a=1$ and $a\varphi \cong \varphi$ is immediate. Now suppose $k \geq 1$. Thus $\varphi \cong \langle 1,a_1\rangle \otimes \psi \cong \psi \oplus a_1\psi$, where $\psi = \langle\langle a_2,...,\rangle\rangle$. By 3.1.16, exists $c,d \in D(\psi)$ with $a \in D(c,a_1d)$. Comparing discriminants, this yields $\langle c,a_1d\rangle \cong \langle a,a_1acd\rangle$. Also $c\psi \cong \psi$ and $d\psi \cong \psi$ by induction on k. It follows that $cd\psi \cong \psi$. Thus

$$a\varphi \cong a(\psi \oplus a_1\psi) \cong a(\psi \oplus a_1cd\psi) \cong \langle a,aa_1cd\rangle \otimes \psi \cong \langle c,a_1d\rangle \otimes \psi \cong c\psi \oplus a_1d\psi \cong \psi \oplus a_1\psi \cong \varphi.$$

□

Corollary 3.1.23. *If* φ *is a Pfister form, then* $D(\varphi)$ *is a subgroup of* G.

Proposition 3.1.24. *Suppose* φ *is a* k*-fold Pfister form,* $k \geq 1$*, that* φ' *is defined by* $\varphi \cong \langle 1\rangle \oplus \varphi'$*, and* $x \in D(\varphi')$*. Then there exist* $x_1,...,x_k \in G$ *with* $x_1 = x$ *and* $\varphi \cong \otimes_{i=1}^{k}\langle 1,x_i\rangle$.

Proof. If $k=1$ this is immediate since $\varphi' = \langle x\rangle$. Suppose $\varphi = \langle\langle a_1,...,a_k\rangle\rangle$, $k \geq 2$. Thus

$$\varphi = \langle 1,a_1\rangle \otimes \psi \cong \psi \oplus a_1\psi$$

so $\varphi' \cong \psi' \oplus a_1\psi$. Here $\psi' = \langle\langle a_2,...,a_k\rangle\rangle$ and ψ' is defined by $\psi \cong \langle 1\rangle \oplus \psi'$. By 3.1.16, exists $y \in D(\psi')$, $z \in D(\psi)$ such that $x \in D(y,a_1z)$. Thus, by 3.1.22, $z\psi \cong \psi$, and by induction on k,

$\psi \cong \langle 1, y\rangle \otimes ....$ Also, $\langle y, a_1 z\rangle \cong \langle x, a_1 xyz\rangle$, so

$$\begin{aligned}\varphi &\cong \psi \oplus a_1\psi \cong \psi \oplus a_1 z\psi \cong \langle 1, a_1 z\rangle \otimes \langle 1, y\rangle \otimes ... \\ &\cong \langle 1, y, a_1 z, a_1 yz\rangle \otimes ... \cong \langle 1, x, a_1 xyz, a_1 yz\rangle \otimes ... \cong \langle 1, x\rangle \otimes \langle 1, a_1 yz\rangle \otimes ... .\end{aligned}$$

□

Corollary 3.1.25. *If φ is a Pfister form which is isotropic, then $\varphi \sim 0$*[2].

Proof. By assumption, $\varphi \cong \langle 1, -1\rangle \oplus ...$, so $\varphi' \cong \langle -1\rangle \oplus ...$, i.e, $-1 \in D(\varphi')$, so by 3.1.24, $\varphi \cong \langle 1, -1\rangle \otimes ... \sim 0$. □

Now, we will work on the fundamental ideal. The argument here is basic the same of the arguments preceeding proposition 1.3.11.

It is a direct consequence of the definition of Witt equivalence that for arbitrary forms φ, ψ over G, $\varphi \sim \psi \Rightarrow \dim(\varphi) \cong \dim(\psi) \pmod 2$. The *modulo 2 dimension* of a form φ is defined by $\dim_2(\varphi) = \dim(\varphi) + 2\mathbb{Z} \in \mathbb{Z}/2\mathbb{Z}$. Thus $\dim_2$ is an invariant with respect to Witt equivalence, and hence defines a ring homomorphism $\dim_2 : R \to \mathbb{Z}/2\mathbb{Z}$. The kernel of $\dim_2$ is the *fundamental ideal of R*, denoted by I.

Note that every even dimensional form is a sum of two dimensional forms. Also, $\langle a, b\rangle \sim \langle 1, a\rangle \oplus -\langle 1, -b\rangle$ for all $a, b \in G$. It follows that I is generated, as an additive group, by the set of 1-fold Pfister forms. Thus the k-th power ideal I^k is additively generated by the k-fold Pfister forms.

Proposition 3.1.26. *Let $k \geq 1$. Then the following are equivalent:*

a - $I^k = 0$.

b - $\varphi \sim 0$ *for all k-fold Pfister form φ.*

c - φ *is isotropic for all k-fold Pfister form φ.*

d - φ *is universal for all $(k-1)$-fold Pfister form φ.*

Proof. (a)⇔(b) and (b)⇒(c) is immediate from definitions involved. (c)⇒(b) follows from 3.1.25.

(b)⇒(d): let φ be a $(k-1)$-fold Pfister form and let $a \in G$. Then $\varphi \otimes \langle 1, -a\rangle \sim 0$ by (b), i.e, $\varphi \cong a\varphi$. Thus by 3.1.22, $a \in D(\varphi)$.

(d)⇒(b): let $\varphi = \langle\langle a_1, ..., a_k\rangle\rangle$ and $\psi = \langle\langle a_1, ..., a_{k-1}\rangle\rangle$. Then $-a_k \in D(\psi)$ by (d), so $-a_k\psi \cong \psi$ by 3.1.22. Thus $\varphi \cong \langle 1, a_k\rangle \otimes \psi \sim 0$. □

Corollary 3.1.27. *a* - $I = 0 \Leftrightarrow G = 1$.

b - $I^2 = 0 \Leftrightarrow Q = 0$.

Proof.

a - By 3.1.26, $I = 0 \Leftrightarrow \langle 1\rangle$ is universal. Since $D(1) = \{1\}$, this in turn, is equivalent to $G = 1$.

b - If $I^2 = 0$, then every 1-fold Pfister form is universal, so in particular $a \in D(1, ab)$ for all $a, b \in G$. Comparing discriminants, $\langle 1, ab\rangle \cong \langle a, b\rangle$ so $q(a, b) = q(1, ab) = 0$. Since this os true for all $a, b \in G$, this implies $Q = 0$. Now suppose $q(a, b) = 0$ for all $a, b \in G$. Thus $\langle 1, ab\rangle \cong \langle a, b\rangle$ so $\langle 1, -a, -b, ab\rangle \sim 0$ i.e, $\langle 1, -a\rangle \oplus \langle 1, -b\rangle \sim 0$ for all $a, b \in G$. This shows $I^2 = 0$.

[2]The notation $\varphi \sim 0$ means the class of φ in the Witt ring is 0, i.e, φ is isometric to a sum of hyperbolic forms.

□

Note that for all $a, b \in G$,

$$\langle 1, -a\rangle \oplus \sim \langle 1, -ab\rangle \oplus \langle 1, -a\rangle \otimes \langle 1, -b\rangle.$$

It folows that the mapping $\alpha : G \to I/I^2$ defined by $\alpha(a) = \langle 1, -a\rangle + I^2$ is a homomorphism from the (multiplicative) group G to the additive group I/I^2. Since the 1-fold Pfister forms generate I, this mapping is, in fact, surjective. We wish to show that α is an isomorphism. For this purpose it is useful to introduce the "signed" discriminant.

First note that the usual discriminant is not invariant with respect to Witt equivalence. To rectify this, we define the **signed discriminant** of a form $\varphi = \langle a_1, ..., a_n\rangle$ to be

$$\mathrm{disc}_\pm(\varphi) = (-1)^{n(n-1)/2}\mathrm{disc}(\varphi) = (-1)^{n(n-1)/2}a_1a_2...a_n \in G.$$

Proposition 3.1.28.

a - If $\dim(\varphi) = n$, $\dim(\psi) = m$, *then* $disc_\pm(\varphi \oplus \psi) = (-1)^{mn} disc_\pm(\varphi) disc_\pm(\psi)$.

b - If $\varphi \sim \psi$ *then* $disc_\pm(\varphi) = disc_\pm(\psi)$.

Proof.

a - $\dim(\varphi \oplus \psi) = n + m$ and $\mathrm{disc}(\varphi \oplus \psi) = \mathrm{disc}(\varphi)\mathrm{disc}(\psi)$. The result now follows by noting that

$$\frac{(m+n)(m+n-1)}{2} = \frac{m(m-1)}{2} + \frac{n(n-1)}{2} + mn.$$

b - In view of 3.1.10(b), we need only to show that $\mathrm{disc}_\pm(\varphi \oplus \langle 1, -1\rangle) = \mathrm{disc}_\pm(\varphi)$, but this is an immediate consequence of (a).

□

It follows from 3.1.28(b) that the signed discriminant induces a mapping $\mathrm{disc}_\pm : R \to G$. By 3.1.28(a), the restriction of this mapping to I is a group homomorphism. Note that if $a, b \in G$, then $\mathrm{disc}_\pm(\langle 1, a\rangle \otimes \langle 1, b\rangle) = \mathrm{disc}_\pm(\langle 1, a, b, ab\rangle) = 1$ by direct computation. Sice the 2-fold Pfister forms generate I^2 it follows $\mathrm{disc}_\pm(I^2) = 1$, so $\mathrm{disc}_\pm$ induces a group homomorphism $\beta : I/I^2 \to G$ defined by $\beta(\varphi + I^2) = \mathrm{disc}_\pm(\varphi)$. Finally, if $a \in G$, then

$$(\beta\alpha)(a) = \beta(\alpha(a)) = \beta(\langle 1, -a\rangle + I^2) = \mathrm{disc}_\pm(1, -a) = a$$

so $\beta\alpha = id$. On the other hand,

$$(\alpha\beta)(\langle 1, a\rangle + I^2) = \alpha(\beta(\langle 1, a\rangle + I^2)) = \alpha(-a) = \langle 1, a\rangle + I^2$$

and $\alpha\beta = id$. Thus α is an isomorphism with inverse β. This proves the following:

Proposition 3.1.29. $I/I^2 \cong G$ *canonically.*

Moreover, from the fact that β is the inverse of α we obtain

Corollary 3.1.30. *For* $\varphi, \psi \in R$, $\varphi \equiv \psi \ mod\ I^2 \Leftrightarrow \dim_2(\varphi) = \dim_2(\psi)$ *and* $disc_\pm(\varphi) = disc_\pm(\psi)$.

In section 1.11, we studied the Witt ring of a field in terms of the filtration

$$R \supseteq I \supseteq I^2 \supseteq ... \supseteq I^k \supseteq ...$$

determined by the fundamental ideal I. Unfortunately, the proof of Hauptsatz depends on a certain methods which is available only in the field case. We can, at least, proceed axiomatically as follows. Let us say that *the quaternionic structure* (G, Q, q) *satisfies* $AP(k)$ if $f = \langle a_1, ..., a_n \rangle \in R$, $f \in I^k$ and $n < 2^k \Rightarrow f \sim 0$. With this terminology we can prove:

Proposition 3.1.31. *$AP(0)$, $AP(1)$ and $AP(2)$ holds for any Q-structure.*

Proof. $AP(0)$ and $AP(1)$ are trivial statements. To prove $AP(2)$ suppose $\varphi \in I^2$, $\dim(\varphi) < 4$ (thus $\dim(\varphi) = 0$ or 2). By 3.1.30, φ is even dimensional and $\text{disc}_{\pm}(\varphi) = 1$. Disregarding the trivial case, we may assume $\varphi = \langle a, b \rangle$. Thus $1 = \text{disc}_{\pm}(\varphi) = -ab$, so $b = -a$. Thus $\varphi = \langle a, -a \rangle \sim 0$. □

However, we generally have the following problem for arbitrary Q-structures:

Given a arbitrary Q-structure, does $AP(k)$ hold for all $k \geq 3$?

3.2 Abstract Witt Rings

We provide a brief account on the abstract Witt rings, as in the chapter 4 of [Mar80]. Unfortunately, we just compute the equivalence of this abstract Witt rings with the Witt rings of a quaternionic structure (and of course, the classical Witt ring of a field). Most of its interesting application, including an approach to the Representation Problem posed in 2.8 are ommited. The reader could consult this in [Mar80].

But even though this section is an introdutory one, we can note the simplification of the language that the abstract Witt rings provides in deal with the study of its ring-theoretic aspects.

Suppose, to begin, that R is the Witt ring of a Q-structure (G, Q, q). Suppose $a, b \in G$. Then by proposition 3.1.20, and the definition of isometry, $\langle a \rangle \sim \langle b \rangle \Leftrightarrow \langle a \rangle \cong \langle b \rangle \Leftrightarrow a = b$. Thus we may identify G with a subset $G_R \subseteq R$. This identifies $1 \in G$ with the unity $1 \in R$ and the distinguished element $-1 \in G$ with $-1 \in R$ (where, as usual in a ring, $-r$ denotes the additive inverse of r). Since $\langle a \rangle \otimes \langle b \rangle \cong \langle ab \rangle$, G_R is a subgroup of the multiplicative group $\dot{R}$ of R, and $G \cong G_R$ as groups. Since every form is expressible as the sum of 1-dimensional forms, it follows that G_R generates R as an additive group. With this as motivation, we define an (abstract) Witt ring:

Definition 3.2.1. *An abstract Witt ring is a pair (R, G_R) where R is a non-trivial commutative ring with unity 1 ($0 \neq 1$), and G_R is a subgroup of the multiplicative group $\dot{R}$ which has exponent 2 and contains -1. We assume:*

W1 - *G_R generates R additively.*

Since $-1 \in G_R$, this is the same as assuming that every element of R is of the form $r = a_1 + ... + a_n$, with $a_1, ..., a_n \in G_R$, and $n \geq 1$. We let I_R denote the ideal of R generated by elements $r \in R$ of the form $r = a + b$ with $a, b \in G_R$. This is the fundamental ideal of R, and we can consider the Arason-Pfister property

$$AP(k): \text{ If } r = a_1 + ... + a_n \in I^k, \text{ with } n < 2^k, \text{ then } r = 0.$$

It is not quite clear what "should" be assumed concerning $AP(k)$. However, we do assume

W2 - *$AP(0)$, $AP(1)$ and $AP(2)$ holds for R.*

Finally, we assume

W3 - *If* $a_1 + ... + a_n = b_1 + ... + b_n$ *and* $n \geq 3$, *then there exist* $a, b, c_3, ..., c_n \in G_R$ *such that* $a_2 + ... + a_n = a + c_3 + ... + c_n$, $a_1 + a = b_1 + b$ *(and hence* $b_2 + ... + b_n = b + c_3 + ... + c_n$*).*

When the context is clear, we will refer to abstract Witt rings just by Witt rings.

Note that the Witt ring associated to a Q-structure is an example of abstract Witt ring (see 3.1.20(a), 3.1.31 and the definition of isometry in a Q-structure). The aim of this section is to proof the converse is also true.

For $r = a_1 + ... + a_r \in R$, we define the *modulo-2 dimension* and the *signed discriminant* of r by $\dim_2(r) = n + 2\mathbb{Z} \in \mathbb{Z}/2\mathbb{Z}$ and $\text{disc}_\pm(r) = (-1)^{n(n-1)/2} a_1 ... a_n \in G_R$. It is necessary to verify:

Proposition 3.2.2. $\dim_2 : R \to \mathbb{Z}/2\mathbb{Z}$ *and* $disc_\pm : R \to G_R$ *are well-defined.*

Proof. By $AP(1)$, $G_R \cap I_R = \emptyset$. From this, it follows that

$$a_1 + ... + a_n = b_1 + ...b_m \Rightarrow n \equiv m \bmod 2$$

thus $\dim_2$ is well-defined. Now, we wish to show that

$$a_1 + ... + a_n = b_1 + ... + b_m \Rightarrow (-1)^{n(n-1)/2} a_1 ... a_n = (-1)^{m(m-1)/2} b_1 ... b_m.$$

By adding enough terms of the form $1 + (-1)$ we are reduced to the case $m = n$. Since the case $m = n = 1$ is immediate, let $n = 2$. In this case, $a_1 + a_2 = b_1 + b_2$ so

$$\begin{aligned}(a_1 - b_1)(a_1 + a_2) &= a_1(a_1 + a_2) - b_1(b_1 + b_2) = a_1^2 + a_1 a_2 - b_1^2 - b_1 b_2 \\ &= 1 + a_1 a_2 - 1 - b_1 b_2 = a_1 a_2 - b_1 b_2.\end{aligned}$$

Thus $a_1 a_2 - b_1 b_2 \in I_R^2$, so by $AP(2)$, $a_1 a_2 = b_1 b_2$. Now suppose $n \geq 3$. Choose $a, b, c_3, ..., c_n$ as in W3. Then by induction on n,

$$a_1 a_2 ... a_n = a_1 a c_3 ... c_n = b_1 b c_3 ... c_n = b_1 b_2 ... b_n,$$

completing the proof. □

Now, suppose that R is the Witt ring of some Q-structure (G, Q, q), and that G is identified with a subgroup of $\dot{R}$ in the canonical way. Then for $a, b \in G$, the element $(1 - a)(1 - b) \in R$ is just the equivalence class of the 2-fold Pfister form $\langle\langle a, b\rangle\rangle \cong \langle 1, -a, -b, ab\rangle$. It follows, using proposition 3.1.20, Witt cancellation, and 3.1.10(e), that for $a, b, c, d \in G$,

$$(1 - a)(1 - b) = (1 - c)(1 - d) \Leftrightarrow q(a, b) = q(c, d).$$

For R an arbitrary Witt ring we define Q_R to be the subset of R consisting of all elements $(1 - a)(1 - b)$, $a, b \in G_R$. The mapping $q_R : G_r \times G_R \to Q_R$ is defined by $q_R(a, b) = (1 - a)(1 - b)$. we take -1 as the distinguished element of G_R, and $0 = q_R(1, 1)$ as the point of Q_R.

Proposition 3.2.3. *For any Witt ring* R, (G_R, Q_R, q_R) *is a* Q*-structure.*

Proof. Q1 is immediate. For Q2, note that $(1 - a)(1 - a) = 1 - a^2 = 1 - 1 = 0$. Concerning Q_3,

$$\begin{aligned}(1 - a)(1 - bc) = 0 &\Leftrightarrow b(1 - a)(1 - bc) = 0 \Leftrightarrow (1 - a)(b - c) = 0 \\ &\Leftrightarrow (1 - a)(1 - 1 + b - c) = 0 \\ &\Leftrightarrow (1 - a)(1 - b) = (1 - a)(1 - c).\end{aligned}$$

To prove Q4, assume $(1-a)(1-b) = (1-c)(1-d)$, with $a, b, c, d \in G_R$. Expanding and cancelling, this yields $-a - b + ab = -c - d + cd$. By W3, exists $p, q, r \in G_R$ such that $-b + ab = p + r$, $-a + p = -c + q$, and $-d + cd = q + r$. Take $x = -r$. Comparing signed discriminants, this yields $p = ax$, $q = cx$. Thus

$$\begin{aligned}(1-a)(1-b) &= 1 - a - b + ab = 1 - a + p + r \\ &= 1 - a + ax - x = (1-a)(1-x).\end{aligned}$$

Similarly, $(1-c)(1-d) = (1-c)(1-x)$. This completes the proof. □

We now obtain a result describing R as quotient of the integral group ring $\mathbb{Z}[G_R]$. By W_1, there is a natural surjetive ring homomorphism $\phi : \mathbb{Z}[G_R] \to R$. We denote by $[a]$ the element $a \in G_R$ viewed as an element of $\mathbb{Z}[G_R]$ (this notation is introduced to avoid confusing elements of $\mathbb{Z}[G_R]$ with elements of R). Thus $\phi([a]) = a$ for all $a \in G_R$. Hence there is an exact sequence

$$0 \longrightarrow J_R \longrightarrow \mathbb{Z}[G_R] \xrightarrow{\phi} R \longrightarrow 0$$

where J_R denotes the kernel of ϕ, so $R \cong \mathbb{Z}[G_R]/J_R$.

Theorem 3.2.4. *J_R is generated as an ideal by the element $[1] + [-1]$ and the elements $([1] - [a])([1] - [b])$ such that $a, b \in G_R$ and $q_R(a, b) = 0$.*

Proof. Let K_R denote the ideal of $\mathbb{Z}[G_R]$ generated by $[1] + [-1]$ and the elements $[a] + [b] - [c] - [d]$ such that $a + b = c + d$ in R.

Claim 1. $K_R = J_R$. Of course, $K_R \subseteq J_R$. Thus, the claim will be estabilished if we show the reduced mapping $\overline{\phi} : \mathbb{Z}[G_R]/K_R \to R$ is injective. Since $[1] + [-1] \in K_R$, every $r \in \mathbb{Z}[G_R]$ is expressible as $r = [a_1] + ... + [a_n] \bmod K_R$ for suitable $a_1, ..., a_n \in G_R$. Thus claim 1 reduces to:

Claim 2. If $a_1 + ... + a_n = b_1 + ... + b_n$ in R, then $[a_1] + ... + [a_n] = [b_1] + ... + [b_n] \bmod K_R$. By adding suitable number of terms $1 + (-1)$, we can assume $m = n$. By definition of K_R, we can also assume $n \geq 3$. Let $a, b, c_3, ..., c_n$ be as in W3. Thus, by induction on n, these congruences holds modulo K_R:

$$\begin{aligned}[a_2] + ... + [a_n] &\equiv [a] + [c_3] + ... + [c_n], \\ [a_1] + [a] &\equiv [b_1] + [b], \\ [b_2] + ... + [b_n] &\equiv [b] + [c_3] + ... + [c_n],\end{aligned}$$

so modulo K_R, we have

$$[a_1] + [a_2] + ... + [a_n] \equiv [a_1] + [a] + [c_3] + ... + [c_n] \equiv [b_1] + [b] + [c_3] + ... + [c_n] \equiv [b_1] + ...[b_n].$$

This proves claim 2 and hence claim 1.

Now suppose $a, b, c, d \in G_R$, and $a + b = c + d$. Comparing signed discriminants, $ab = cd$. Let $x = -ab = -cd$. Thus $b = -ax$, $d = -cx$, so $a - ax = c - cx$, then $1 - x = ac - acx$ and $(1 - x)(1 - acx) = 0$, so $q_R(x, ac) = 0$. Finally, modulo the ideal generated by $[1] + [-1]$ we have these congruences

$$\begin{aligned}[a] + [b] - [c] - [d] &\equiv [a] - [ax] + [c] + [cx] \equiv [a]([1] - [x] - [ac] + [acx]) \\ &\equiv [a]([1] - [x])([1] - [ac]),\end{aligned}$$

finalizing the proof. □

At this point, we can realize that this theory try to imitate the arguments developed in section 1.3. The class of Witt rings is made into a category as follows. If R and S are Witt rings, a *morphism* $\alpha : R \to S$ is a (unitary) ring homomorphism such that $\alpha(G_R) \subseteq G_S$.

Corollary 3.2.5. *Suppose $\alpha : R \to S$ is a morphism of Witt rings. Then the restriction $\alpha : G_R \to G_S$ is a morphism of Q-structures. Conversely, each Q-structure morphism $\alpha : G_R \to G_S$ lifts uniquely to a morphism $\alpha : R \to S$.*

Proof. The first assertion follow from the definition of morphisms of Witt rings. By W1, if a morphism of the Q-structures lifts at all, then it lifts uniquely. The existence of a lifiting follows from theorem 3.2.4 using the fact that if $(1-a)(1-b) = 0$ then $(1-\alpha(a))(1-\alpha(b)) = 0$. □

Finally note that if (G, Q, q) is a Q-structure, there is a (abstract) Witt ring R with (G_R, Q_R, q_R) isomorphic to (G, Q, q) (in fact, R is the Witt ring constructed in section 3.1.3). Combining this with the results just proved, we have the following major result:

Theorem 3.2.6. *The category of Witt rings and the category of Q-structures are naturally equivalent.*

For finalizing this section, concerning about morphism of Witt rings, the exact relationship between then and ring homomorphism is not quite clear. However, it is worth pointing out the following result:

Proposition 3.2.7. *Suppose R and S are Witt rings satisfying $AP(3)$. Then R and S are isomorphic as Witt rings iff they are isomorphic as rings.*

Proof. ($\Rightarrow$) is immediate. For ($\Leftarrow$), suppose $\alpha : R \cong S$ is a ring isomorphism. Thus $\alpha(I_R)$ is an ideal of index 2 in S. Thus, if $a \in G_S$, then $a \equiv 1 \bmod \alpha(I_R)$ (since $a \notin \alpha(I_R)$). In particular, $-1 \equiv 1 \bmod \alpha(I_R)$, so $a + b \equiv 0 \bmod \alpha(I_R)$ for all $a, b \in G_S$. Thus $I_S \subseteq \alpha(I_R)$, so $I_S = \alpha(I_R)$ by maximality of I_S. Thus $\alpha(I_R)^k = I_S^k$ for all $k \geq 1$ so α induces a group isomorphism

$$\alpha_k : I_R^k / I_R^{k+1} \cong I_S^k / I_S^{k+1} \text{ for all } k \geq 1.$$

Combining the natural isomorphisms $G_R \cong I_R/I_R^2$, $G_S \cong I_S/I_S^2$ with α_1, this yields a group isomorphism $\beta : G_R \to G_S$. Note if $c \in G_R$, $\beta(c)$ is characterized as the unique element of G_S satisfying $\beta(c) \equiv \alpha(c) \bmod I_S^2$. We claim that β is an isomorphism of Q-structures. This, togheter with 3.2.5 will complete the proof. But note that the unique lifting of β may not coincide with α.

From $\alpha(-1) = -1 \in G_S$ follows $\beta(-1) = -1$. Now suppose $a, b \in G_R$ and $q_R(a, b) = 0$. We wish to show $q_S(\beta(a), \beta(b)) = 0$. Applying α to $0 = q_R(a, b) = (1-a)(1-b)$ we obtain $0 = (1-\alpha(a))(1-\alpha(b))$. Since $\beta(a) \equiv \alpha(a)$ and $\beta(b) \equiv (\alpha(b)$ modulo I_S^2, this yields

$$q_S(\beta(a), \beta(b)) = (1-\beta(a))(1-\beta(b)) \equiv (1-\alpha(a))(1-\alpha(b)) \equiv 0 \bmod I_S^3.$$

Since we are assuming $AP(3)$, this implies $q_S(\beta(a), \beta(b)) = 0$. By symmetry, we also have $q_S(\beta(a), \beta(b)) = 0 \Rightarrow q_R(a, b) = 0$. This proves the claim and hence the proposition. □

3.2.1 The local-global property of Pfister

The next natural step for this theory, is to obtain a result related to the Pfister local-global principle 1.5.1.

Let start with the basic definitions: given a witt ring R, by a *signature* of R one means a (unitary) ring homomorphism $\sigma : R \to \mathbb{Z}$. We denote by X_R the (possible empty) set of all signatures of R.

Recall $\mathbb{Z}$ is a Witt ring with $G_{\mathbb{Z}} = \{1, -1\}$. Also, if $\sigma \in X_R$, then $\sigma(G_R) \subseteq \sigma(\dot{R}) = \dot{\mathbb{Z}}$. Thus a signature of R is just a morphism $\sigma : R \to \mathbb{Z}$ of Witt rings.

Note for $a, b \in G_{\mathbb{Z}}$, $q_{\mathbb{Z}}(a, b) = 0$ except if $a = b = -1$. It follows from this observation and corollary 3.2.5 that the signatures of R correspond in a one-to-one fashion with the group homomorphisms $\sigma : G_R \to \{1, -1\}$ (i.e, *characters* of G_R) satisfying $\sigma(-1) = -1$ and $q_R(a, b) = 0 \Leftrightarrow$ either $\sigma(a) = 1$ or $\sigma(b) = 1$ for all $a, b \in G_R$. Since

$$q_R(a, b) = 0 \Leftrightarrow 1 - a = b(1 - a) \Leftrightarrow b \in D\langle 1, a\rangle,$$

replacing a by $-a$, this allows one to rephrase the last condition satisfied by σ as follows:

$$b \in D\langle 1, a\rangle \text{ and } \sigma(a) = 1 \Rightarrow \sigma(b) = 1 \text{ for all } a, b \in G_R.$$

In case F is a field of characteristic $\neq 2$, then the signatures of the Witt ring $R(F)$ correspond exactly to the orderings of F.

Proposition 3.2.8. *The set of signatures of $R(F)$ (denoted $X(F)$) and the set of orderings of F are in canonical one-to-one correspondence.*

Proof. Each ordering P of F correspond to a signature σ_P by

$$\sigma_P(a) = \begin{cases} 1 \text{ if } a \in P \\ -1 \text{ if } a \notin P \end{cases}$$

and if a signature σ is given, we recover an ordering P such that $\sigma = \sigma_P$ via $P := \{a \in \dot{F} : \sigma(a) = 1\}$. □

Theorem 3.2.9 (Pfister Local-Global Principle)**.** *Suppose $r \in R$ and $\sigma(r) = 0$ for all $\sigma \in X_R$. Then there exist $n \geq 0$ such that $2^n r = 0$.*

Let us now denote by R_t the torsion subgroup of $(R, +)$.

Corollary 3.2.10. *R_t is 2-primary. For $r \in R$, $r \in R_t \Leftrightarrow \sigma(r) = 0$ for all $\sigma \in X_R$.*

Corollary 3.2.11. *The following are equivalent:*

a - $X_R = \emptyset$.

b - $R_t = R$.

c - $char(R) > 0$.

Corollary 3.2.12. *If I_R^k is torsion-free, then $AP(k)$ holds for R.*

Corollary 3.2.13. *If I_R^3 is torsion free then $AP(k)$ holds for all $k \geq 1$.*

3.2.2 Prime Ideals, the Nilradical and Units

Theorem 3.2.14. *Let P be a prime ideal of R, $P \neq I_R$. Then $2 \notin P$ and there exists a unique $\sigma \in X_R$ such that $ker(\sigma) \subseteq P$.*

For the purpose of the next corollary we adopt the following notation: for $\sigma \in X_R$, let $P_\sigma = \ker(sigma)$. This P_σ is a prime ideal of R and $R/P_\sigma \cong \mathbb{Z}$. For $\sigma \in X_R$ and p any prime integer we let $P_{\sigma,p}$ be the unique prime ideal of R such that $P_\sigma \subseteq P_{\sigma,p}$ and $R/P_{\sigma,p} \cong \mathbb{Z}/p\mathbb{Z}$. The existence and uniqueness of $P_{\sigma,p}$ follows from $R/P_\sigma \cong \mathbb{Z}$ and the well-know ideal structure of $\mathbb{Z}$.

Corollary 3.2.15. *The prime ideals I_R, P_σ, $\sigma \in X_R$; and $P_{\sigma,p}$, $\sigma \in X_R$, p in odd prime, are all distinct and are the complete set of prime ideals of R.*

Corollary 3.2.16. *If $X_R \neq \emptyset$, then I_R is the only prime ideal of R.*

Corollary 3.2.17.

$$Nil(R) = \Big\{ R_t, \text{ if } X_R \neq \emptyset I_R, \text{ if } X_R = \emptyset.$$

Theorem 3.2.18. *a - If $X_R = \emptyset$, $\dot{R} = 1 + I_R$.*

b - If $X_R \neq \emptyset$,

$$\dot{R} = \{r \in R : \sigma(r) = \pm 1 \text{ for all } \sigma \in X_R\} = G_R(1 + R_t).$$

Corollary 3.2.19. *If R is any abstract Witt ring, then $\dot{R} = G_R(1 + Nil(R))$.*

3.2.3 Pfister quotients

If J is any ideal of R and $\overline{R} = R/J$ then we can define $G_{\overline{R}}$ to be the image of G_R in $\overline{R}$ by the natural projection. It is of interest to know when $\overline{R} = (\overline{R}, G_{\overline{R}})$ is again a Witt ring. In this section we construct an important class of quotients of this type. In particular, we show that $R/\mathrm{Nil}(R)$ is a Witt ring.

Let us fix a Pfister form $p = \langle\langle a_1, ..., a_k \rangle\rangle$ over G_R, $p \neq 0$ and let us denote the associated Pfister element $(1+a)...(1+a_k) \in R$ by $\tilde{p}$. Let us denote by $\mathrm{Ann}(\tilde{p})$ the annihilator of $\tilde{p}$ in R, that is $\mathrm{Ann}(\tilde{p}) = \{r \in R : r\tilde{p} = 0\}$. This is an ideal of R.

Lemma 3.2.20. *$Ann(\tilde{p})$ is generated as an ideal by the elements $1 - x$, $x \in D(\tilde{p})$.*

Now let $\overline{R} = R/\mathrm{Ann}(\tilde{p})$ and let $G_{\overline{R}}$ denote the image of G_R in $\overline{R}$. Note that for $a \in G_R$,

$$a \equiv 1 \bmod(\mathrm{Ann}(\tilde{p})) \Leftrightarrow (1-a)\tilde{p} = 0 \Leftrightarrow a\tilde{p} = \tilde{p} \Leftrightarrow ap = p \Leftrightarrow a \in D(p).$$

It follow $G_{\overline{R}} = R/D(p)$.

Proposition 3.2.21. *$\overline{R} = (\overline{R}, G_{\overline{R}})$ is a Witt ring.*

We will refer to the quotients $R/\mathrm{Ann}(\tilde{p})$, p an anisotropic Pfister form over G_R, as *Pfister quotients* of R. Thus we have proved that every Pfister quotient of R is a Witt ring. We will also use the term Pfister quotient to indicate a slightly more general type of quotient of R. A set $\mathcal{S}$ of anisotropic Pfister forms will be called *directed* if for all $p \in \mathcal{S}$ there is a $r \in \mathcal{S}$ such that $D(p), D(q) \subseteq D(r)$.

Now, suppose $\mathcal{S}$ is a directed set of Pfister forms and $p, q \in \mathcal{S}$ with $D(p) \subseteq D(q)$. Then by lemma 3.2.20, $\mathrm{Ann}(\tilde{p}) \subseteq \mathrm{Ann}(\tilde{q})$, so the identity map in R induces a morphism of Witt rings $R/\mathrm{Ann}(\tilde{p}) \to R/\mathrm{Ann}(\tilde{q})$. Thus we have a directed system of Witt rings and morphisms. In this situation we can always form the direct limit.

Lemma 3.2.22. *Let $\{R_i\}_{i \in I}$ be any directed system in the category of Witt rings. Then the direct limit $\varinjlim_{i \in I} R_i$ exists.*

We wish to apply this to the directed system of Witt rings arising from a directed set $\mathcal{S}$ of Pfister forms. In this case,

$$\varinjlim_{p \in \mathcal{S}} R/\mathrm{Ann}(\tilde{p}) = R/\bigcup_{p \in \mathcal{S}} D(p).$$

The associated group for this Witt ring is

$$\varinjlim_{p\in\mathcal{S}} G/D(p) = G_R/\bigcup_{p\in\mathcal{S}} D(p).$$

Such quotients of R will also be reffered to as *Pfister quotients*. One can, of course, view the previous definition as being a special case of this one where $\mathcal{S}$ is a singleton set $\{p\}$.

Now suppose $X_R \neq$. The $\mathrm{Nil}(R) = R_t \cup_{n\geq 0} \mathrm{Ann}(2^n)$. Since the system of Pfister forms $\{\langle 1,1\rangle^n : n \geq 0\}$ is directed, it follows that $\overline{R} = R/\mathrm{Nil}(R)$ is a Pfister quotient of R and hence is itself a Witt ring, with $G_{\overline{R}} = G_R/\cup_{n\geq 0} D\langle 1,1\rangle^n$. Note that $X_{\overline{R}}$ is canonically identified with X_R. On the other hand, if $X_R = \emptyset$, then $\mathrm{Nil}(R) = I_R$ so $\overline{R} = R/\mathrm{Nil}(R) = \mathbb{Z}/2\mathbb{Z}$. This can also be viewed as a Witt ring with $G_{\overline{R}} = 1$.

Combining the above, we have proved the following:

Corollary 3.2.23. *If R is a Witt ring, $\overline{R} = R/Nil(R)$ and $G_{\overline{R}}$ = the image of G_R in $\overline{R}$ by the natural projection, then $\overline{R} = (\overline{R}, G_{\overline{R}})$ is a Witt ring with $Nil(\overline{R}) = 0$.*

We will denote the Witt ring $R/\mathrm{Nil}(R)$ by R_{red}. In case F is a field we will refer to R_{red} as *the reduced Witt ring of F*.

3.2.4 Reduced Witt rings

We will say a Witt ring R is *reduced* if $\mathrm{Nil}(R) = 0$. Thus, if R is any Witt ring, then R_{red} is a reduced Witt ring. We now give a necessary and sufficient condition, in terms of the associated Q-structure, that a Witt ring is reduced.

Theorem 3.2.24. *For an arbitrary Witt ring R, R is reduced if and only if q_R satisfies*

$$q_R(a,a) = 0 \Rightarrow a = 1$$

for all $a \in G_R$.

Corollary 3.2.25. *Let R be a reduced Witt ring, f be a form over G_R, and $n \geq 1$. Then*

a - $D(n \times f) = D(f)$.

b - If $\dim(f) \geq 2$ and $n \times f$ is isotropic, then so is f.

Recall that isotropic forms are always universal. For reduced Witt rings we have the converse:

Corollary 3.2.26. *Let R be a reduced Witt ring, f be a form over G_R with $\dim(f) \geq 2$. Then the following are equivalent:*

a - f is isotropic.

b - f is universal.

c - There exist $x \in G_R$ with $x, -x \in D(f)$.

3.3 Cordes Scheme

As observed by Cordes in [Cor76], the existence of a field with prescribed properties relating to quadratic forms can frequently be determined by observing what must happen to the value sets of binary quadratic forms. For this reason, the theory of Cordes schemes borns, and we make a brief introduction following [Cor76], [Kul79], [KSS88]. Here, we describe the category of Cordes Schemes and what is the apropriated notion of isometry of forms.

Definition 3.3.1. *A pre-quadratic scheme is a triple $(G, -1, V)$, where G is a group of exponent 2, i.e, $g^2 = 1$ for all $g \in G$; -1 is a distinguished element of G with the notation $-a = (-1) \cdot a$, and V is a mapping assigning to each $a \in G$ a subgroup $V(a)$ of G, satisfying the following axioms for all $a, b, c \in G$:*

C1 - *$a \in V(a)$ for every $a \in G$.*

C2 - *$b \in V(-a)$ implies $a \in V(-b)$ for all $a, b \in G$.*

A pre-quadratic scheme is said to be reduced if satisfies

$$V(1) = \{1\}. \tag{red}$$

Definition 3.3.2. *A quadratic form f of dimension n in a pre-scheme G, is any n-tuple $f = \langle a_1, ..., a_n \rangle$ of elements of G. The set Df of elements of G represented by f is defined inductively as follows:*

$$\begin{aligned} D\langle a_1 \rangle &= \{a_1\}, \\ D\langle a_1, ..., a_n \rangle &= \bigcup \{a_1 V(a_1 x) : x \in D\langle a_2, ..., a_n \rangle\} \text{ for } n \geq 2. \end{aligned}$$

In particular, for a binary form $\langle a, b \rangle$ we have $D\langle a, b \rangle = aV(ab) = bV(ab) = D(b, a)$[3]*.*

All these have natural meaning in case of the pre-scheme of a field F of characteristic not 2. Here G is the group of square classes $\dot{F}/\dot{F}^2$, -1 is the coset $(-1)\dot{F}$ and $V(a\dot{F}^2)$ is the value group of the quadratic form $\langle 1, a \rangle$ viewed as a subgroup of G. However, it turns out that in the abstract situation the value set $D\langle a_1, ..., a_n \rangle$ depends in general on the order of diagonal entries. To rectify this we introduce

Definition 3.3.3. *A pre-scheme $(G, -1, V)$ is said to be a Cordes scheme (or quadratic scheme) if it satisfies the following axiom:*

C3 - *$D\langle a, b, c \rangle = D\langle b, a, c \rangle$ for all $a, b, c \in G$.*

Ilustrating the versatile of Cordes schemes structure, we have the following

Theorem 3.3.4. *For a triple $(G, -1, V)$, where G is a group of exponent 2, i.e, $g^2 = 1$ for all $g \in G$; -1 is a distinguished element of G, and V is a mapping assigning to each $a \in G$ a subgroup $V(a)$ of G, the following are equivalent:*

i - *$(G, -1, V)$ is a Cordes Scheme.*

ii - *$(G, -1, V)$ satisfies C2 and C3.*

[3] From $a, ab \in V(ab)$ we get $b = a(ab) \in V(ab)$. So $a, b \in V(ab)$, and since $V(ab)$ is a subgroup, we have $aV(ab) = bV(ab)$.

iii - $(G, -1, V)$ *satisfies C1 and*

$$b \in V(-a)V(-ac) \Rightarrow a \in V(-b)V(-bc). \tag{C4}$$

iv - $(G, -1, V)$ *satisfies C1 and*

$$bV(-a) \cap V(-ac) \neq \emptyset \Rightarrow aV(-b) \cap V(-bc) \neq \emptyset. \tag{C5}$$

v - $(G, -1, V)$ *satisfies*

$$b \in V(-a)V(-ac) \Rightarrow ab \in V(-b)V(-bc). \tag{C6}$$

Proof. (i)⇒(ii) is immediate.

(ii)⇒(i) observe that without assuming anything on G we have $a \in D(a, b) = aV(ab)$ and

$$a \in D(a, b, c) = \bigcup_{x \in bV(bc)} \{aV(ax)\}$$

for all $a, b, c \in G$. Thus $a \in D(a, 1, -1)$ and by $C3$, $a \in D(1, a, -1)$. It follows $a \in V(x)$, where $x \in D(a, -1) = aV(-a)$. Thus $x = ay$ with $y \in V(-a)$ and $a \in V(ay)$. By C2, $-ay \in V(-a)$ and so $-a = -ay \cdot y \in V(-a)$. By C2 again, $a \in V(a)$, proving C1.

(i)⇒(iii) first of all, we claim that $y \in D(a, b, c)$ iff $-ab \in V(bc)V(-ay)$. For this, note that

$$D(a, b, c) = \bigcup \{aV(au) : u \in bV(bc)\} = \bigcup \{aV(abx) : x \in V(bc)\}.$$

Hence $y \in D(a, b, c)$ iff exists $x \in V(bc)$ with $y \in aV(abx)$, i.e, $ay \in V(abx)$. By C2, this holds iff $-abx \in V(-ay)$ or equivalently, $-ab \in xV(-ay)$ with $x \in V(bc)$. Note that we do not use C3 in this proof.

Now, using the claim, by $b \in V(-a)V(-ac)$ we get $-c \in D(-a, ab, -b) = D(-a, -b, ab)$. By C3, $-c \in D(-b, -a, ab) = D(-b, ab, -a)$. Using the claim again, we obtain $a \in V(-b)V(-bc)$, as desired.

(iii)⇒(i) by $D(a, b, c) = \bigcup \{aV(abx) : x \in V(bc)\}$ we get

$$D(a, b, c) = abcD(bc, ac, ab) = abcD(bc, ab, ac).$$

Similarly, $D(b, a, c) = abcD(ac, ab, bc)$. using C4 and the claim, we get

$$\begin{aligned} y \in D(ac, ab, bc) &\Leftrightarrow -bc \in V(ac)V(-acy) \\ &\Leftrightarrow -ac \in V(bc)V(-bcy) \\ &\Leftrightarrow y \in D(bc, ab, ac) \end{aligned}$$

obtaining C3.

(iii)⇔(iv) follow by a general group-theoretic fact: $b \in HK$ iff $Hb \cap K \neq \emptyset$ where H and K are subgroups of an arbitrary group G.

(iii)⇒(v) suppose $b \in V(-a)V(-ac)$. Then $a \in V(-b)V(-bc)$ and since $-b \in V(-b)V(-bc)$, we get $-abV(-b)V(-bc)$.

(v)⇒(iii) applying C6 twice, we get

$$b \in V(-a)V(-ac) \Rightarrow a \in V(ab)V(abc). \qquad (*)$$

Taking $b = c = 1$ and using (*) we get $a \in V(a)$, proving C1. Finally, by C6 and C1 we obtain $b \in V(-a)V(-ac) \Rightarrow -a \in V(-b)V(-bc)$, i.e, we prove C4. □

Definition 3.3.5. *Let $(G, -1, V)$ and $(H, -1, W)$ be pre-schemes. A c-morphism is a group homomorphism $f : G \to H$ such that $f(-1) = -1$ and $f(V(a)) \subseteq W(f(a))$ for all $a \in G$.*

The category of pre-schemes and c-morphisms will be denoted by $\mathcal{PCS}$. Similarly, the category of Cordes schemes (respectively reduced Cordes schemes) and c-morphisms will be denoted by $\mathcal{CS}$ (respectively $\mathcal{RCS}$).

The notion of isometry of quadratic forms can be introduced in abstract pre-schemes in two different ways.

Definition 3.3.6. *Two forms $f = \langle a_1, ..., a_n\rangle$ and $g = \langle b_1, ..., b_n\rangle$ in a pre-scheme S are said to be chain isometric, written $f \sim g$ if*

i - $a_1 = b_1$, *when* $n = 1$.

ii - $a_1a_2 = b_1b_2$ *and* $D\langle a_1, a_2\rangle = D\langle b_1, b_2\rangle$, *when* $n = 2$.

iii - *For* $n \geq 3$, *there exists a chain of forms* $f_0 = f, f_1, f_2, ..., f_k = g$, $k \geq 0$, *such that for each* $i = 0, ..., k-1$, *the form* f_i *is simply-equivalent to* f_{i+1} *(remember 1.2.4).*

Definition 3.3.7. *Two forms f and g as above is said to be strongly isometric, written $f \cong g$, if*

i - $a_1 = b_1$, *when* $n = 1$.

ii - $a_1a_2 = b_1b_2$ *and* $D\langle a_1, a_2\rangle = D\langle b_1, b_2\rangle$, *when* $n = 2$.

iii - *For* $n \geq 3$, *there exists* $a, b, c_3, ..., c_n \in G$ *such that* $\langle a_1, a\rangle \cong \langle b_1, b\rangle$, $\langle a_2, ..., a_n\rangle \cong \langle a, c_3, ..., c_n\rangle$ *and* $\langle b_2, ..., b_n\rangle \cong \langle b, c_3, ..., c_n\rangle$.

Lemma 3.3.8. *For arbitrary forms φ, ψ, ψ' over a Cordes scheme S, $\psi \cong \psi' \Leftrightarrow \varphi \oplus \psi \cong \varphi \oplus \psi'$.*

Proof. Just copy (literally!) the proof of lemma 3.1.12! □

Theorem 3.3.9. *For a pre-scheme S the following are equivalent:*

i - *Strongly isometry $\cong$ is transitive.*

ii - *Strongly isometry $\cong$ is transitive on 3-dimensional forms.*

iii - *The pre-scheme S is a Cordes scheme.*

Proof. (i)⇒(ii) and (ii)⇔(iii) follow by the definitions involved. We just need to prove (ii)⇒(i). By induction on the dimension, which, when 2 or 3 are taken care of by assumption. Assume that $\langle a_1, ..., a_n\rangle \cong \langle b_1, ..., b_n\rangle = \psi$ and $\psi \cong \langle c_1, ..., c_n\rangle$, and that $\cong$ is transitive on forms of dimension

$n-1 \geq 3$. The hypotheses yield $\alpha, \beta, \gamma, \delta, y_i, z_i \in G$, $3 \leq i \leq n$, such that (I) and (II) below hold true

$$\langle a_1, \alpha\rangle \cong \langle b_1, \beta\rangle,\ \langle a_2, ..., a_n\rangle \cong \langle \alpha, \vec{y}\rangle \text{ and } \langle b_2, ..., b_n\rangle \cong \langle \beta, \vec{y}\rangle; \tag{I}$$
$$\langle b_1, \gamma\rangle \cong \langle c_1, \delta\rangle,\ \langle b_2, ..., b_n\rangle \cong \langle \gamma, \vec{z}\rangle \text{ and } \langle c_2, ..., c_n\rangle \cong \langle \delta, \vec{z}\rangle, \tag{II}$$

where $\vec{y} = \langle y_3, ..., y_n\rangle$ and $\vec{z} = \langle z_3, ..., z_n\rangle$. By induction, $\cong$ is transitive on $(n-1)$-forms, and so, $\langle \beta, \vec{y}\rangle \cong \langle \gamma, \vec{z}\rangle$, since both are isometric to $b_2, ..., b_n\rangle$. Thus, there are $x, t, y.\vec{t} = \langle t_4, ..., t_n\rangle \in G$ such that

$$\langle \beta, x\rangle \cong \langle \gamma, y\rangle,\ \langle \vec{y}\rangle \cong \langle x, \vec{t}\rangle \text{ and } \langle \vec{z}\rangle \cong \langle y, \vec{t}\rangle. \tag{III}$$

Now, by the preservation of isometry by sum (lemma 3.3.8), the first isometry in (I), (II) and (III) as well as 3-transitivity, we may write

$$\begin{aligned}\langle a_1, \alpha, x\rangle &= \langle a_1, \alpha\rangle \oplus \langle x\rangle \cong \langle b_1, \beta\rangle \oplus \langle x\rangle \cong \langle b_1\rangle \oplus \langle \beta, x\rangle \\ &\cong \langle b_1\rangle \oplus \langle \gamma, y\rangle \cong \langle b_1, \gamma\rangle \oplus \langle y\rangle \cong \langle c_1, \delta\rangle \oplus \langle y\rangle = \langle c_1, \delta, y\rangle.\end{aligned}$$

Therefore, there are $u, v, w \in G$ such that

$$\langle a_1, u\rangle \cong \langle c_1, v\rangle,\ \langle \alpha, x\rangle \cong \langle u, w\rangle \text{ and } \langle \delta, y\rangle \cong \langle v, w\rangle. \tag{IV}$$

The preservation of isometry by sum, the transitivity of $\cong$ for $(n-1)$-forms, the second and the third isometry in (I) and (II), respectively, together with the last two in (III) and (IV), yield

$$\begin{aligned}\langle a_2, ..., a_n\rangle \cong \langle \alpha, \vec{y}\rangle \cong \langle \alpha, x, \vec{t}\rangle \cong \langle u, w, \vec{t}\rangle \text{ and} \\ \langle c_2, ..., c_n\rangle \cong \langle \delta, \vec{z}\rangle \cong \langle \delta, y, \vec{t}\rangle \cong \langle v, w, \vec{t}\rangle,\end{aligned}$$

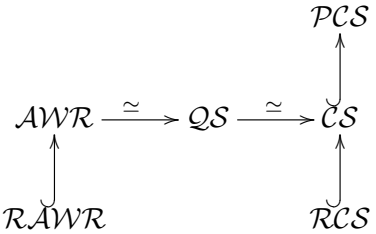
isometries which, together with the first one in (IV), prove that $\langle a_1, ..., a_n\rangle \cong \langle c_1, ..., c_n\rangle$. □

Theorem 3.3.10. *Let S be a Cordes scheme. Given two forms f and g over S, we have*

$$f \cong g \Leftrightarrow f \sim g.$$

3.4 A First Functorial Picture

After this introduction to our first abstract theories, we will describe our first functorial picture



Here, $\mathcal{RAWR}$ and $\mathcal{RCS}$ are the categories of reduced abstract Witt rings and reduced Cordes schemes respectively. We already describe the equivalence between $\mathcal{AWR}$ and $\mathcal{QS}$. So, left to us, create the connection between $\mathcal{QS}$ and $\mathcal{CS}$[4].

[4]Of course, we do not talk about reduced abstract Witt rings. However, once we estabilish the equivalence between

Proposition 3.4.1. *Let (G, Q, q) be a quaternionic structure. For all $a \in G$, define $V_G(a) = \{b \in G : q(-a, b) = 0\}$. Then $(G, -1, V_G)$ is a pre-scheme.*

Proof. Firstly, we need to prove that $V_G(a)$ is in fact a subgroup. By 3.1.9(i) $q(-a, 1) = 0$ for all $a \in G$, so $1 \in V_G(a)$. Now, let $b, c \in V_G(a)$.

$$b, c \in V_G(a) \Rightarrow q(-a, b) = 0 = q(-a, c) \overset{Q3}{\Rightarrow} q(-a, bc) = 0$$

and $bc \in V_G(a)$. Therefore $V_G(a)$ is a subgroup of G. Note that $a \in V_G(a)$ since $q(-a, a) = 0$ by Q2, and if $b \in V_G(a)$,

$$q(-a, b) = 0 \overset{Q1}{\Rightarrow} q(b, -a) = 0 = q(-(-b), -a) \Rightarrow -a \in V_G(-b).$$

Then, we have that $(G, -1, V_G)$ is a pre-scheme. □

To prove that $(G, -1, V_G)$ is a Cordes scheme, we need to translate the notion of representation in both theories. Remember, given a form $f = \langle a_1, ..., a_n \rangle$ in a pre-scheme $(G, V, -1)$, the set $D_{\mathcal{C}}\langle f \rangle$ of elements of G represented by f (in the sense of Cordes schemes) is:

$$\begin{aligned} D_{\mathcal{C}}\langle a_1 \rangle &= \{a_1\}, \\ D_{\mathcal{C}}\langle a_1, ..., a_n \rangle &= \bigcup \{a_1 V(a_1 x) : x \in D\langle a_1, ..., a_n \rangle\} \text{ for } n \geq 2. \end{aligned}$$

In particular, for a binary form $\langle a, b \rangle$ we have $D_{\mathcal{C}}\langle a, b \rangle = aV(ab) = bV(ab)$. Hence,

$$D_{\mathcal{C}}\langle a_1, ..., a_n \rangle = \bigcup_{x \in D_{\mathcal{C}}\langle a_1, ..., a_n \rangle} D_{\mathcal{C}}(a_1, x).$$

On the other hand, in the sense of quaternionic structures, given a form $f = \langle a_1, ..., a_n \rangle$ in a quaternionic structure (G, Q, q), $D_{\mathcal{Q}}\langle f \rangle$ of elements of G represented by f is:

$$D_Q(f) = \{x \in G : \text{ there exists } x_2, ..., x_n \in G \text{ such that } f \cong \langle x, x_2, ..., x_n \rangle\}.$$

By the inductive description of isometry on quaternionic structures, we have

$$D_{\mathcal{Q}}\langle a_1, ..., a_n \rangle = \bigcup_{x \in D_{\mathcal{Q}}\langle a_1, ..., a_n \rangle} D_{\mathcal{Q}}(a_1, x).$$

Now, we are ready to prove the theorem desired:

Theorem 3.4.2. *Let (G, Q, q) be a quaternionic structure. With the notation developed in 3.4.1, $(G, -1, V_G)$ is a Cordes scheme. Moreover, this correspondence gives a functor $\mathcal{C} : \mathcal{QS} \to \mathcal{CS}$.*

Proof. For the first affirmation, we just need to prove C3. The first step, is to prove that $D_{\mathcal{C}}(a, b) = D_Q(a, b)$ for all $a, b \in G$. For this, note that for all $a, b \in G$

$$\begin{aligned} D_Q(a, b) &= \{x \in G : \text{ there exist } y \in G \text{ such that } \langle x, y \rangle \cong \langle a, b \rangle\} \\ &= \{x \in G : \text{ there exist } y \in G \text{ such that } xy = ab \text{ and } q(x, y) = q(a, b)\} \\ &\overset{y=xab}{=} \{x \in G : \text{ such that } \langle x, xab \rangle \cong \langle a, b \rangle\}. \end{aligned}$$

$\mathcal{AWR}$, $\mathcal{QS}$ and $\mathcal{CS}$, the equivalence between $\mathcal{RAWR}$ and $\mathcal{RCS}$ will follow.

In particular, $D_Q(1,a) = \{x \in G : \text{ such that } \langle x, xa\rangle \cong \langle 1, a\rangle\}$ and $q(x,xa) = 0$ for all $a \in G$, and this implies $D_Q(a,b) = aD_Q(1,ab)$. This yields

$$\begin{aligned} V(a) &= \{x \in G : q(-a,x) = 0\} \overset{q(x,-x)=0}{\Rightarrow} \\ V(a) &= \{x \in G : q(x,xa) = 0\} = D_Q(1,a) \end{aligned}$$

for all $a \in G$. Therefore

$$D_{\mathcal{C}}(a,b) = aV(ab) = aD_Q(1,ab) = D_Q(a,b).$$

The second step is prove that $D_{\mathcal{C}}(a,b,c) = D_Q(a,b,c)$ for all $a,b,c \in G$:

$$D_{\mathcal{C}}(a,b,c) = \bigcup_{x \in D_{\mathcal{C}}(b,c)} D_{\mathcal{C}}(a,x) = \bigcup_{x \in D_Q(b,c)} D_Q(a,x) = D_Q(a,b,c).$$

Finally, by proposition 3.1.10(a) we have

$$\begin{aligned} D_Q(a,b,c) &= \{x \in G : \text{ there exist } y,z \in G \text{ such that } \langle x,y,z\rangle \cong \langle a,b,c\rangle\} \\ &= \{x \in G : \text{ there exist } y,z \in G \text{ such that } \langle x,y,z\rangle \cong \langle b,a,c\rangle\} = D_Q(b,a,c), \end{aligned}$$

finalizing the proof of C3. Hence $(G, V_G, -1)$ is a Cordes scheme.

Now, for the second affirmation, let $f : (G, Q_G, q_G) \to (H, Q_H, q_H)$ be a QS-morphism and $a \in G$. Of course, we already have $f(-1) = -1$ (and hence, $f(-a) = -f(a)$). Now, given $b \in V(a)$, we have

$$\begin{aligned} b \in V_G(a) &\Rightarrow q_G(-a,b) = 0 \Rightarrow q_H(f(-a), f(b)) = 0 \\ &\Rightarrow q_H(-f(a), f(b)) = 0 \Rightarrow f(b) \in V_H(f(a)). \end{aligned}$$

Then f is also a C-morphism. Defining $\mathcal{C}(G,Q,q) = (G, V_G, -1)$ and $\mathcal{C}(f) = f$ we have the desired functor $\mathcal{C} : \mathcal{QS} \to \mathcal{CS}$. □

Now, we will work in the converse of theorem 3.4.2. Let start with a Cordes scheme $(G, V, -1)$. Here, the construction is exactly the same made for the theorem 3.1.1: we define Q_G to be the set of all isometry classes of quadratic forms of the type $\langle 1, -a, -b, ab\rangle$, with $a, b \in G$ and consider Q_G to be a "pointed set" with point 0 equal to the isometry class of $\langle 1, -1, 1, -1\rangle$. In the sequel, we define $q_G : G \times G \to Q_G$ to be the map sending (a,b) to the isometry class of $\langle 1, -a, -b, ab\rangle$.

Theorem 3.4.3. *Let $(G, V, -1)$ be a Cordes scheme. Then (G, Q_G, q_G) is a quaternionic structure. Moreover, this correspondence provides a functor $\mathcal{Q} : \mathcal{CS} \to \mathcal{QS}$.*

Proof. We need to verify the properties of definition 3.1.8 for (G, Q_G, q_G). Let $a,b,c,d \in G$. With the identification via isometry classes,

$$q(a,b) = \langle 1, -a, -b, ab\rangle = \langle 1, -b, -a, ba\rangle = q(b,a)$$

gives Q1 and $q(a,-a) = \langle 1, -a, a, -1\rangle = 0$ gives Q2. For Q3, suppose that $q(a,b) = q(a,c)$. Then $\langle 1, -a, -b, ab\rangle \cong \langle 1, -a, -c, ac\rangle$, and by Witt's cancellation, $\langle -b, ab\rangle \cong \langle -c, ac\rangle$. By definition of isometry on Cordes schemes and theorem 3.3.9, we have

$$\begin{aligned} \langle -b, ab\rangle \cong \langle -c, ac\rangle &\Leftrightarrow -bV(-a) = -cV(-a) \Leftrightarrow bV(-a) = cV(-a) \\ &\Leftrightarrow abcV(-a) = aV(-a). \end{aligned} \tag{3.1}$$

Keeping this in mind, lets us examine what $q(a, bc) = 0$ means.

$$\begin{aligned} q(a,bc) = 0 &\Leftrightarrow \langle 1, -a, -bc, abc\rangle = \langle 1, -1, 1, -1\rangle \\ &\Leftrightarrow \langle -a, -bc, abc\rangle = \langle -1, 1, -1\rangle, \end{aligned}$$

and this happens if and only if there exists $x, y, z \in G$ such that $\langle -a, x\rangle \cong \langle -1, y\rangle$, $\langle -bc, abc\rangle \cong \langle x, z\rangle$ and $\langle 1, -1\rangle \cong \langle y, z\rangle$. Taking $x = a$, $y = 1$ and $z = -1$, we already have $\langle -a, a\rangle \cong \langle -1, 1\rangle$ and $\langle 1, -1\rangle \cong \langle 1, -1\rangle$. To prove that $\langle -bc, abc\rangle \cong \langle a, -1\rangle$, is just observe that $(-bc) \cdot (abc) = a \cdot (-1)$ and $abcV(-a) = aV(-a)$ by 3.1. Hence, $q(a, b) = q(a, c) \Rightarrow q(a, bc) = 0$. Conversely, suppose $q(a, bc) = 0$. Then by the same argument above, we conclude $abcV(-a) = aV(-a)$, and by 3.1 follows $q(a, b) = q(a, c)$.

Finally, for Q4 we will repeat the same argument given in the field case: suppose $q(a, b) = q(c, d)$, i.e, $\langle 1, -a, -b, ab\rangle \cong \langle 1, -c, -d, cd\rangle$. By Witt's Cancellation, $\langle -a, -b, -ab\rangle \cong \langle -c, -d, cd\rangle$. By definition of isometry on Cordes schemes and theorem 3.3.9, there exist $e, f, g \in G$ with $\langle -b, ab\rangle \cong \langle e, f\rangle$, $\langle -d, cd\rangle \cong \langle f, g\rangle$ and $\langle -a, e\rangle \cong \langle -b, g\rangle$. Comparing discriminants we get $ef = -a$, $gf = -c$, so $e = -af$ and $g = -cf$. Taking $x = -f$, we have $e = ax$, $g = cx$, so $\langle -b, ab\rangle \cong \langle -x, ax\rangle$ and $\langle -d, cd\rangle \cong \langle -x, cx\rangle$. Adding $\langle 1, -a\rangle$ and $\langle 1, -c\rangle$ respectively we obtain $q(a, b) = q(a, x)$ and $q(c, d) = q(c, x)$. Therefore (G, Q_G, q_G) is a quaternionic structure.

Now, let $f : (G, V_G, -1) \to (H, V_H, -1)$ be a C-morphism. Since f is in particular a group homomorphism, we have

$$q_G(a, b) = 0 \Rightarrow \langle 1, -a, -b, ab\rangle = 0 \Rightarrow \langle 1, -f(a), -f(b), f(a)f(b)\rangle = 0 \Rightarrow q_H(f(a), f(b)) = 0.$$

Then f is a QS-morphism. Defining $\mathcal{Q}(G, V, -1) = (G, Q_G, q_G)$ and $\mathcal{Q}(f) = f$, we have the desired functor $\mathcal{Q} : \mathcal{CS} \to \mathcal{QS}$. □

Corollary 3.4.4. *The functors $\mathcal{Q}$ and $\mathcal{C}$ are quasi-inverse equivalences and the categories $\mathcal{CS}$ and $\mathcal{QS}$ are equivalent.*

So the first picture is complete. We emphasize this is the first time that these connections are made with this level of details.

Chapter 4

A second generation of abstract theories

In the decade of 80's, a new abstract theory appears: the Marshall's Abstract Space of Orderings (AOS). They are important because generalize both theory of orderings on fields and the reduced theory of quadratic forms. Since the abstract theories of chapter 3 does not have field-theoretic methods to deal with the reduced case, the AOS solves this issue.

But only in the decade of 90's that arise a (finitary) first-order theory that generalize the reduced and non-reduced theory of quadratic forms simultaneously (in the sense that we will see in subsection 4.2.3). This theory is the Special Groups of F. Miraglia and M. Dickmann. It takes as primitive the binary isometry, is a first-order theory and treat the reduced and non-reduced case in a very elegant way. This simplicity brings new methods and tools to the algebraic theory of quadratic forms, culminating in a proof of Marshall's and Lam conjecture.

4.1 Space of Orderings

We basically cover almost chapters 1,2 and 3 of [Mar96].

4.1.1 Basic Definitions

We need some elementary facts about groups of exponent 2 and their character groups.

A group of exponent 2 is a (necessarily abelian) group G satisfying $a^2 = 1$ for all $a \in G$. A *character* on a group G of exponent 2 is a homomorphism $x : G \to \{1, -1\}$. The *character group* G of exponent 2 is $\chi(G) := \mathrm{Hom}(G, \{1, -1\})$ the set of all characters on G, with the group operation defined pontwise, i.e, $(xy)(a) := x(a)y(a)$ for all $a \in G$.

If G is a group of exponent 2, then $\chi(G)$ has a natural topology making in into a topological group. The topology is just the weakest such that the mapping $x \mapsto x(a)$, $a \in G$, are continuous, giving $\{1, -1\}$ the discrete topology.

Proposition 4.1.1. *For any group G of exponent 2:*

i - *$\chi(G)$ is compact.*

ii - *For each subgroup H of G, $\chi(G/H)$ is a closed subgroup of $\chi(G)$.*

iii - *Conversely, if S is any closed subgroup of $\chi(G)$ then $S = \chi(G/H)$ where $H = \bigcap_{x \in S} Ker(x)$.*

Proof. We are identifying characters in G/H with characters of G containing H in their kernels (we can do it because of homomorphism theorem!).

i - Denote by $\{-1,1\}^G$ the set of all functions from G to $\{-1,1\}$ with the product topology, giving $\{-1,1\}$ the discrete topology. Then $\chi(G) \subseteq \{-1,1\}^G$ and the topology on $\chi(G)$ is the induced topology. Since $\{-1,1\}^G$ is compact by Tychonoff's theorem, it suffices to check that $\chi(G)$ is closed in $\{-1,1\}^G$. Suppose $x \in \{-1,1\}^G$ is in the closure of $\chi(G)$. For each $a, b \in G$, the set

$$U = \{y \in \{-1,1\}^G : y(a) = x(a),\ y(b) = x(b),\ y(ab) = x(ab)\}$$

is a neighbourhood of x in $\{-1,1\}^G$. Thus $U \cap \chi(G) \neq \emptyset$, say $y \in U \cap \chi(G)$. Then $y(ab) = y(a)y(b)$ so $x(ab) = y(ab) = y(a)y(b) = x(a)x(b)$. This proves that x is a character of G, so $x \in \chi(G)$.

ii - $\chi(G/H)$ is compact by item (i), so it is closed in $\chi(G)$.

iii - Again, by homomorphism theorem, we can identificate S with a subseteq of $\chi(G/H)$. Of course, we shall abuse of this identification and write $S \subseteq \chi(G/H)$. For the other inclusion, replacing G by G/H, we are reduced to the case where $H = \{1\}$. Thus we are assuming $S \subseteq \chi(G)$ is a closed subgroup such that $\bigcap_{x\in S} \mathrm{Ker}(x) = \{1\}$, and we want to show $S = \chi(G)$.

It suffices to handle the case where G is finite. Suppose K is any finite subgroup of G and denote by $S|_K$ the set of restrictions $x|_K$, $x \in S$. This is a subgroup of $\chi(K)$ and $\bigcap_{x\in S} \mathrm{Ker}(x|_K) = \{1\}$. Thus, if we know the result in the finite case, then $S|_K = \chi(K)$. This means that, for each $y \in \chi(G)$ and each finite subgroup K of G, there exist $x \in S$ such that $x|_K = y|_K$. Since S is closed in $\chi(G)$, this implies (by compacity) that $S = \chi(G)$.

So suppose G is finite (then the topology is discrete). Let $\{x_1, ..., x_n\}$ be a subset of S chosen minimal such that $\cap_{i=1}^n \mathrm{Ker}(x_i) = \{1\}$. Consider the chain of subgroups

$$G \supseteq \mathrm{Ker}(x_1) \supseteq \mathrm{Ker}(x_1) \cap \mathrm{Ker}(x_2) \supseteq ... \supseteq \cap_{i=1}^n \mathrm{Ker}(x_i) = \{1\}.$$

For $j = 1, ..., n$, $\mathrm{Ker}(x_j)$ has index 2 in G and $\cap_{i=1}^{j-1} \mathrm{Ker}(x_i) \nsubseteq \mathrm{Ker}(x_j)$ by the minimal choice of the subset $\{x_1, ..., x_n\}$. Thus $(\cap_{i=1}^{j-1} \mathrm{Ker}(x_i)) \cdot \mathrm{Ker}(x_j) = G$ so

$$\frac{\cap_{i=1}^{j-1} \mathrm{Ker}(x_i)}{\cap_{i=1}^{j} \mathrm{Ker}(x_i)} \cong \frac{(\cap_{i=1}^{j-1} \mathrm{Ker}(x_i)) \cdot \mathrm{Ker}(x_j)}{\mathrm{Ker}(x_j)} = \frac{G}{\mathrm{Ker}(x_j)}.$$

This means $\cap_{i=1}^{j} \mathrm{Ker}(x_i)$ has index 2 in $\cap_{i=1}^{j-1} \mathrm{Ker}(x_i)$, $j = 1, ..., n$ so $\{1\} = \cap_{i=1}^n \mathrm{Ker}(x_i)$ has index 2^n in G, i.e, $|G| = 2^n$. Thus, by counting, we see that the natural injection $G \hookrightarrow \prod_{i=1}^n G/\mathrm{Ker}(x_i)$ is surjective so we get elements $a_1, ..., a_n \in G$ such that $x_i(a_j) = -1$ if $i = j$ and 1 otherwise. Then every element $a \in G$ is expressible uniquely as $a = \prod_{i=1}^n a_i^{e_i}$, $e_i \in \{0, 1\}$, so $\{a_1, ..., a_n\}$ is a $\mathbb{Z}_2$-basis of G. Follow this that $\{x_1, ..., x_n\}$ is the dual basis of $\chi(G)$. Since $\{x_1, ..., x_n\} \subseteq S$, this means $S = \chi(G)$.

□

A topological space X is called a *Boolean space* if it is compact, Hausdorff and the clopen sets form a basis for the topology. For example, if G is a group of exponent 2 then $\chi(G)$ is a Boolean Space. Boolean spaces are also characterized as compact Hausdorff spaces which are totally disconnected (i.e, the connected components are singleton sets). This is a consequence of the following general result which we record now for future use:

Lemma 4.1.2. *For any compact topological space X which is normal (i.e, disjoint closed sets can be separated), the connected component of any $x \in X$ is the intersection of all clopen sets in X containing x.*

Proof. Let $x \in X$ and $Z \subseteq X$ be the intersection of all clopen sets containing x. If C_x is the connected component of x, C_x must be a subset of Z (because of the topology of subspace). If we show that Z is connected, it will follow that $Z = C_x$. Suppose this is false so we have non-empty closed sets Z_1, Z_2 in Z with $Z_1 \cup Z_2 = Z$ and $Z_1 \cap Z_2 = \emptyset$. Z is closed in X since it is the intersection of clopen sets, so Z_1, Z_2 are closed in X. Since X is normal, there exist disjoint open sets U_1, U_2 in X with $U_1 \supseteq Z_1$ and $U_2 \supseteq Z_2$. Consider the closed sets $V_1 = X \setminus U_1$, $V_2 = X \setminus U_2$. Then $V_1 \cap V_2 \cap Z = \emptyset$ so by compactness, $V_1 \cap V_2 \cap Y = \emptyset$ for some clopen set Y in X with $Z \subseteq Y$. Y decomposees as a disjoint union of two non-empty open sets $Y = (U_1 \cap Y) \cup (U_2 \cap Y)$. This means $U_1 \cap Y$ and $U_2 \cap Y$ are clopen in Y (and hence in X). Say $x \in U_1 \cap Y$. Then $U_1 \cap Y$ is a clopen set containing x and $Z \nsubseteq U_1 \cap Y$ which contradicts the definition of Z. □

Now, rewrite some terminology of the reduced theory relative to a fix proper preordering $T \subseteq F$, F a formally real field. Remember that $X_T = \{P \supseteq T : P \in \mathrm{Sper}(F)\}$. Let $G_T = \dot{F}/\dot{T}$.

For any set X, $\{-1,1\}^X$ denotes the set of all functions $a : X \to \{-1,1\}$. This is a group with operation given by $(ab)(x) = a(x)b(x)$. Note that $a^2 = 1$ for all $a \in \{-1,1\}^X$.

Lemma 4.1.3. *G_T is naturally identified with a subgroup of $\{-1,1\}^{X_T}$.*

Proof. Each $a \in \dot{F}$ gives rise to a function $\overline{a} = \overline{a}_T : X_T \to \{-1,1\}$ given by

$$\overline{a}(P) = \begin{cases} 1 \text{ if } a \in P \\ -1 \text{ if } a \in -P. \end{cases}$$

Moreover, $\overline{a}\overline{b} = \overline{ab}$ so we have a group homomorphism from G_T into $\{-1,1\}^{X_T}$ given by $a\dot{T} \mapsto \overline{a}$. If $a \notin T$ then by 2.1.2 and 2.1.4 there exist $P \in X_T$ with $\overline{a}(P) = -1$. Thus the mapping $aT^* \mapsto \overline{a}$ is injective. □

Thus we can identify G_T with a subgroup of $\{-1,1\}^{X_T}$ by identifying the coset $a\dot{T}$ with $\overline{a} = \overline{a}_T$ for each $a \in \dot{F}$.

A *quadratic form* with entries in G_T is an n-tuple $\varphi = \langle \overline{a}_1, ..., \overline{a}_n \rangle$, $\overline{a}_1, ..., \overline{a}_n \in G_T$. n is called the *dimension* of φ. $\prod_{i=1}^n \overline{a}_i \in G_T$ is called the *discriminant* of φ. For each $P \in X_T$, the *signature* of φ at P is $\varphi(P) := \sum_{i=1}^n \overline{a}_i(P) \in \mathbb{Z}$. We say $\overline{b} \in G_T$ is *represented* by $\varphi = \langle \overline{a}_1, ..., \overline{a}_n \rangle$ if $b = \sum_{i=1}^n a_i t_i$ for some $t_1, ..., t_n \in T$. The *value set* of φ consists of all elements $\overline{b} \in G_T$ represented by φ. This is denoted by $D(\varphi)$ or by $D\langle \overline{a}_1, ..., \overline{a}_n \rangle$. Thus, if $\overline{a} \in G_T$, then $D\langle \overline{a} \rangle = \{\overline{a}\}$ and, if $n \geq 3$, then

$$\overline{b} \in D\langle \overline{a}_1, ..., \overline{a}_n \rangle \Leftrightarrow \overline{b} \in D\langle \overline{a}, \overline{c} \rangle \text{ for some } \overline{c} \in D\langle \overline{a}_2, ..., \overline{a}_n \rangle.$$

Since we are not allowing $c = 0$, this requires a word of explanation: suppose $b = \sum_{i=1}^n a_i t_i$. If $\sum_{i=1}^n a_i t_i \neq 0$, take $c = \sum_{i=1}^n a_i t_i$. If $\sum_{i=1}^n a_i t_i = 0$, then $b = a_1 t_1 = a_1 t_1 + c0$ so, in this case, we can take $\overline{c}$ arbitrary in $D\langle \overline{a}_2, ..., \overline{a}_n \rangle$.

Thus by induction on the dimension, the study of value sets reduces to the 2-dimensional case. In this case, we have the following result giving a description of value sets which does not refer to the addition on F:

Lemma 4.1.4.

$$D\langle \overline{a}_1, \overline{a}_2 \rangle = \{\overline{b} \in G_T : \textit{for all } P \in X_T, \textit{ either } \overline{b}(P) = \overline{a}_1(P) \textit{ or } \overline{b}(P) = \overline{a}_2(P)\}.$$

Proof. Let $b \in \dot{F}$, $b = t_1a_1 + t_2a_2$, $t_1, t_2 \in T$, and let $P \in X_T$. We want to show $\overline{b}(P) = \overline{a_1}(P)$ or $\overline{b}(P) = \overline{a_2}(P)$. If $\overline{a_2}(P) = -\overline{a_1}(P)$ it is immediate. If $\overline{a_1}(P) = \overline{a_2}(P) = 1$, then the equation $b = t_1a_1 + t_2a_2$ forces $\overline{b}(P) = 1$. Similarly, if $\overline{a_1}(P) = \overline{a_2}(P) = -1$.

To prove the other inclusion, assume for each $P \in X_T$, $\overline{b}(P) = \overline{a_1}(P)$ or $\overline{a_2}(P)$. We want to show that $b \in Ta_1 + Ta_2$, i.e, that $b/a_1 \in T + T(a_2/a_1)$. Suppose this is not the case, and consider the preordering $T' = T + T(a_2/a_1)$. By 2.1.2 and 2.1.4 we have an ordering P with $b/a_1 \notin P$ and $P \supseteq T'$. Since $T' \supseteq T$ and $a_2/a_1 \in T'$, this means $P \in X_T$, $\overline{(a_2/a_1)}(P) = 1$, $\overline{b/a_1}(P) = -1$. Thus $\overline{a_1}(P) = \overline{a_2}(P)$ and $\overline{b}(P) = -\overline{a_1}(P)$. This contradicts the assumption. □

The next result is perhaps surprising: every represented element has a "transversal" representation:

Lemma 4.1.5. *Suppose $a_1, ..., a_n, b \in \dot{F}$. Then the following are equivalent:*

i - $\overline{b} \in D\langle \overline{a}_1, ..., \overline{a}_n \rangle$.

ii - $b = \sum_{i=1}^{n} a_i'$ *for some* $a_1', ..., a_n' \in \dot{F}$ *such that* $\overline{a}_i' = \overline{a}_i$, *i.e,* $a_i' = t_ia_i$ *for some* $t_i \in \dot{T}$, $i = 1, ..., n$.

Proof. (ii)⇒(i) is just the definition. For (i)⇒(ii) we can suppose

$$b = \sum_{j=1}^{n} t_ja_j,\ t_1, ..., t_n \in T.$$

Using the identity $p = (\frac{p+1}{2})^2 - (\frac{p-1}{2})^2$, we get

$$\frac{a_1 + ... + a_n}{b} = r^2 - s^2 = (1 + r^2) - (1 + s^2)$$

for some $r, s \in F$. Thus

$$(1 + r^2)b = a_1 + ... + a_n + (1 + s^2)b = \sum_{j=1}^{n}(1 + (1 + s^2)t_j)a_j,$$

so $b = \sum_{j=1}^{n} a_j'$, where $a_j' = \frac{1+(1+s^2)t_j}{1+r^2}a_j$. □

This lemma gives an interesting intrepretation of value sets. The multiplication on G_T satisfies $\overline{a}\overline{b} = \overline{ab}$, i.e, it is just the operation on G_T induced by the multiplication on $\dot{F}$. We could try to do the same thing with the addition and define $\overline{a} + \overline{b} = \overline{a + b}$, but this is not well-defined. Instead of getting a single output, we get a whole set of outputs, namely we get the set $D\langle \overline{a}, \overline{b} \rangle = \{\overline{a' + b'} : a' + b' \neq 0, \overline{a'} = \overline{a}, \overline{b'} = \overline{b}\}$. Thus, in studying value sets, we are just studying what remains of the addition when we pass from F to G_T.

Spaces of orderings were introduced by Murray Marshall in the 1980's in an attempt to axiomatize the reduced theory of quadratic forms:

Definition 4.1.6 (Space of Orderings)**.** *An abstract ordering space or space of orderings, abbreviated AOS, is a pair (X, G) satisfying:*

AX1 - *X is a non-empty set, G is a subgroup of $\{-1, 1\}^X$, G contais the constant function -1, and G separates points in X (i.e, if $x, y \in X$, $x \neq y$, then there exists $a \in G$ such that $a(x) \neq a(y)$).*

Although it is convenient to define elements of G to be functions on X, it is equally important to realize that we can view elements of X as a characters on G. By AX1 we have a natural embedding of X into the character group $\chi(G)$ obtained by identifying $x \in X$ with the character $a \mapsto a(x)$. Since $(ab)(x) = a(x)b(x)$ for all $a, b \in G$ this is a character on G and since G separates points in X this identification is legitimate. Once this is identification is made, $x(a) = a(x)$ so $Ker(x) = \{a \in G : a(x) = 1\}$ and $\bigcap_{x\in X} Ker(x) = \{1\}$. It follows from this and 4.1.1(iii) that X generates $\chi(G)$ topologically, i.e, $\chi(G)$ is the smallest closed subgroup of $\chi(G)$ containing X.

If $a, b \in G$ we define the **value set** *$D(a, b)$ to be the set of all $c \in G$ such that for each $x \in X$ either $c(x) = a(x)$ or $c(x) = b(x)$. In particular, a and b are both elements of $D(a, b)$.*

AX2 - *If $x \in \chi(G)$ satisfies $x(-1) = -1$ and $a, b \in ker(x) \Rightarrow D(a, b) \subseteq ker(x)$, then x is in the image of the natural embedding $X \hookrightarrow \chi(G)$.*

AX3 (Associativity) - *For all $a, b, c \in G$, if $t \in D(a, r)$ for some $r \in D(b, c)$ then $t \in D(s, c)$ for some $s \in D(a, b)$.*

Elements of X are often referred to as *orderings*. If $x \in X$, $\ker(x)$ is sometimes called the *positive cone* of x.

If $x \in X$ then, viewing x as a character on G, we have $x(-1) = (-1)x = -1$ and $a, b \in \ker(x) \Rightarrow D(a, b) \subseteq \ker(x)$. AX2 is just saying that every character on G having these properties is in X. AX1 and AX2 are trivial in the sense that they can be "forced" in a natural way: suppose X is any set and G is any subgroup of $\{-1, 1\}^X$ containing the constant function -1. Let $\tilde{X}$ denote the set of all characters $x \in G$ satisfying the conditions of the hypothesis of AX2. Then $(\tilde{X}, G)$ satisfies AX1 and AX2 and the binary values sets $D(a, b)$ for $(\tilde{X}, G)$ are the same as those for (X, G). Of course, if (X, G) is already itself satisfies AX1 and AX2, then $\tilde{X} = X$.

Thus, in a certain sense, AX3 is the only non-trivial axiom. In the concrete case (X_T, G_T), AX3 is just saying that what remains of the addition is associative.

Since the definition of a space of orderings is motivated by the example (X_T, G_T) considered above, it is important to chech the following:

Theorem 4.1.7. *If T is a proper preordering in a formally real field F, then the pair (X_T, G_T) is a space of orderings.*

Proof. Since T is proper, $X_T \neq \emptyset$. By 4.1.10, G_T can be viewed as a subgroup of $\{-1, 1\}^{X_T}$, and $-\overline{1} \in G_T$ plays the role of the constant function -1. If $P, Q \in X_T$, $P \neq Q$, then there exists $a \in P$, $a \notin Q$, so $\overline{a}(P) = 1$, $\overline{a}(Q) = -1$. This proves that G_T separates points in X_T.

Suppose $x \in \chi(G_T)$ satisfies the conditions of the hypothesis of AX2 and let

$$P = \{a \in \dot{F} : \overline{a} \in \ker(x)\} \cup \{0\}.$$

Then P is an ordering containing T (to prove that $P+P \subseteq P$ we use that $\overline{a}+\overline{b} \subseteq D(\overline{a}, \overline{b}) \subseteq \ker(x)$). This means that $P \in X_T$ and x is the character on G_T corresponding to P.

Suppose $a_1, a_2, a_3 \in \dot{F}$ and $\overline{b} \in D(\overline{a}_1, \overline{c})$ for some $\overline{c} \in D(\overline{a}_2, \overline{a}_3)$. Using 4.1.4 twice we see that $b = t_1a_1 + t_2a_2 + t_3a_3$ for some $t_1, t_2, t_3 \in T$. If $t_1a_1 + t_2a_2 \neq 0$ then $\overline{b} \in D(\overline{d}, \overline{a}_3)$ where $d = t_1a_1 + t_2a_2$, and $\overline{d} \in D(\overline{a}_1, \overline{a}_2)$. If $t_1a_1 + t_2a_2 = 0$, then $b = t_3a_3$, so we can take $\overline{d} \in D(\overline{a}_1, \overline{a}_2)$ arbitrary in this case. □

For any spacing of orderings (X, G), X has a natural topology, namely the weakest topology such that the functions $a : X \to \{-1, 1\}$, $a \in G$, are continuous, giving $\{-1, 1\}$ the discrete topology.

This can also be described as the topology induced by our natural embedding $X \hookrightarrow \chi(G)$ where $\chi(G)$ is topologized as in last section. The sets

$$U(a) := \{x \in X : a(x) = 1\},\ a \in G,$$

are clopens. Using the fact that $a(x) = -1$ iff $-a(x) = 1$, we see that these sets form a subbasis for the topology on X, i.e, the clopens sets

$$U(a_1, ..., a_n) := \bigcap_{j=1}^{n} U(a_j) = \{x \in X : a_1(x) = ... = a_n(x) = 1\}$$

form a basis for the topology on X.

Theorem 4.1.8. *For any space of orderings (X, G), X is a Boolean space.*

Proof. Let $u : X \hookrightarrow \chi(G)$ be the natural embedding. Since $\chi(G)$ is a Boolean space, it suffices to show that $u(X)$ is closed in $\chi(G)$. This follows from AX2. Suppose $x \in \chi(G)$ is in the closure of $u(X)$. Then, for any elements $a, b, c \in G$, there exist $y \in X$ such that $x(a) = a(y)$, $x(b) = b(y)$, $x(c) = c(y)$ and $x(-1) = (-1)(y)$. This forces $x(-1) = -1$, and if $c \in D(a, b)$, $x(a) = 1$, $x(b) = 1$, it forces $x(c) = 1$. Thus by AX2, $x \in u(X)$. □

Spaces of orderings form a category, i.e, we not only have objects, we also have morphisms.

Definition 4.1.9. *A morphism α from an AOS (X, G) to an AOS (Y, H) is a mapping $\alpha : X \to Y$ such that for each $h \in H$, the composite function $h \circ \alpha : X \to \{-1, 1\}$ is an element of G (and in particular, α is surjective). Note that this implies that α induces a group homomorphism $h \mapsto h \circ \alpha$ from H to G. Also $\alpha^{-1}(U(h)) = U(h \circ \alpha)$ for each $h \in H$, so α is continuous.*

An isomorphism from (X, G) to (Y, H) is a morphism $\alpha : X \to Y$ which is bijective and such that the induced group homomorphism $h \mapsto h \circ \alpha$ is also bijective.

4.1.2 Quadratic Forms and the Witt Ring

We work now with a fixed space of orderings (X, G).

Forms, dimension and discriminant of a form, signatures of a form, and isometry of forms are defined exactly as in the concrete case $(X, G) = (X_T, G_T)$: A (quadratic) **form** with entries in G is an n-tuple $\varphi = \langle a_1, ..., a_n \rangle$, $a_1, ..., a_n \in G$. n is called the **dimension** of φ. $\prod_{j=1}^{n} a_j \in G$ is called the **discriminant** of φ. For each $x \in X$, the **signature** of φ at x is $\varphi(x) := \sum_{j=1}^{n} a_j(x) \in \mathbb{Z}$.

The value set of a binary form $\langle a, b \rangle$ has already been defined. The value set of an n-dimensional form is defined inductively if $n \geq 3$:

$$D\langle a_1, ..., a_n \rangle := \bigcup_{b \in D\langle a_2, ..., a_n \rangle} D\langle a_1, b \rangle.$$

For a 1-dimensional form, we define $D\langle a \rangle := \{a\}$. We say b is **represented** by a form φ if $b \in D(\varphi)$.

We use standard notation from quadratic form theory: If $\varphi = \langle a_1, ..., a_n \rangle$, $\psi = \langle b_1, ..., b_m \rangle$ and $c \in G$, we define

$$\varphi \oplus \psi := \langle a_1, ..., a_n, b_1, ..., b_m \rangle;$$
$$\varphi \otimes \psi := \langle a_1 b_1, ..., a_i b_j, ..., a_n b_m \rangle.$$

Also, if $k \geq 1$, $k \times \varphi = \varphi \oplus ... \oplus \varphi$ k times.

Forms of the shape $\langle 1, a_1\rangle \otimes ... \otimes \langle 1, a_n\rangle$ are called **Pfister forms** (specifically n-fold Pfister forms) and denoted by $\langle\langle a_1, ..., a_n\rangle\rangle$.

Theorem 4.1.10.

i - $D(\varphi)$ *does not depend on the order of entries of* φ.

ii - $D(c\varphi) = cD(\varphi)$ *for any* $c \in G$.

iii - $c \in D(\varphi \oplus \psi)$ *iff* $c \in D(a, b)$ *for some* $a \in D(\varphi)$, $b \in D(\psi)$.

iv - $c \in D(\varphi_1 \oplus ... \oplus \varphi_k)$ *iff* $c \in D(a_1, ..., a_k)$ *for some* $a_i \in D(\varphi_i)$, $i = 1, ..., k$.

Proof.

i - We proof by induction on $n = \dim(\varphi)$. Let $\varphi = \langle a_1, ..., a_n\rangle$. The result is immediate if $n = 1$ or $n = 2$. Suppose $n \geq 3$. It suffices to show that the value set does not change if we permute two adjacent entries a_i, a_j. If $i, j \geq 2$, this follows by induction step. This leaves the case $i = 1$, $j = 2$. Suppose $b \in D\langle a_2, a_1, ..., a_n\rangle$. Thus $b \in D\langle a_2, c\rangle$, $c \in D\langle a_1, d\rangle$, $d \in D\langle a_3, ..., a_n\rangle$. By AX3, $b \in D\langle a_1, e\rangle$ for some $e \in D\langle a_2, d\rangle$. This proves that $b \in D\langle a_1, a_2, ..., a_n\rangle$.

ii - This is an immediate consequence of the definition of D. Recall that $c^2 = 1$.

iii - Let $\varphi = \langle a_1, ..., a_k\rangle$, $\psi = \langle a_{k+1}, ..., a_n\rangle$.

($\Rightarrow$): If $k = 1$, $c \in D\langle a_1, b\rangle$, $b \in D\langle a_2, ..., a_n\rangle$ so we can take $a = a_1$. If $k \geq 2$ then $c \in D\langle a_1, d\rangle$, $d \in D(\varphi' \oplus \psi)$ where $\varphi' = \langle a_2, ..., a_k\rangle$. By induction, we have $d \in D\langle e, f\rangle$, $e \in D(\varphi')$, $f \in D(\psi)$. By AX3 we have $c \in D\langle g, f\rangle$ for some $g \in D\langle a_1, e\rangle$. Thus $g \in D(\psi)$ so we can take $a = g$, $b = f$.

($\Leftarrow$): If $k = 1$ then $c \in D\langle a_1, b\rangle$ (since $a \in D\langle a_1\rangle$ so $a = a_1$) so $c \in D(\varphi \oplus \psi)$. If $k \geq 2$ then $a \in D\langle a_1, d\rangle$, $d \in D(\varphi')$ where $\varphi' = \langle a_2, ..., a_k\rangle$. By AX3, $c \in D\langle a_1, e\rangle$ where $e \in D\langle d, b\rangle$. By induction on k, $e \in D(\varphi' \oplus \psi)$. This proves $c \in D(\varphi \oplus \psi)$.

iv - This follows from (iii) by induction on k.

□

We say that a set $M \subseteq G$ is **additively closed** if $a, b \in M$ implies $D\langle a, b\rangle \subseteq M$.

Corollary 4.1.11.

i - $D(\varphi)$ *is the smallest additively closed set containing the entries of* φ.

ii - $D(k \times \varphi = D(\varphi)$ *for each* $k \geq 1$.

Proof.

i - Say $\varphi = \langle a_1, ..., a_n\rangle$. Using

$$D\langle a_1, ..., a_n\rangle = \bigcup_{b \in \langle a_2, ..., a_n\rangle} D\langle a_1, b\rangle$$

and induction on n, we see that any additively closed set containing $a_1, ..., a_n$ must contain $D(\varphi)$. Thus it only remains to check that $D(\varphi)$ is additively closed. Suppose $a, b \in D(\varphi)$ and $c \in D\langle a, b\rangle$. Then $c \in D(\varphi \oplus \varphi)$ and by 4.1.10(i),

$$D(\varphi \oplus \varphi) = D(\langle a_1, a_1\rangle \oplus ...\langle a_n, a_n\rangle)$$

so, by 4.1.10(iv), $c \in D\langle d_1, ..., d_n\rangle$ for some $d_1 \in D\langle a_i, a_i\rangle$, $i = 1, ..., n$. Thus $d_i(x) = a_i(x)$ for all $x \in X$ so $d_i = a_i$, $i = 1, ..., n$, hence $c \in D(\varphi)$.

ii - This follows by (i) since φ and $k \times \varphi$ have the same entries.

□

Definition 4.1.12. *The relation $\cong$ (called isometry) on forms with entries in G is defined as follows: For 1-dimensional forms $\langle a\rangle \cong \langle b\rangle$ is defined to mean $a = b$. For 2-dimensional forms $\langle a_1, a_2\rangle \cong \langle b_1, b_2\rangle$ is defined to mean that the two forms have the same signature, i.e, $a_1(x)+a_2(x) = b_1(x)+b_2(x)$ for all $x \in X$. For $n \geq 3$, the isometry relation $\cong$ is defined inductively by $\langle a_1, ..., a_n\rangle \cong \langle b_1, ..., b_n\rangle$ iff there are $a, b, c_3, ..., c_n \in A$ such that $\langle a_1, a\rangle \cong \langle b_1, b\rangle$, $\langle a_2, ..., a_n\rangle \cong \langle a, c_3, ..., c_n\rangle$ and $\langle b_2, ..., b_n\rangle \cong \langle b, c_3, ..., c_n\rangle$.*

Theorem 4.1.13 (Alternative description of value sets and isometry)**.**

i - $b_1 \in D(\varphi) \Leftrightarrow \varphi \cong \langle b_1, ..., b_n\rangle$ for some $b_1, ..., b_n \in G$, where $n = \dim \varphi$.

ii - $\varphi \cong \psi \Leftrightarrow \dim \varphi = \dim \psi$ and $\varphi(x) = \psi(x)$ for all $x \in X$.

The proof of this will be made in next section. It is hard to overemphasize the importance of 4.1.13. It allows us to describe a space of orderings in a completely different way:

Definition 4.1.14 (Alternative definition of Space of Ordering)**.** *A space of ordering can be defined to be a pair (X, G) satisfying the following axioms:*

(α) *X is a non-empty set, G is a subgroup of $\{-1, 1\}^X$ containing the constant function -1, and G separates points in X.*

(β) *The image of the natural embedding $u : X \hookrightarrow \chi(G)$, $x \mapsto (a \mapsto a(x))$ is closed in $\chi(G)$.*

(γ) *If φ, ψ are forms with entries in G and $c \in D(\varphi \oplus \psi)$, then $c \in D(a, b)$ for some $\in D(\varphi)$, $b \in D(\psi)$.*

Here (**and this is crucial**), the value sets and isometry are supposed to be defined as in the statement of 4.1.13, i.e, $\varphi \cong \psi$ is defined to mean that $\dim(\varphi) = \dim(\psi)$ and $\varphi(x) = \psi(x)$ for all $x \in X$, and $D(\varphi)$ denotes the set of all elements $b \in G$ such that $\varphi \cong \langle b, b_2, ..., b_n\rangle$ for some $b_2, ..., b_n \in G$ (where $n = \dim(\varphi)$).

Theorem 4.1.15. *The two description of a space of orderings are equivalent.*

Proof. Suppose (X, G) is a space of orderings. (α) is just AX1. As explained in the proof of 4.1.8, (β) is a consequence of AX2. According to 4.1.13 the definitions of isometry and value set coincide with the alternate definitions, so (γ) is just 4.1.10(iii).

Conversely, suppose (X, G) is a space of orderings in the alternate sense. AX1 is just (α). Now, suppose $x \in \chi(G)$ satisfies the conditions given in AX2. We want to show that $x \in X$. By (β), X is closed in $\chi(G)$ so if $x \notin X$, then we have some open set S in $\chi(G)$ with $x \in S$ and $S \cap X = \emptyset$. Since $x(-1) = -1$ we can suppose S has the form

$$S = \{y \in \chi(G) : y(a_i) = 1,\ a_1, ..., a_n \in G\}.$$

Consider the Pfister form $\varphi = \langle 1, a_1\rangle \otimes ... \otimes \langle 1, a_n\rangle$. For any $y \in X$, $a_i(y) = -1$ for some i so

$$\varphi(y) = \prod_{j=1}^{n}(1 + a_j(y)) = 0.$$

According to our definition of isometry and value sets, this means $\varphi \cong 2^{n-1} \times \langle 1, -1\rangle$, so $-1 \in D(\varphi)$. On the other hand, expanding φ as $\varphi \cong \psi \oplus a_1\psi$ where $\psi = \langle 1, a_2\rangle \otimes ... \otimes \langle 1, a_n\rangle$, and using (γ) and induction on n, we see that $D(\varphi) \subseteq \ker(x)$. Suppose $a \in D(\varphi)$. By (γ), $a \in D(b, a_1c)$ for some $b, c \in D(\psi)$ and, by induction on n, $b, c \in \ker(x)$. Since x satisfies the conditions of AX2 and $a_1 \in \ker(x)$, this forces $a \in \ker(x)$. Since $-1 \in D(\varphi)$, this yields $-1 \in \ker(x)$, a contradiction. This proves that (X, G) satisfies AX2.

Suppose $b \in D\langle a_1, c\rangle$ for some $c \in D\langle a_2, a_3\rangle$. Then

$$\langle a_1, a_2, a_3\rangle \cong \langle a_1, c, a_2a_3c\rangle \cong \langle b, a_1bc, a_2a_3c\rangle,$$

so $b \in D\langle a_1, a_2, a_3\rangle$. By (γ), there exists $d \in D\langle a_1, a_2\rangle$ such that $b \in D\langle d, a_3\rangle$. This proves AX3. □

Actually, there is another description of space of orderings: the structure $(X, G, -1)$ is an AOS if it verifies the following conditions:

O1 - X is closed in $\chi(G)$ (equivalently, in $\{\pm 1\}^G$).

O2 - $\sigma(-1) = -1$ for all $\sigma \in X$.

O3 - $\bigcap_{\sigma \in X} \mathrm{Ker}(\sigma) = \{1\}$.

O4 - If φ, ψ are forms over G and $x \in G$, then $x \in D_X(\varphi \oplus \psi)$ implies that there are $y \in D_X(\varphi)$ and $z \in D_X(\psi)$ such that $x \in D_X(y, z)$.

The content of this definition is the same. (α) and (β) collectively are equivalent to O1, O2 and O3. (γ) is just O4.

For the rest of this section we will develop some basic properties of $\cong$.

Theorem 4.1.16.

a - If $b_i = a_{\pi(i)}$, $i = 1, ..., n$ for some permutation π of $\{1, ..., n\}$, then $\langle a_1, ..., a_n\rangle \cong \langle b_1, ..., b_n\rangle$.

b - $\varphi \cong \psi \Rightarrow \dim \varphi = \dim \psi$, $disc(\varphi) = disc(\psi)$, $\varphi(x) = \psi(x)$ for all $x \in X$, $D(\varphi) = D(\psi)$ and $c\varphi \cong c\psi$ for all $c \in G$.

c - The relation $\cong$ is an equivalence relation.

d - For any forms $\varphi, \varphi', \psi, \psi'$ over G, if $\varphi \cong \varphi'$ and $\psi \cong \psi'$ then $\varphi \oplus \psi \cong \varphi' \oplus \psi'$.

e - (Witt's Cancellation) For any forms $\varphi, \varphi', \psi, \psi'$ over G, if $\varphi \cong \varphi'$ and $\varphi \oplus \psi \cong \varphi' \oplus \psi'$ then $\psi \cong \psi'$.

Proof.

a - We prove by induction on n. If $n = 1$ or 2 there is nothing to show. Now, suppose $n \geq 3$. We have two cases:

Case $\pi(1) = i \geq 2$ - take $a = a_i$, $b = a_1$ and $c_3, ..., c_n$ to be the elements left after a_1 and a_i are deleted from the list $a_1, ..., a_n$. Then $a, c_3, ..., c_n$ is a permutation of $a_2, ..., a_n$, $b, c_3, ..., c_n$ a permutation of $b_2, ..., b_n$ and b_1, b is a permutation of a_1, a. So by induction we have

$$\langle a_1, a\rangle \cong \langle b_1, b\rangle,\ \langle a_2, ..., a_n\rangle \cong \langle a, c_3, ..., c_n\rangle \text{ and } \langle b_2, ..., b_n\rangle \cong \langle b, c_3, ..., c_n\rangle.$$

Then $\langle a_1, ..., a_n\rangle \cong \langle b_1, ..., b_n\rangle$.

Case $\pi(1) = 1$ **-** take $a = b = a_2$ and $c_i = a_i$ for $i \geq 2$ to be the witnesses of the isometry $\langle a_1, ..., a_n\rangle \cong \langle b_1, ..., b_n\rangle$.

b - The fact that $\varphi \cong \psi \Rightarrow \dim\varphi = \dim\psi$ is already encapsuled in definition of $\cong$ (4.1.12). To prove the other statements we use induction. Suppose $\varphi = \langle a_1, ..., a_n\rangle$ and $\psi = \langle b_1, ..., b_n\rangle$.

For $\varphi \cong \psi \Rightarrow \mathrm{disc}(\varphi) = \mathrm{disc}(\psi)$, if $\dim\varphi = 1$ there is nothing to do. If $\dim\varphi = 2$ and $a_1(x)a_2(x) \neq b_1(x)b_2(x)$ for some $x \in X$, then $a_1(x) + a_2(x) \neq b_1(x) + b_2(x)$, its contradict the definition of 2-isometry. Now, if $\dim\varphi = n$, there are $a, b, c_3, ..., c_n \in A$ such that

$$\langle a_1, a\rangle \cong \langle b_1, b\rangle,\ \langle a_2, ..., a_n\rangle \cong \langle a, c_3, ..., c_n\rangle \text{ and} \langle b_2, ..., b_n\rangle \cong \langle b, c_3, ..., c_n\rangle.$$

By induction, we have

$$\begin{aligned} a_1a &= b_1b \\ a_2...a_n &= ac_3...c_n \\ b_2...b_n &= bc_3...c_n \end{aligned}$$

so

$$a_1a_2...a_n = a_1ac_3...c_n = b_1bc_3...c_n = b_1b_2...b_n.$$

For $\varphi \cong \psi \Rightarrow \varphi(x) = \psi(x)$ for all $x \in X$, if $\dim\varphi = 1$ or 2 this is already in definition 4.1.12. Now, if $\dim\varphi = n$, there are $a, b, c_3, ..., c_n \in A$ such that

$$\langle a_1, a\rangle \cong \langle b_1, b\rangle,\ \langle a_2, ..., a_n\rangle \cong \langle a, c_3, ..., c_n\rangle \text{ and} \langle b_2, ..., b_n\rangle \cong \langle b, c_3, ..., c_n\rangle.$$

By induction, we have

$$\begin{aligned} a_1(x) + a(x) &= b_1(x) + b(x) \\ a_2(x) + ... + a_n(x) &= a(x) + c_3(x) + ... + c_n(x) \\ b_2(x) + ... + b_n(x) &= b(x) + c_3(x) + ... + c_n(x) \end{aligned}$$

so

$$\begin{aligned} a_1(x) + a_2(x) + ... + a_n(x) &= a_1(x) + a(x) + c_3(x) + ... + c_n(x) \\ &= b_1(x) + b(x) + c_3(x) + ... + c_n(x) \\ &= b_1(x) + b_2(x) + ... + b_n(x). \end{aligned}$$

For $\varphi \cong \psi \Rightarrow D(\varphi) = D(\psi)$, since $\langle a_1, ..., a_n\rangle \cong \langle b_1, ..., b_n\rangle$, $\{a_1, ..., a_n\} \subseteq D\langle b_1, ..., b_n\rangle$. By 4.1.11(ii) $D\langle a_1, ..., a_n\rangle \subseteq D\langle b_1, ..., b_n\rangle$. By the same argument we have $D\langle b_1, ..., b_n\rangle \subseteq D\langle a_1, ..., a_n\rangle$, and so, the equality.

Finally, for $\varphi \cong \psi \Rightarrow c\varphi \cong c\psi$ for all $c \in G$, if $\dim\varphi = 1$ there is nothing to do and if $\dim\varphi = 2$, by

$$a_1(x) + a_2(x) = b_1(x) + b_2(x) \Rightarrow c(x)a_1(x) + c(x)a_2(x) = c(x)b_1(x) + c(x)b_2(x)$$

we obtain $c\varphi \cong c\psi$. Now, if $\dim\varphi = n$, there are $a, b, c_3, ..., c_n \in A$ such that

$$\langle a_1, a\rangle \cong \langle b_1, b\rangle,\ \langle a_2, ..., a_n\rangle \cong \langle a, c_3, ..., c_n\rangle \text{ and} \langle b_2, ..., b_n\rangle \cong \langle b, c_3, ..., c_n\rangle.$$

By induction, we have

$$\langle ca_1, ca\rangle \cong \langle cb_1, cb\rangle,\ \langle ca_2, ..., ca_n\rangle \cong \langle ca, cc_3, ..., cc_n\rangle \text{ and} \langle cb_2, ..., cb_n\rangle \cong \langle cb, cc_3, ..., cc_n\rangle.$$

Then $c\varphi \cong c\psi$.

c - We just need to prove transitivity. Suppose φ, ψ, τ are n-dimensional forms, saying $\varphi = \langle a_1, ..., a_n\rangle$, $\psi = \langle b_1, ..., b_n\rangle$, $\tau = \langle c_1, ..., c_n\rangle$; such that $\varphi \cong \psi$ and $\psi \cong \tau$. We show by induction on n that $\varphi \cong \tau$. This is immediate if $n = 1$ or 2 (remember definition 4.1.12).

For $n = 3$, by item (b) we know that $c_1 \in D(\psi) = D(\varphi)$ so $c_1 \in D(a_1, a)$ for some $a \in D(a_2, a_3)$. So there are $c, d_3 \in G$ with $\langle a_1, a\rangle \cong \langle c_1, c\rangle$ and $\langle a_2, a_3\rangle \cong \langle a, d_3\rangle$. Getting these information together, we have:

$$\begin{aligned}\langle c_1, c_2, c_3\rangle = \tau &\cong \psi\\ \psi \cong \varphi &= \langle a_1, a_2, a_3\rangle\\ \langle a_1, a_2, a_3\rangle &= \langle c_1, c, d_3\rangle\end{aligned}$$

comparing signatures (by item (b)), we get

$$c_1(x) + c_2(x) + c_3(x) = c_1(x) + c(x) + d_3(x)$$

for all $x \in X$. Hence $c_2(x) + c_3(x) = c(x) + d_3(x)$ wich yields $\langle c_2, c_3\rangle \cong \langle c, d_3\rangle$. Thus complete the proof that $\varphi \cong \tau$ if $n = 3$.

Now assume $n \geq 4$. Let us write

$$\begin{aligned}\varphi &= \langle a_1, ..., a_n\rangle = \langle a_1\rangle \oplus \varphi'\\ \psi &= \langle b_1, ..., b_n\rangle = \langle b_1\rangle \oplus \psi'\\ \tau &= \langle c_1, ..., c_n\rangle = \langle c_1\rangle \oplus \tau'\end{aligned}$$

Since $\varphi \cong \psi$, there exist $x, y \in G$ and a $n-2$-dimensional form α with

$$\langle a_1, x\rangle \cong \langle b_1, y\rangle,\ \varphi' \cong \langle x\rangle \oplus \alpha \text{ and } \psi' \cong \langle y\rangle \oplus \alpha,$$

and since $\psi \cong \tau$, there exist $z, w \in G$ and another $n-2$-dimensional form β with

$$\langle b_1, z\rangle \cong \langle c_1, w\rangle,\ \psi' \cong \langle z\rangle \oplus \beta \text{ and } \tau' \cong \langle w\rangle \oplus \beta.$$

By induction $\langle y\rangle \oplus \alpha \cong \langle z\rangle \oplus \beta$, so there exist $u, v \in G$ and a $n-3$-dimensional form γ with

$$\langle u, y\rangle \cong \langle v, z\rangle\ \alpha \cong \langle u\rangle \oplus \gamma \text{ and } \beta \cong \langle v\rangle \oplus \gamma.$$

Putting these isometries together and using transitivity in the $n = 3$, we get

$$\langle a_1, x, u\rangle \cong \langle b_1, y, u\rangle \cong \langle b_1, z, v\rangle \cong \langle c_1, w, v\rangle;$$

hence $\langle a_1, x, u\rangle \cong \langle c_1, w, v\rangle$ provides $a, c, d \in G$ such that

$$\langle a_1, a\rangle \cong \langle c_1, c\rangle,\ \langle x, u\rangle \cong \langle a, d\rangle \text{ and } \langle w, v\rangle \cong \langle c, d\rangle.$$

Take $\delta = \langle d \rangle \oplus \gamma$. Then

$$\varphi' \cong \langle x \rangle \oplus \alpha \cong \langle x, u \rangle \oplus \gamma \cong \langle a, d \rangle \oplus \gamma = \langle a \rangle \oplus \delta$$
$$\tau' \cong \langle w \rangle \oplus \beta \cong \langle w, v \rangle \oplus \gamma \cong \langle c, d \rangle \oplus \gamma = \langle c \rangle \oplus \delta.$$

By induction again, we get $\varphi' \cong \langle a \rangle \oplus \delta$ and $\tau' \cong \langle c \rangle \oplus \delta$. Since $\langle a_1, a \rangle \cong \langle c_1, c \rangle$, this implies $\varphi \cong \tau$.

d - Since $\varphi \oplus \psi \cong \psi \oplus \varphi$ and $\varphi \otimes \psi \cong \psi \otimes \varphi$ by item (a), it suffices to prove this in the case where $\varphi = \varphi'$. Since $c\psi \cong c\psi'$ if $\psi \cong \psi'$ by item (b), it suffices to prove the result for $\oplus$. On the other hand, since

$$\langle a_1, ..., a_n \rangle \oplus \psi = \langle a_1 \rangle \oplus (\langle a_2, ..., a_n \rangle \oplus \psi),$$

by induction on dimension, we are reduced to the case where $\dim(\varphi) = 1$, say $\varphi = \langle a \rangle$.

Let $\psi = \langle x \rangle \oplus \delta$. Then

$$\langle a, x \rangle \cong \langle a, x \rangle,\ \psi \cong \langle x \rangle \oplus \delta \text{ and } \psi' \cong \langle x \rangle \oplus \delta.$$

By definition 4.1.12 $\langle a \rangle \oplus \psi \cong \langle a \rangle \oplus \psi'$.

e - Using the previous item, if $\varphi \cong \varphi'$ then

$$\varphi \oplus \psi \cong \varphi' \oplus \psi' \Rightarrow (\varphi' \oplus \varphi) \oplus \psi \cong (\varphi \oplus \varphi') \oplus \psi'$$

and by transitivity of $\cong$, it suffices to prove this in the case where $\varphi = \varphi'$. Again, since

$$\langle a_1, ..., a_n \rangle \oplus \psi = \langle a_1 \rangle \oplus (\langle a_2, ..., a_n \rangle \oplus \psi),$$

by induction on dimension, we are reduced to the case where $\dim(\varphi) = 1$.

Let $\varphi = \langle a \rangle$ and suppose $\langle a \rangle \oplus \psi \cong \langle a \rangle \oplus \psi'$. By definition, there are $x, y \in G$ and a $n-2$ dimensional form δ such that

$$\langle a, x \rangle \cong \langle a, y \rangle,\ \psi \cong \langle x \rangle \oplus \delta \text{ and } \psi' \cong \langle y \rangle \oplus \delta.$$

Comparing discriminants we get $x = y$, then

$$\psi \cong \langle x \rangle \oplus \delta \cong \langle y \rangle \oplus \delta \cong \psi'$$

and by transitivity, $\psi \cong \psi'$.

□

Consider now the set of equivalence classes of forms over G with respect to the equivalence relation $\cong$. By 4.1.16(d), the operations $\oplus$ and $\otimes$ on forms induce binary operations of this set. Associativity and commutativity of these operations and the distributive property follow from 4.1.16(a). Thus, the resulting structure is "almost" a ring, but additive inverse fail to exist.

To retify this situation we got a slightly coarser equivalence relation called Witt equivalence. A form $\langle a, -a \rangle$, $a \in G$, is called a **hyperbolic form** or a **hyperbolic plane**. Note that $\langle a, -a \rangle \cong \langle 1, -1 \rangle$ for any $a \in G$. we say φ and ψ are **Witt equivalent**, denoted $\varphi \sim \psi$, if there exist integers $k, l \geq 0$ such that

$$\varphi \oplus k \times \langle 1, -1 \rangle \cong \psi \oplus l \times \langle 1, -1 \rangle.$$

This is an equivalence relation and the sum and product of forms induce binary operations on the set of equivalence classes of forms with respect to Witt equivalence. The resulting system is a commutative ring with 1. We will denote this ring by $W = W(X, G)$, and refer to it as the **Witt ring** associated to the space of orderings (X, G). The zero of W is the class of the empty form $0 = \langle\rangle$ and the unity of W is the class of $\langle 1\rangle$. The additive inverse of the class of $\varphi = \langle a_1, ..., a_n\rangle$ is the class of $-\varphi = \langle a_1, ..., a_n\rangle$.

Definition 4.1.17. *A form φ will be called isotropic if there exists a form ψ such that $\varphi \cong \langle 1, -1\rangle \oplus \psi$. Otherwise, φ will be called **anisotropic**. A form φ is said to be universal if $D(\varphi) = G$.*

Theorem 4.1.18.

i - $\varphi \cong \psi \Leftrightarrow \varphi \sim \psi$ *and* $\dim \varphi = \dim \psi$.

ii - φ *is isotropic iff there exists a form* ψ *with* $\varphi \sim \psi$, $\dim \varphi > \dim \psi$.

iii - φ *is isotropic iff* φ *is universal iff* $D(\varphi) \cap D(-\varphi) \neq \emptyset$.

iv - *If* φ *is anisotropic then so is* $n \times \varphi$ *for any* $n \geq 1$.

v - *If* $\varphi \oplus \psi$ *is isotropic then there exists* $b \in D(\varphi)$ *with* $-b \in D(\psi)$.

Proof.

i - ($\Rightarrow$) is clear (taking $k = l = 0$). For ($\Leftarrow$), suppose

$$\varphi \oplus k \times \langle 1, -1\rangle \cong \psi \oplus l \times \langle 1, -1\rangle.$$

Comparing dimensions and using $\dim \varphi = \dim \psi$, this yields $k = l$. Thus $\varphi \cong \psi$ by Witt's cancellation.

ii - ($\Rightarrow$) is immediate from definition. For ($\Leftarrow$) suppose

$$\varphi \oplus k \times \langle 1, -1\rangle \cong \psi \oplus l \times \langle 1, -1\rangle.$$

Then, comparing dimensions and using $\dim \varphi > \dim \psi$, this yields $k < l$. Thus, by Witt's cancellation, $\varphi \cong (k - l) \times \langle 1, -1\rangle \oplus \psi$, so φ is isotropic.

iii - Suppose $\varphi \cong \langle 1, -1\rangle \oplus \psi$. Since $\langle 1, -1\rangle \cong \langle a, -a\rangle$ for all $a \in G$, this yields $\varphi \cong \langle a, -a\rangle \oplus \psi$, so $a \in D(\varphi)$ by 4.1.13(a). In the sequence, if φ is universal, then

$$D(\varphi) = G \Rightarrow D(\varphi) \cap D(-\varphi) \neq \emptyset.$$

Now suppose $D(\varphi) \cap D(-\varphi) \neq \emptyset$, say $\varphi = \langle a_1, a_2, ..., a_n\rangle$, $-a_1 \in D(\varphi)$. Since $D\langle a_1\rangle = \{a_1\}$ and $-a_1 \neq a_1$, we get $n \geq 2$. Also, $-a_1 \in D(\varphi)$ so $-a_1 \in D(a_1, a)$ for some $a \in D(a_2, ..., a_n)$. Then given $x \in X$, by definition of D we get $-a_1(x) = a_1(x)$ or $-a_1(x) = a(x)$, and we obtain $-a_1 = a$. Thus $-a_1 \in D(a_2, ..., a_n)$ and by 4.1.13(i), $\langle a_2, ..., a_n\rangle \cong -a_1, c_3, ..., c_n\rangle$ for some $c_3, ..., c_n \in G$. Thus

$$\varphi \cong \langle a_1, ..., a_n\rangle \cong a_1, -a_1, c_3, ..., c_n\rangle \cong \langle 1, -1, c_3, ..., c_n\rangle.$$

This proves that φ is isotropic.

iv - By 4.1.11(ii), $D(n \times \varphi) = D(\varphi)$, so this is immediate from (iii).

v - Say $\varphi = \langle a \rangle \oplus \varphi'$. By hypothesis, $\varphi \oplus \psi \cong \langle 1, -1 \rangle \oplus \tau \cong \langle a, -a \rangle \oplus \tau$, so, by Witt's cancellation, $\varphi' \oplus \psi \cong \langle -a \rangle \oplus \tau$, i.e, $-a \in D(\varphi' \oplus \psi)$. If φ is 1-dimensional then $\varphi' \oplus \psi = \psi$ and we can take $b = a$. Otherwise, by 4.1.13, we get $c \in D(\varphi')$, $d \in D(\psi)$ such that $-a \in D(c, d)$. Then $\langle c, d \rangle \cong \langle -a, -acd \rangle$, i.e, $\langle a, c \rangle \cong \langle -d, -acd \rangle$, so $-d \in D(a, c) \subseteq D(\varphi)$. Thus we can take $b = -d$ in this case.

□

4.1.3 Pfister's local-global principle

Theorem 4.1.19 (Pfister's local-global principle)**.** *For any forms φ, ψ with entries in G,*

$$\varphi \sim \psi \Leftrightarrow \varphi(x) = \psi(x) \text{ for all } x \in X.$$

Proof. If $\varphi \sim \psi$ then, using 4.1.16(b) plus the fact that $\langle 1, -1 \rangle$ has signature 0, we see that $\varphi(x) = \psi(x)$ for any $x \in X$. For the other implication, by considering the form $\varphi \oplus -\psi$, it suffices to show that if $\varphi(x) = 0$ for all $x \in X$ then $\varphi \sim 0$.

Suppose $\varphi \nsim 0$. By 4.1.18(b), we can suppose φ anisotropic. By 4.1.18(d), $2^n \times \varphi \nsim 0$ for all $n \geq 0$. Use Zorn's lemma to choose a multiplicative set S in the Witt ring $W = W(X, G)$ with $2 \in S$ maximal subject to the condition that $\psi \otimes \varphi \nsim 0$ for all $\psi \in S$ (i.e, $S \cap \mathrm{Ann}(\varphi) = \emptyset$, where $\mathrm{Ann}(\varphi) \subseteq W$ denotes the annihilator of φ)[1].

Claim 1. If $a \in G$ then either $\langle 1, a \rangle \in S$ or $\langle 1, -a \rangle \in S$ (but not both).

For this, suppose $\langle 1, a \rangle \notin S$. Since $\langle 1, a \rangle \otimes \langle 1, a \rangle \sim 2 \times \langle 1, a \rangle$ and $2 \in S$, the multiplicative set generated by S and $\langle 1, a \rangle$ is $S \cup (\langle 1, a \rangle \otimes S)$. By the maximality pf S, $\langle 1, a \rangle \otimes \psi_1 \otimes \varphi \sim 0$ for some $\psi_1 \in S$. Similarly, if $\langle 1, -a \rangle \in S$, $\langle 1, -a \rangle \otimes \psi_2 \otimes \varphi \sim 0$ for some $\psi_2 \in S$. Since $2 \sim \langle 1, 1 \rangle \sim \langle 1, a \rangle \otimes \langle 1, -a \rangle$, this implies that $2 \times \psi \times \varphi \sim 0$ where $\psi = \psi_1 \otimes \psi_2$. Since $2 \times \psi \in S$, this is a contradiction. If both $\langle 1, a \rangle$ and $\langle 1, -a \rangle$ are in S, then $\langle 1, a \rangle \otimes \langle 1, -a \rangle \sim 0 \in S$, a contradiction.

Using Claim 1, we have a well-defined function $x : G \to \{1, -1\}$ given by $x(a) = 1$ if $\langle 1, a \rangle \in S$ and $x(a) = -1$ if $\langle 1, -a \rangle \in S$. Note that

$$\langle 1, a \rangle \in S \Leftrightarrow \langle 1, -a \rangle \notin S \Leftrightarrow \langle 1, -a \rangle \otimes \psi \otimes \varphi \sim 0,$$

i.e, $a\psi \otimes \varphi \sim \psi \otimes \varphi$ for some $\psi \in S$. It follows from this that x is a character on G.

Claim 2. $x \in X$.

For this, suppose $a, b \in \ker(x)$, $c \in D(a, b)$, and $c \notin \ker(x)$. Then $\langle a, b \rangle \cong \langle c, cab \rangle$. Also $a\psi \otimes \varphi \sim \psi \otimes \varphi$, $b\psi \otimes \varphi \sim \psi \otimes \varphi$ and $c\psi \otimes \varphi \sim -\psi \otimes \varphi$ for some $\psi \in S$[2]. Then $\langle a, b \rangle \otimes \psi \otimes \varphi \sim 2 \times \psi \otimes \varphi$, $\langle c, cab \rangle \otimes \psi \otimes \varphi \sim -2 \otimes \psi \otimes \varphi$, so $4 \times \psi \otimes \varphi \sim 0$ contradicting $4 \times \psi \in S$. Thus $a, b \in \ker(x)$, $c \in D(a, b)$ implies $c \in \ker(x)$ so, by AX2, $x \in X$.

To complete the proof we need to show the following:

[1] Of course, sometimes the phrase "use Zorn's lemma to ..." is not elusive, since we need to find a poset, and search for some upper bound that is not appear at first sight. In our proof of Pfister local global principle, could be helpful think in terms of rings and ideals, keeping in mind that this subset S lives in the Witt ring $W = W(X, G)$.

[2] At first time there is no reason to the form ψ be the same for a, b and c. However, if $a\psi_1 \otimes \varphi \sim \psi_1 \otimes \varphi$, $b\psi_2 \otimes \varphi \sim \psi_2 \otimes \varphi$ and $c\psi_3 \otimes \varphi \sim -\psi_3 \otimes \varphi$, we just take $\psi = \psi_1 \otimes \psi_2 \otimes \psi_3$.

Claim 3. $\varphi(x) \neq 0$.
For this, suppose $\varphi = \langle a_1, ..., a_n\rangle$ and let $e_j = a_j(x)$, so

$$\varphi(x) = \sum_{j=1}^{n} a_j(x) = \sum_{j=1}^{n} e_j.$$

By definition of x, $\langle 1, a(x)a\rangle \in S$ for all $a \in G$. Thus $\langle 1, e_j a_j\rangle \in S$ so $\varphi \otimes \prod_{j=1}^{n}\langle 1, e_j a_j\rangle \nsim 0$. On the other hand, $a_i\langle 1, e_i a_i\rangle \cong e_i\langle 1, e_i a_i\rangle$, so

$$\varphi \otimes \prod_{j=1}^{n}\langle 1, e_i a_i\rangle = \langle a_1, ..., a_n\rangle \otimes \prod_{j=1}^{n}\langle 1, e_j a_j\rangle \cong \langle e_1, ..., e_n\rangle \otimes \prod_{j=1}^{n}\langle 1, e_j a_j\rangle.$$

It follows that $\langle e_1, ..., e_n\rangle \nsim 0$. Each e_j is 1 or -1 so this means $\sum_{j=1}^{n} e_j \nsim 0$. □

Now we are in position to prove Theorem 4.1.13:

Proof of Theorem 4.1.13.

i - This is immediate for $n = 1$. if $\langle a_1, a_2\rangle \equiv \langle b_1, b_2\rangle$ then $b_1 \in D\langle a_1, a_2\rangle$ and $a_1a_2 = b_1b_2$ (so $b_2 = a_1a_2b_1$). Conversely, if $b_1 \in D\langle a_1, a_2\rangle$ then $\langle a_1, a_2\rangle \equiv \langle b_1, b_2\rangle$, where $b_2 := a_1a_2b_1$. Now, suppose $n \geq 3$. If $\langle a_1, ..., a_n\rangle \equiv \langle b_1, ..., b_n\rangle$ then we have $a, b, c_3, ..., c_n$ satisfying the conditions written above. Thus $b_1 \in D\langle a_1, a\rangle$ and, by induction, $a \in D\langle a_2, ..., a_n\rangle$, so $b \in D\langle a_1, ..., a_n\rangle$. Conversely, suppose $b_1 \in D\langle a_1, ..., a_n\rangle$. Then $b_1 \in D\langle a_1, a\rangle$ for some $a \in D\langle a_2, ..., a_n\rangle$. Thus $\langle a_1, a\rangle \equiv \langle b_1, b\rangle$ where $b = a_1ab_1$ and, by induction, $\langle a_2, ..., a_n\rangle \equiv \langle a, c_3, ..., c_n\rangle$ for some $c_3, ..., c_n$. Thus $\langle a_1, ..., a_n\rangle \equiv \langle b_1, ..., b_n\rangle$, where $b_2 := b$ and $b_i : c_i$ for $i = 3, ..., n$.

ii - ($\Rightarrow$) is just 4.1.16(b).

($\Leftarrow$) If $\dim\varphi = \dim\psi$ and $\varphi(x) = \psi(x)$ for all $x \in X$ then, applying 4.1.19, we get $\varphi \sim \psi$. Since $\dim\varphi = \dim\psi$, 4.1.18(i) provides $\varphi \cong \psi$.

□

denote $\mathbb{Z}^X$ the set of all functions $f : X \to \mathbb{Z}$. This is a ring with operations define pontwise, i.e,

$$(f + g)(x) = f(x) + g(x),\ (fg)(x) = f(x)g(x).$$

By the ($\Rightarrow$) implication of 4.1.19 we have a well-defined mapping $\sigma : W \to \mathbb{Z}^X$ sending the Witt equivalence class of φ to the function $x \mapsto \varphi(x)$ and it is easy to check that σ is a ring homomorphism.

Corollary 4.1.20. *For any space of orderings (X, G), the natural ring homomorphism*

$$\sigma : W(X, G) \to \mathbb{Z}^X$$

is injective.

Proof. Immediate from 4.1.19. □

Thus we can identify $W = W(X, G)$ with a subring of $\mathbb{Z}^X$ (the subring generated by the elements of G).

Recall that X is given the weakest topology such that each $a \in G$ is continuous. Using the fact that any sum of continuous functions is continuous, we see that W is actually a subring of $C(X, \mathbb{Z})$, the ring of all continuous function from X to $\mathbb{Z}$. Here, $\mathbb{Z}$ is given the discrete topology.

Our next result shows how to recover the space of orderings (X, G) from its Witt ring:

Theorem 4.1.21. *Suppose (X, G) is a space of orderings with Witt ring $W = W(X, G)$. Then:*

i - G is naturally identified with the unit subgroup of W.

ii - X is naturally identified with the set of all ring homomorphisms from W into $\mathbb{Z}$.

Proof.

i - We have

$$a = b \Leftrightarrow \langle a \rangle \cong \langle b \rangle \Leftrightarrow \langle a \rangle \sim \langle b \rangle$$

and $\langle a \rangle \otimes \langle b \rangle \sim \langle ab \rangle$ so the mapping $a \mapsto \langle a \rangle$ identifies G with a subgroup of the unity group of W.

Suppose $\varphi = \langle a_1, ..., a_n \rangle$ is a unity in W. For fixed $x \in X$, let $k =$ the number of positive entries of φ and $l =$ the number of negative entries. Then $k + l = n$ and $k - l = \varphi(x) = \pm 1$. This forces n to be odd, say $n = 2m + 1$, and $\varphi(x) = 1 \Leftrightarrow k = m$, $l = m + 1$ and $\varphi(x) = -1 \Leftrightarrow k = m + 1$, $l = m$. It follows that $\varphi(x) = a(x)$, where $a := (-1)^m \prod_{j=1}^{n} a_j$. From this it follows, using 4.1.19 that $\varphi \sim \langle a \rangle$.

ii - Each $x \in X$ defines a ring homomorphism $\varphi \mapsto \varphi(x)$ from W into $\mathbb{Z}$. Conversely, suppose $f : W \to \mathbb{Z}$ is any ring homomorphism. Consider the function $x : G \to \{-1, 1\}$ given by $x(a) = f(\langle a \rangle)$. Then $x(-1) = -1$, $x(ab) = x(a)x(b)$. Suppose $c \in D(a, b)$ and $x(a) = x(b) = 1$. Then applying f to $\langle a, b \rangle \cong \langle c, cab \rangle$, we see that

$$2 = x(a) + x(b) = x(c)(1 + x(a)x(b)) = 2x(c),$$

so $x(c) = 1$. Thus, by AX2, $x \in X$. Since $f(\langle a \rangle) = x(a) = a(x)$ for all $a \in G$ and W is generated by the 1-dimensional forms $\langle a \rangle$, f coincides with mapping $\varphi \mapsto \varphi(x)$.

□

4.1.4 Subspaces and preorderings

We continue to assume that (X, G) is a space of orderings. Recall: for any $a \in G$, $U(a)$ denotes the set of all $x \in X$ such that $a(x) = 1$. These sets are clopen and form a subbasis for the topology on X. The clopens sets

$$U(a_1, ..., a_n) := \bigcap_{j=1}^{n} U(a_i),\ n \geq 1,\ a_1, ..., a_n \in G,$$

are a basis for the topology.

Definition 4.1.22. *A subset $Y \subseteq X$ is called a subspace of X (more precisely, of (X, G)) if Y is expressible as $Y = \bigcap_{a \in S} U(a)$ for some (not necessarily finite) subset $S \subseteq G$. The subspace generated by a subset Y in X is just the smallest subspace of (X, G) containing Y, i.e, it is the intersection of all sets $U(a)$ such that $a = 1$ on Y. For any subspace Y of X, $G|_Y$ denotes the group of all restrictions $a|_Y$, $a \in G$ and, for any form $\varphi = \langle a_1, ..., a_n \rangle$ with entries in G, $\varphi|_Y$ denotes the associated form with entries in $G|_Y$, i.e, $\varphi|_Y = \langle a_1|_Y, ..., a_n|_Y \rangle$.*

When we speak of a subspace Y of (X, G), we are often referring to the pair $(Y, G|_Y)$. If $Y \neq \emptyset$, we will prove that this is a space of orderings, conform 4.1.25.

Let F be a formally real field. Subspaces of the full space of orderings $(X_{\sum F^2}, G_{\sum F^2})$ have the form (X_T, G_T) where T is a preordering in F. If $Y \subseteq X_{\sum F^2}$ is a subspace, say $\bigcap_{\overline{a}\in S} U(\overline{a})$, then $Y = X_T$ where T is the preordering in F generated by the elements a, $\overline{a} \in S$, and $G|_Y = G_T$. If T is a preordering of F, then $X_T = \bigcap_{a\in T\setminus\{0\}} U(\overline{a})$. If T, T' are preorderings in F then $X_{T'}$ is a subspace of X_T iff $T' \supseteq T$.

A **preordering** in G is a subgroup T of G which is additively closed, i.e, $a, b \in T \Rightarrow D(a, b) \subseteq T$.

Our first objective is to relate subspaces, preorderings and Pfister forms.

Theorem 4.1.23.

i - Let $\psi = \langle 1, c_1\rangle \oplus ... \oplus \langle 1, c_k\rangle$, $Y = U(c_1, ..., c_k)$. Then the preordering generated by $c_1, ..., c_k$ is

$$D(\psi) = \{b \in G : b\psi \cong \psi\} = \{b \in G : b = 1 \text{ on } Y\}.$$

ii - For any set $S \subseteq G$, the preordering generated by S is $\{b \in G : b = 1 \text{ on } \bigcap_{c\in S} U(c)\}$.

Proof.

i - Denote the preordering generated by $c_1, ..., c_k$ by T. ψ is the sum of the s-dimensional forms $\langle c_{i_1}, ..., c_{i_s}\rangle$, $1 \leq i_1 < ... < i_s \leq k$, $0 \leq s \leq k$, so, according to 4.1.11(i), $D(\psi)$ is the smallest addtively closed subset of G containing the products $c_{i_1}, ..., c_{i_s}$. Since these products are in T, this yields the inclusion $D(\psi) \subseteq T$. Since the set $\{b \in G : b = 1 \text{ on } Y\}$ is a preordering containing $c_1, ..., c_k$ we also have $T \subseteq \{b \in G : b = 1 \text{ on } Y\}$.

Suppose now that $b \in G$, $b = 1$ on Y. Comparing signatures and using 4.1.13, we see that $\psi \cong b\psi$ (the signature of each side at x is 2^n if $x \in Y$ and 0 otherwise). Finally, since $1 \in D(\psi)$, $\psi \cong b\psi$ implies $b \in D(\psi)$, completing the proof.

ii - By the same argument in previous item we have $\subseteq$. For the other, suppose $b = 1$ on $\bigcap_{c\in S} U(c)$. Since b is continuous and X is compact, this implies that $b = 1$ on $U(c_1, ..., c_k)$ for some finite subset $\{c_1, ..., c_k\} \subseteq S$. Thus, by item (i), b lies in the preordering generated by $c_1, ..., c_k$.

□

Corollary 4.1.24. *There is a natural one-to-one inclusion reversing correspondence between subspaces of X and preorderings in G.*

Proof. If Y is any subspace, then $T = \{b \in G : b = 1 \text{ on } Y\}$ is a preordering. If $T \subseteq G$ is any preordering then $Y = \bigcap_{c\in T} U(c)$ is a subspace and by 4.1.23(ii), $T = \{b \in G : b = 1 \text{ on } Y\}$. □

Observe that the kernel of the surjective group homomorphism $G \mapsto G|_Y$, $a \mapsto a|_Y$, is precisely the preordering corresponding to Y.

Theorem 4.1.25. *For any (non-empty) subspace $Y \subseteq X$, the pair $(Y, G|_Y)$ is a space of orderings.*

We prove 4.1.25 by showing that $(Y, G|_Y)$ satisfies the axioms (α), (β) and (γ) of the alternative definition. We use the following result:

Theorem 4.1.26.

i - Suppose $\psi = \langle 1, c_1\rangle \oplus ... \oplus \langle 1, c_k\rangle$, $Y = U(c_1, ..., c_k)$, $\varphi = \langle a_1, ..., a_n\rangle$ *and* $\varphi|_Y = \langle a_1|_Y, ..., a_n|_Y\rangle$. *Then*

$$\begin{aligned} b|_Y \in D(\varphi|_Y) &\Leftrightarrow b \in D(\varphi \otimes \psi) \\ &\Leftrightarrow b \in D(a_1 s_1, ..., a_n s_n) \text{ for some } s_1, ..., s_n \in D(\psi). \end{aligned}$$

ii - Suppose $Y \subseteq X$ *is any subspace. Then* $b|_Y \in D(a_1|_Y, ..., a_n|_Y) \Leftrightarrow b \in D(a_1 s_1, ..., a_n s_n)$ *for some* $s_1, ..., s_n \in G$ *such that* $s_i = 1$ *on* Y, $i = 1, ..., n$.

Proof. Here we are using the alternate definition of value sets and isometry. In the end, both definitions are the same, see 4.1.13.

i - Suppose $b|_Y \in D(\varphi|_Y)$ so $\varphi \cong \langle b_1, ..., b_n\rangle$ on Y for some $b_1, ..., b_n \in G$ with $b_1 = b$. Comparing signatures, $\varphi \otimes \psi \cong \langle b_1, ..., b_n\rangle \otimes \psi$ on X. Since $1 \in D(\varphi)$, this proves $b = b_1 \in D(\varphi \otimes \psi)$. In turn, using $\varphi \otimes \psi \cong a_1\psi \oplus ... \oplus a_n\psi$ and (γ), $b \in D(\varphi \otimes \psi)$ implies that $b \in D(a_1 s_1, ..., a_n s_n)$ for some $s_1, ..., s_n \in D(\psi)$. In turn, since $s_i = 1$ on Y, this implies $b|_Y \in D(\varphi|_Y)$.

ii - The implication $(\Leftarrow)$ follow immediate by the definitions involved in. For $(\Rightarrow)$, say $Y = \bigcap_{c\in S} U(c)$. By assumption $\langle a_1, ..., a_n\rangle \cong \langle b_1, ..., b_n\rangle$ on Y for some $b_1, ..., b_n \in G$ with $b_1 = b$. Y is the intersection of the sets $U(c_1, ..., c_k)$, $c_1, ..., c_k \in S$ and the function

$$x \mapsto \sum_{j=1}^{n} a_j(x) - \sum_{j=1}^{n} b_j(x)$$

is continuous so, by compactness, $\langle a_1, ..., a_n\rangle \cong \langle b_1, ..., b_n\rangle$ on $U(c_1, ..., c_k)$ for some $c_1, ..., c_k \in S$. By (i) we get $b \in D(a_1 s_1, ..., a_n s_n)$ where $s_i \in D(\langle 1, c_1\rangle \oplus ... \oplus \langle 1, c_k\rangle)$, $i = 1, ..., n$. Since $Y \subseteq U(c_1, ..., c_k)$ and $s_i = 1$ on $U(c_1, ..., c_k)$ we see that $s_i = 1$ on Y, $i = 1, ..., n$.

□

Proof of Theorem 4.1.25. (α) and (β) are direct consequence of definition 4.1.22. For (γ), suppose $a|_Y \in D(\varphi|_Y \oplus \psi|_Y)$, $\varphi = \langle b_1, ..., b_n\rangle$, $\psi = \langle c_1, ..., c_l\rangle$. Then, by 4.1.15,

$$a \in D(b_1 s_1, ..., b_k s_k, c_1 t_1, ..., c_l t_l), \text{ with } s_i = t_j = 1 \text{ on } Y.$$

Thus, by (γ) for (X, G), we have $b \in D(b_1 s_1, ..., b_k s_k)$, $c \in D(c_1 t_1, ..., c_l t_l)$ with $a \in D(b, c)$. Then $a|_Y \in D(b|_Y, c|_Y)$, $b|_Y \in D(\varphi|_Y)$, $c|_Y \in D(\psi|_Y)$. □

If $Y \subseteq X$ is a subspace, the inclusion $Y \hookrightarrow X$ is a morphism from the space of orderings $(Y, G|_Y)$ to the space of orderings (X, G). The associated group homomorphism from G to $G|_Y$ is just the restriction mapping $a \mapsto a|_Y$. The associated ring homomorphism from $W(X, G)$ to $W(Y, G|_Y)$ is given by $\langle a_1, ..., a_n\rangle \mapsto \langle a_1|_Y, ..., a_n|_Y\rangle$. This is surjective because the restriction map $G \mapsto G|_Y$ is surjective.

Theorem 4.1.27. *For any (non-empty) subspace* $Y \subseteq X$, *the kernel of the ring homomorphism* $W(X, G) \to W(Y, G|_Y)$ *is generated as an ideal by the elements* $\langle 1, -s\rangle$, $s \in G$, $s|_Y = 1$.

Proof. Of course, these elements are in the kernel. Conversely, suppose $\varphi = \langle a_1, ..., a_n\rangle$ in the kernel. Thus $\varphi|_Y \sim 0$ so, in particular, n is even. Since $\varphi \sim 0$ on Y, by continuity of $x \mapsto \varphi(x)$ and compactness, $\varphi \sim 0$ on $U(c_1, ..., c_k)$ for some $c_1, ..., c_k$ with $c_i|_Y = 1$. Thus $\varphi \otimes \psi \sim 0$ where $\psi := \langle 1, c_1\rangle \otimes ... \otimes \langle 1, c_k\rangle$ (since $\varphi \otimes \psi$ has signature 0 at each $x \in X$). Since $\varphi \otimes \psi \sim a_1\psi \oplus ... \oplus a_n\psi$, this

means $a_1\psi\oplus...\oplus a_n\psi$ is isotropic so, by 4.1.18(e), we get $s_1 \in D(\psi)$ with $-a_1s_1 \in D(a_2\psi\oplus...\oplus a_n\psi)$ so, by 4.1.10, $-a_1s_1 \in D(a_2s_2, ..., a_ns_n)$ for some $s_2, ..., s_n \in D(\psi)$. Thus $\langle a_1s_1, ..., a_ns_n\rangle$ is isotropic so $\langle a_1s_1, ..., a_ns_n\rangle \sim \tau$ for some τ of dimension $n-2$. Thus

$$\begin{aligned}\varphi = \langle a_1, ..., a_n\rangle &\sim \langle a_1s_1, ..., a_ns_n\rangle \oplus a_1\langle 1, -s_1\rangle \oplus ... \oplus a_n\rangle 1, -s_n\rangle \\ &\sim \tau \oplus a_1\langle 1, -s_1\rangle \oplus ... \oplus a_n\langle 1, -s_n\rangle.\end{aligned}$$

Since $s_i \in D(\psi)$, $s_i|_Y = 1$, $i = 1, ..., n$, τ is also in the kernel, so the result follows by induction on the dimension. □

4.1.5 Fans II

Suppose G is any group of exponent 2, with multiplication as the operation. Fix $e \in G$, $e \neq 1$ (to play the role of the constant function -1), and set $X = \{x \in \chi(G) : x(e) = -1\}$. Elements of G are viewed as functions on X by defining $a(x) = x(a)$ for all $a \in G$, $x \in X$. The pair (X, G) constructed in this way, is called a *fan*.

Theorem 4.1.28. *Any fan (X, G) is a space of orderings.*

Proof. We check AX1, AX2 and AX3.

Claim 1. If H is any subgroup of G maximal subject to the condition $e \notin H$ then $H = \ker(x)$ for some $x \in X$. For this, suppose $b \notin H$. Then $H \cup bH$ is a subgroup of G containing H properly, so $e \in H \cup bH$. Since $e \notin H$, this means $e \in bH$, i.e, $b \in eH$. Thus $H \cup eH = G$ so we have a character $x : G \to \{1, -1\}$ with $\ker(x) = H$. Then $e \notin \ker(x)$, so $x(e) = -1$, i.e, $x \in X$.

We are identifying G with a subgroup of $\{1, -1\}^X$ by identifying $a \in G$ with the function $a : X \to \{1, -1\}$ given by $a(x) = x(a)$. This is legitimate: if $a \neq b$, then $ab \neq 1$ so $e \notin \{1, eab\}$. Thus by Zorn's Lemma, we get a subgroup H of G with $\{1, eab\} \subseteq H$ maximal subject to the condition $e \notin H$. By Claim 1, $H = \ker(x)$ for some $x \in X$. Thus $x(eab) = 1$, i.e, $x(a) = -x(b)$ i.e, $a(x) = -b(x)$. This proves a, b are distinct as functions on X. AX1 is now proved. Note that $e(x) = x(e) = -1$ for all $x \in X$, so $e = -1$, proving AX2. To prove AX3 we need the following

Claim 2. If $a, b \in G$, $ab \neq -1$, then $D(a, b) = \{1, b\}$. For this, suppose $c \notin \{a, b\}$. Then $-1 \notin \{1, ab, -ac, -bc\}$ so, By Zorn's Lemma, we have a subgroup H of G with $\{1, ab, -ac.-bc\} \subseteq H$ maximal subject to the condition $-1 \notin H$. By Claim 1 we have $x \in X$ with $\ker(x) = H$. Thus $(ab)(x) = 1$, i.e, $a(x) = b(x)$, and $(-ac)(x) = 1$, i.e, $c(x) = a(x) \neq -a(x)$. Thus

$$a(x) + b(x) \neq c(x) + a(x)b(x)c(x),$$

so $\langle a, b\rangle \ncong \langle c, abc\rangle$, i.e, $c \notin D(a, b)$.

Now suppose $b \in D(a_1, c)$ for some $c \in D(a_2, b_3)$. We want to show that $b \in D(d, a_3)$ for some $d \in D(a_1, a_2)$. If $a_1a_2 \neq -1$, $a_1a_3 \neq -1$, $a_2a_3 \neq -1$, then, by Claim 2, $c = a_2$ or a_3 and $b = a_1, a_2$ or a_3. Thus we can take $d = a_1$ or a_2 in this case. If $a_1a_2 = -1$, then $D(a_1, a_2) = G$ so we can take $d = b$. If $a_ia_3 = -1$, $i = 1$ or 2, then $D(a_i, a_3) = G$, so we can take $d = a_i$. This proves AX3. □

Theorem 4.1.29. *For a space of orderings (X, G), the following are equivalent:*

a - (X, G) is a fan.

b - $D\langle 1, a\rangle = \{1, a\}$ *for all* $a \in G$, $a \neq -1$.

c - *For all* $a_1, ..., a_n \in G$, *if* $a_i a_j \neq -1$ *for* $i \neq j$, *then* $D\langle a_1, ..., a_n\rangle = \{a_1, ..., a_n\}$.

d - *If* x *is any element character of* G *satisfying* $x(-1) = -1$ *then* $x \in X$.

Proof. (a)⇒(b): Follows by the proof of 4.1.28.

(b)⇒(c): $D(a) = \{a\}$ is true in general. Also, $D(a, b) = aD(1, ab)$, so if (b) holds, then

$$D(a, b) = a\{1, ab\} = \{a, b\}$$

if $ab \neq -1$. Now suppose $b \in D(a_1, ..., a_n)$, $n \geq 3$ and $a_i a_j \neq -1$ for $i \neq j$. Thus $b \in D(a_1, c)$ for some $c \in D(a_2, ..., a_n)$. By induction $c = a_j$ for some $j \geq 2$. Thus $b \in D(a_1, a_j)$ so $b = a_1$ or a_j. Anyway, this means $b \in \{a_1, ..., a_n\}$.

(c)⇒(d): We have to show that $a, b \in \ker(x) \Rightarrow D(a, b) \subseteq \ker(x)$. But this is immediate once $ab \neq -1$ (since $-1 \notin \ker(x)$) so, by (c), $D(a, b) = \{a, b\} \subseteq \ker(x)$. Thus, applying AX2, we see that $x \in X$.

(d)⇒(a): this is immediate fom definition of fan, taking $e = -1$. □

When is a finite space of orderings a fan? Suppose (X, G) is a space of orderings with X finite (so G is also finite). Viewing elements of X as characters, we have $\bigcap_{x\in X} \ker(x) = \{1\}$, so we can find some smallest subset $\{x_1, ..., x_n\}$ of X with $\bigcap_{j=1}^{n} \ker(x_j) = \{1\}$. We refer to any such subset as a **minimal generating** set for X. Note that the condition $\bigcap_{j=1}^{n} \ker(x_j) = \{1\}$ just means that the subspace of (X, G) generated by $x_1, ..., x_n$ is all of X.

Theorem 4.1.30. *Suppose* (X, G) *is a space of orderings having a minimal generating set* $x_1, ..., x_n$. *Then:*

i - $|G| = 2^n$.

ii - $x_1, ..., x_n$ *is a* $\mathbb{Z}_2$ *basis for the character group* $\chi(G)$. *In particular, each* $x \in X$ *is expressible uniquely as*

$$x = \prod_{i=1}^{n} x_i^{e_i},\ e_i \in \{0, 1\}.$$

iii - *A necessary condition for a character* $x = \prod_{i=1}^{n} x_i^{e_i}$, $e_i \in \{0, 1\}$, *to be in* X *is that*

$$\sum_{i=1}^{n} e_1 \cong 1\ (mod\ 2).$$

In particular, $n \leq |X| \leq 2^{n-1}$.

iv - (X, G) *is a fan iff* $|X| = 2^{n-1}$, *so* X *consists of all products*

$$x = \prod_{i=1}^{n} x_i^{e_i},\ and\ \sum_{i=1}^{n} e_1 \cong 1\ (mod\ 2).$$

Proof. By the argument in the proof of 4.1.1(ii), the natural injection

$$G \hookrightarrow \prod_{j=1}^{n} G/\ker(x_j)$$

is surjective, etc, so (i) and (ii) follows. (iii) and (iv) follows since each $x \in X$ must satisfy $x(-1) = (-1)(x) = -1$. □

If (X, G) is any space of orderings then, by a **fan** in X (more precisely, a fan in (X, G)), we mean a subspace Y of X such that the space of orderings $(Y, G|_Y)$ is a fan. For example, in the space of orderings $(X_{\sum F^2}, G_{\sum F^2})$, F a formally real field, we have the fans $(X_{F^2U_\alpha^+}, G_{F^2U_\alpha^+})$ associated to the real places $\alpha : F \to \mathbb{R} \cup \{\infty\}$.

A fan is said to be **trivial** if it has one or two elements. For any $x, y \in X$, $\{x\}$ and $\{x, y\}$ are trivial fans. The 4 elements fans are specially important. These consist of 4 distinct orderings x_1, x_2, x_3, x_4 such that $\prod_{j=1}^n x_j = 1$ (i.e, $\prod_{j=1}^4 a(x_j) = 1$ for all $a \in G$).

Finally, every fan is realized as the full space of orderings $(X_{\sum F^2}, G_{\sum F^2})$ of some formally real field F. To see this, take $F = \mathbb{R}((\Gamma))$, where Γ is the direct sum of suitably many copies of $\mathbb{Z}$ ordered in some way (e.g, lexicographically). In this situation, F has a unique real place α and $U_\alpha^+ \subseteq F^2$, so $F^2U_\alpha^+ = F^2 = \sum F^2$.

4.1.6 The Representation Problem II

Let (X, G) be any space of orderings. The representation theorem describes the image of the Witt ring $W = W(X, G)$ in $C(X, Z)$. We state the representation theorem in 4.1.33 below, but we start with the following easier result:

Theorem 4.1.31. *Suppose $f : X \to \mathbb{Z}$ is a continuous function. Then $2^n f$ is represented by a form (i.e, there exists a form φ with entries in G such that $2^n f = \varphi(x)$ for all $x \in X$) for some integer $n \geq 0$. In particular, the cokernel of the embedding $W \hookrightarrow C(X, \mathbb{Z})$ is 2-primary torsion.*

Proof. f is continuous and $\mathbb{Z}$ discrete, so f is locally constant, i.e, for each $x \in X$, there exists a basic set $U(a_1, ..., a_n)$ with $x \in U(a_1, ..., a_n)$ and f constant on $U(a_1, ..., a_n)$. By compactness, there exist elements $a_{ij} \in G$, $i = 1, ..., k$, $j = 1, ..., v_i$ such that X is the union of the sets $U(a_{i1}, ..., a_{iv_i})$, $i = 1, ..., k$, and f is constant on each $U(a_{i1}, ..., a_{iv_i})$. Take $\overline{G} \subseteq G$ to be the subgroup of G generated by -1 and the elements a_{ij}. For $x \in X$, let

$$\overline{x} := \{y \in X : a(y) = a(x) \text{ for all } a \in \overline{G}\}$$

and let $\overline{X} = \{\overline{x} : x \in X\}$. Thus, if we view the elements of X as characters on G, then elements of $\overline{X}$ are just restrictions of elements of X to the subgroup $\overline{G}$. In particular, elements of $\overline{X}$ can be viewed as characters on the finite group $\overline{G}$, so $\overline{X}$ is finite. Also, if $\overline{x} = \overline{y}$, then $a_{ij}(x) = a_{ij}(y)$ for all i, j so x, y lie in the same $U(a_{i1}, ..., a_{iv_i})$, so $f(x) = f(y)$. Thus we get a well-defined function $\overline{f} : \overline{X} \to \mathbb{Z}$ such that $\overline{f}(\overline{x}) = f(x)$ for all $x \in X$. Now fix a $\mathbb{Z}_2$-basis $-1, a_1, ..., a_n$ for $\overline{G}$ and define

$$p_{\overline{x}} = \langle 1, a_1(x)a_1\rangle \otimes ... \otimes \langle 1, a_n(x)a_n\rangle,$$

$\overline{x} \in \overline{X}$ (this depends only on $\overline{x}$, not on x). Then

$$p_{\overline{x}} = \begin{cases} 2^n \text{ if } \overline{y} = \overline{x} \\ 0 \text{ if } \overline{y} \neq \overline{x} \end{cases}$$

Thus

$$\left(\sum_{\overline{x} \in \overline{X}} \overline{f}(\overline{x}) p_{\overline{x}}\right)(y) = 2^n f(\overline{y}) = 2^n f(y)$$

for each $y \in X$ so

$$2^n f = \sum_{\overline{x} \in \overline{X}} \overline{f}(\overline{x}) p_{\overline{x}}.$$

Since $p_{\overline{x}} \in W$ and $\overline{f}(\overline{x}) \in \mathbb{Z}$, this proves $2^n f \in W$. □

We can expand $p_{\overline{x}}$ as $p_{\overline{x}} = \sum_S a_S(x)\langle a_S\rangle$, S running through all subsets of $\{1, ..., n\}$, where $a_S := \prod_{i \in S} a_i$. Then, substituting, we obtain

$$2^n f = \sum_{\overline{x} \in \overline{X}} \overline{f}(\overline{x}) p_{\overline{x}} = \sum_{\overline{x} \in \overline{X}} \overline{f}(\overline{x}) \sum_S a_S(x)\langle a_S\rangle = \sum_S m_S \langle a_S\rangle,$$

where

$$m_S = \sum_{\overline{x} \in \overline{X}} \overline{f}(\overline{x}) \sum_S a_S(x).$$

In certain cases, we may able to improve on 4.1.31. For example, if each of the integers m_S is divisible by 2^n then we get $f = \sum_S \frac{m_S}{2^n}\langle a_S\rangle \in W$.

Before deal with the Representation Theorem, we need a lemma:

Lemma 4.1.32. *Suppose $a_1, a_2 \in G$ and φ_1, φ_2 are forms such that*

$$\varphi_1 \otimes \langle 1, a_1\rangle \cong \varphi_2 \otimes \langle 1, a_2\rangle. \tag{*}$$

Then there exists a form φ such that $\varphi|_{U_{a_i}} \cong \varphi_i|_{U_{a_i}}$, $i = 1, 2$.

Proof. Let

$$S := D(\varphi_1 \otimes \langle 1, a_1\rangle) = D(\varphi_2 \otimes \langle 1, a_2\rangle).$$

By 4.1.26(i),

$$S|_{D(\varphi_1 \otimes \langle 1, a_1\rangle)} = S|_{D(\varphi_2 \otimes \langle 1, a_2\rangle)},$$

$i = 1, 2$. Pick $p \in S$ and decompose $\varphi_i \cong \langle p\rangle \oplus \varphi_i'$ on $U(a_i)$, so

$$\varphi_i \otimes \langle 1, a_i\rangle \cong \langle p, pa_i\rangle \oplus \varphi_i' \oplus \langle 1, a_i\rangle$$

on X, $i = 1, 2$. Rewriting (*) using this, and cancelling the 1-dimensional form $\langle p\rangle$, we obtain

$$\langle pa_1\rangle \oplus \varphi_i' \otimes \langle 1, a_1\rangle \cong \langle p, a_2\rangle \otimes \varphi_2' \oplus \langle 1, a_2\rangle.$$

Multiplying this by a_2 and adding $\langle -pa_1, a_2\rangle$ to each side yields

$$\langle pa_1a_2\rangle \oplus a_2\varphi_1' \otimes \langle 1, a_1\rangle \cong \langle p\rangle \oplus \varphi_2' \otimes \langle 1, a_2\rangle$$

and

$$\langle 1, -1\rangle \oplus a_2\varphi_1' \otimes \langle 1, a_1\rangle \cong p\langle 1, -a_1a_2\rangle \oplus \varphi_2' \otimes \langle 1, a_2\rangle. \tag{4.1}$$

It follows that the right side of 4.1 is isotropic so, by 4.1.18(v), there exists $s \in D(1, -a_1a_2)$ such that $-ps \in D(\varphi_2' \otimes \langle 1, a_2\rangle)$. Thus $-ps|_{U(a_2)} \in D(\varphi_2'|_{U(a_2)})$ so $\varphi_2' \cong \langle -ps\rangle \oplus \varphi_2''$ on $U(a_2)$ and then

$$\varphi_2' \otimes \langle 1, a_2\rangle \cong \langle -ps, -psa_2\rangle \oplus \varphi_2'' \otimes \langle 1, a_2\rangle$$

on X. Also, $\langle 1, -a_1a_2\rangle \cong \langle s, -sa_1a_2\rangle$. Rewriting 4.1 using these last two relations, we obtain

$$\langle 1,-1\rangle \oplus a_2\varphi_1' \otimes \langle 1, a_1\rangle \cong \langle ps, -psa_1a_2, -ps, -psa_2\rangle \oplus \varphi_2'' \otimes \langle 1, a_2\rangle.$$

Cancelling the hyperbolic planes $\langle 1,-1\rangle \cong \langle ps, -ps\rangle$, and multiplying by a_2, this yields

$$\varphi_1' \otimes \langle 1, a_1\rangle \cong \langle -psa_1, -ps\rangle \oplus \varphi_2'' \otimes \langle 1, a_2\rangle. \tag{4.2}$$

It follows that $-ps \in D(\varphi_1' \otimes \langle 1, a_1\rangle)$ so $\varphi_1' \cong \langle -ps\rangle \oplus \varphi_1''$ on $U(a_1)$, i.e,

$$\varphi_1' \otimes \langle 1, a_1\rangle \cong \langle -ps, -psa_1\rangle \oplus \varphi_1''\langle 1, a_1\rangle$$

on X. Rewritting 4.2 using this, and cancelling, we obtain $\varphi_1'' \otimes \langle 1, a_1\rangle \cong \varphi_2'' \otimes \langle 1, a_2\rangle$ on X. Since

$$\varphi_i \cong \langle p\rangle \otimes \varphi_i' \cong \langle p, -ps\rangle \otimes \varphi_i''$$

on $U(a_i)$, $i = 1, 2$, we are done by induction on the dimension. □

Theorem 4.1.33 (Representation Theorem)**.** *Suppose $f : X \to \mathbb{Z}$ is a continuous function. Then the following are equivalent:*

a - *$2^n f$ is represented by a form (i.e, there exists a form φ with entries in G such that $2^n f = \varphi(x)$ for all $x \in X$).*

b - *$\sum_{x\in Y} f(x) \equiv 0 \,mod\, |Y|$ holds for all finite fans $Y \subseteq X$.*

c - *$\sum_{x\in Y} a(x)f(x) \equiv 0 \,mod\, |Y|$ holds for all finite fans $Y \subseteq X$ and for all $a \in G$.*

Proof. (a)⇒(b) Suppose f is represented by $\langle a_1, ..., a_n\rangle$ and $Y \subseteq X$ is a finite fan. Then $f(y) = \sum_{j=1}^n a_i(y)$ so

$$\sum_{y\in Y} f(y) = \sum_{j=1}^{n} (\sum_{y\in Y} a_i(y)).$$

Thus we are reduced to showing

$$\sum_{y\in Y} a(y) \equiv 0 \bmod |Y| \text{ for any } a \in G.$$

There are two cases. If $a = \pm 1$ on Y then $\sum_{y\in Y} a(y) \pm |Y|$. If $a \neq \pm 1$ on Y, then $Y = U(a|_Y) \cup U(-a|_Y)$ and, since Y is a fan, $U(a|_Y)$ and $U(-a|_Y)$ each have half as many elements as Y so

$$\sum_{y\in Y} a(y) = |U(a|_Y)| - |U(-a|_Y)| = 0.$$

(b)⇒(c) We want to show that $\sum_{x\in Y} a(x)f(x) \equiv 0 \bmod |Y|$ for any finite fan $Y \subseteq X$. This is immediate from (b) if $a = \pm 1$ on Y. Otherwise

$$\begin{aligned}\sum_{x\in Y} a(x)f(x) &= \sum_{x\in U(a|_Y)} f(x) - \sum_{x\in U(-a|_Y)} f(x) \\ &= 2\left(\sum_{x\in U(a|_Y)} f(x)\right) - \left(\sum_{x\in Y} f(x)\right) \equiv 0 \bmod |Y|.\end{aligned}$$

Here, we are using the fact that $Y = U(a|_Y) \cup U(-a|_Y)$ and that $U(a|_Y)$ is a fan with $1/2|Y|$ elements, so

$$\sum_{x \in U(a|_Y)} f(x) \equiv 0 \bmod 1/2|Y|.$$

(c)⇒(a) Assume the result is false. Thus f is not represented by a form. We look at all subspaces Y in X such that $f|_Y$ is not represented by a form. We use Zorn's Lemma to get a minimal such Y. One has to observe that if Y_i, $i \in I$ is some chain of subspaces, then $Y = \bigcap_{i \in I} Y_i$ is a subspace and, if $f|_Y$ is represented by a form, say $\langle a_1|_Y, ..., a_n|_Y \rangle$, then, by continuity, the set

$$U = \{x \in X : f(x) = \sum_{j=1}^{n} a_j(x)\}$$

is open in X and contains Y so, by compacteness it contains Y_i (so $f|_{Y_i}$ is represented by $\langle a_1|_Y, ..., a_n|_Y \rangle$) for some $i \in I$. Thus Zorn's Lemma does apply. So now we have the subspace Y with $f|_Y$ not represented, and Y is minimal with this property. Of course, every fan in Y is also a fan in X, so our assumption that

$$\sum_{x \in Z} a(x) f(x) \equiv 0 \bmod |Z|$$

for all $a \in G$ still holds for all finite fans $Z \subseteq Y$. To simplify notation, we replace X by Y. So now f is not represented, but $f|_Y$ is represented for each proper subspace Y of X.

Claim. (X, G) is not a fan. For suppose (X, G) is a fan. Go to the notation used in the proof of 4.1.31. Pick any subgroup $H \subseteq G$ so that $G = \overline{G} \times H$ (direct product). Let Y consist of all characters $x : G \to \{-1, 1\}$ such that $x|_H = 1$, and $x(-1) = -1$. Since X is a fan and $Y \subseteq X$, so Y is a fan. Since $-1, a_1, ..., a_n$ is a basis for $\overline{G}$, we see that $|Y| = 2^n$. Finally, we see that for each $\overline{x} \in \overline{X}$, there exists a unique $y \in Y$ such that $\overline{x} = \overline{y}$. Thus

$$m_S = \sum_{\overline{x} \in \overline{X}} \overline{f}(\overline{x}) a_S(x) = \sum_{y \in Y} f(y) a_S(y) \equiv 0 \bmod 2^n$$

for each subset S of $\{1, ..., n\}$ so, $f \in W$ (each m_S is divisible by 2^n). This proves the claim.

Thus (X, G) is not a fan, so, by 4.1.29, there exists $a \in G$, $a \neq -1$, $D(1, a) \neq \{1, a\}$. Thus there exists $b \in D(1, a)$, $b \neq 1, a$. Thus $\langle 1, a \rangle \cong \langle b, ab \rangle$, i.e, $\langle -a, b, ab \rangle \sim \langle 1 \rangle$. Take $a_1 = -a$, $a_2 = b$, $a_3 = ab$. Note $a_i \neq 1$, $i = 1, 2, 3$, so $U(a_i)$ is a proper subset of X. By the minimal choice of X, $f|_{U(a_i)}$ is represented, $i = 1, 2, 3$. Also $\langle a_1, a_2, a_3 \rangle \sim \langle 1 \rangle$ so, comparing signatures

$$\text{For each } x \in X \text{ exactly one of } a_1(x), a_2(x), a_3(x) \text{ is } -1. \qquad (*)$$

In particular, $U(a_i) \cap U(a_j) = X$ if $i \neq j$. Thus we can assume $U(a_i) \neq \emptyset$ (otherwise $U(a_j) = X$). Now, let φ_i be a form with entries in G such that $\varphi_i|_{U(a_i)}$ represents $f|_{U(a_i)}$, $i = 1, 2, 3$. We can assume $\varphi_3 \sim 0$[3]. We can also assume $\varphi_i|_{U(a_i)}$ is anisotropic, $i = 1, 2$. Recall that by 4.1.26(i), $D(\varphi_i|_{U(a_i)}) = D(\varphi_i \otimes \langle 1, a_i \rangle)|_{U(a_i)}$. This means $\varphi_i \otimes \langle 1, a_i \rangle$ is anisotropic, $i = 1, 2$ (see 4.1.18(iii)). Consider these two forms carefully. Let $x \in X$. By (*), there are three possibilities. If $a_1(x) = a_2(x) = 1$, then $\varphi_i(x) = f(x)$, $i = 1, 2$, so

$$(\varphi_1 \otimes \langle 1, a_1 \rangle)(x) = 2f(x) = (\varphi_2 \otimes \langle 1, a_2 \rangle)(x).$$

[3]Replace f by $g : f - \varphi_3$ if necessary. There is no harm in doing this. f is represented iff g is represented.

If $a_1(x) = 1$, $a_2(x) = -1$, then $a_3(x) = 1$, so $\varphi_1(x) = f(x) = \varphi_3(x) = 0$ and $\langle 1, a_2\rangle(x) = 0$, so

$$(\varphi_1 \otimes \langle 1, a_1\rangle)(x) = 0(\varphi_2 \otimes \langle 1, a_2\rangle)(x).$$

Similarly, if $a_1(x) = -1$ and $a_2(x) = 1$. Thus $\varphi_1 \otimes \langle 1, a_1\rangle$ and $\varphi_2 \otimes \langle 1, a_2\rangle$ have the same signature at each $x \in X$ and both are anisotropic, so $\varphi_1 \otimes \langle 1, a_1\rangle \cong \varphi_2 \otimes \langle 1, a_2\rangle$ (see 4.1.18(i) and 4.1.13). By lemma 4.1.32 there exists a form φ such that $\varphi|_{U_{a_i}} \cong \varphi_i|_{U_{a_i}}$, $i = 1, 2$. In particular, this φ represents f, contradiction. So the theorem is proved. □

It is important observe that the notion of fans and the representation problem context for AOS, provides a generalization for the context of the reduced theory of quadratic forms, covered in chapter 2.

4.2 Special Groups

For special groups, we follow chapters 1,2 and 3 of [DM00]. This is a rich theory, and sadly the most important applications, like the proof of Marshall's Conjecture, the Boolean hull and the invariants are left to a posterior work.

4.2.1 Basic Definitions

Let A be a set and $\equiv$ a binary relation on $A \times A$. We extend $\equiv$ to a binary relation $\equiv_n$ on A^n, by induction on $n \geq 2$, as follows:

i - $\equiv_2 = \equiv$.

ii - $\langle a_1, ..., a_n\rangle \equiv_n \langle b_1, ..., b_n\rangle$ if and only there are $x, y, z_3, ..., z_n \in A$ such that $\langle a_1, x\rangle \equiv \langle b_1, y\rangle$, $\langle a_2, ..., a_n\rangle \equiv_{n-1} \langle x, z_3, ..., z_n\rangle$ and $\langle b_2, ..., b_n\rangle \equiv_{n-1} \langle y, z_3, ..., z_n\rangle$.

Whenever clear from the context, we frequently abuse notation and indicate the aforedescribed extension $\equiv$ by the same symbol.

Definition 4.2.1 (Special Group)**.** *A special group (SG) is an tuple $(G, -1, \equiv)$, where G is a group of exponent 2, i.e, $g^2 = 1$ for all $g \in G$; -1 is a distinguished element of G, and $\equiv \subseteq G \times G \times G \times G$ is a relation (the special relation), satisfying the following axioms for all $a, b, c, d, x \in G$:*

SG 0 - *$\equiv$ is an equivalence relation on G^2;*

SG 1 - *$\langle a, b\rangle \equiv \langle b, a\rangle$;*

SG 2 - *$\langle a, -a\rangle \equiv \langle 1, -1\rangle$;*

SG 3 - *$\langle a, b\rangle \equiv \langle c, d\rangle \Rightarrow ab = cd$;*

SG 4 - *$\langle a, b\rangle \equiv \langle c, d\rangle \Rightarrow \langle a, -c\rangle \equiv \langle -b, d\rangle$;*

SG 5 - *$\langle a, b\rangle \equiv \langle c, d\rangle \Rightarrow \langle ga, gb\rangle \equiv \langle gc, gd\rangle$, for all $g \in G$.*

SG 6 (3-transitivity) - *the extension of $\equiv$ for a binary relation on G^3 is a transitive relation.*

A group of exponent 2 satisfying SG0-SG5 is called *pre-special group* (PSG). A PSG (or SG) $(G, -1, \equiv)$ is *reduced* (RPSG, RSG respectively) if $1 \neq -1$ and if $\langle a, a\rangle \equiv \langle 1, 1\rangle \Rightarrow a = 1$.

Definition 4.2.2. *Let G be a psg. A form φ on G is an n-tuple $\langle a_1, ..., a_n\rangle$ of elements of G; n is called the dimension of φ,* $\dim(\varphi)$. *We also call φ a n-form.*

By convention, two forms of dimension 1 are isometric if and only if they have the same coefficients. If $\varphi = \langle a_1, ..., a_n\rangle$ is a form on G, define

a - The *set of elements represented by* φ as

$$D_G(\varphi) = \{b \in G : \exists\, z_2, ..., z_n \in G \text{ such that } \varphi \equiv_G \langle b, z_2, ..., z_n\rangle\}.$$

b - The *discriminant* of φ as $d(\varphi) = \prod_{i=1}^{n} a_i$.

c - *Direct sum* as $\varphi \oplus \theta = \langle a_1, ..., a_n, b_1, ..., b_m\rangle$.

d - *Tensor product* as $\varphi \otimes \theta = \langle a_1b_1, ..., a_ib_j, ..., a_nb_m\rangle$. If $a \in G$, $\langle a\rangle \otimes \varphi$ is written $a\varphi$.

A form φ on G is *isotropic* if there is a form ψ over G such that $\varphi \equiv_G \langle 1, -1\rangle \oplus \psi$; otherwise it is said to be *anisotropic*. We say that φ is *universal* if $D_G(\varphi) = G$.

Lemma 4.2.3. *Let $(G, \equiv_G, -1)$ be a pre-special group. Let a, b, c, d be elements of G and φ, ψ be n-forms on G. Then*

a - $\langle a, b\rangle \equiv \langle c, d\rangle$ if and only if $ab = cd$ and $ac \in D_G(1, cd)$. Further, $c \in D_G(1, a)$ if and only if $\langle c, ac\rangle \equiv \langle 1, a\rangle$.

b - $\varphi \equiv \psi$ implies $d(\varphi) = d(\psi)$.

Proof. a - If $\langle a, b\rangle \equiv \langle c, d\rangle$, then by SG3 $ab = cd$ and by SG5 $\langle ac, bc\rangle \equiv \langle 1, cd\rangle$, so $ac \in D_G(c, d)$. Conversely, suppose that $ab = cd$ and $ac \in D_G(c, d)$. Then there exist $x \in G$ such that $\langle ac, x\rangle \equiv \langle 1, cd\rangle$, and by SG3, $acx = cd \Rightarrow ax = d$.

$$\begin{aligned}\langle ac, x\rangle \equiv \langle 1, cd\rangle &\overset{ab=cd}{\Rightarrow} \langle ac, x\rangle \equiv \langle 1, ab\rangle \\ &\overset{SG5}{\Rightarrow} \langle c, ax\rangle \equiv \langle a, b\rangle \\ &\Rightarrow \langle c, d\rangle \equiv \langle a, b\rangle.\end{aligned}$$

b - We proceed by induction on $\dim\varphi = \dim\psi = n$. If $n = 1$ there is nothing to do, and if $n = 2$ is just SG3 (or the previous item). Now, Let $n \geq 3$ and $\varphi = \langle a_1, ..., a_n\rangle$ and $\psi = \langle b_1, ..., b_n\rangle$. If $\varphi \equiv \psi$, there exist $x, y, z_3, ..., z_n \in G$ such that $\langle a_1, x\rangle \equiv \langle b_1, y\rangle$, $\langle a_2, ..., a_n\rangle \equiv \langle x, z_3, ..., z_n\rangle$ and $\langle b_2, ..., b_n\rangle \equiv \langle y, z_3, ..., z_n\rangle$. Therefore $a_1x = b_1y$ and by induction hypothesis, $a_2...a_n = xz_3...z_n$ and $b_2...b_n = yz_3...z_n$. Hence

$$a_2...a_n = xz_3...z_n \Rightarrow a_1a_2...a_n = a_1xz_3...z_n = b_1yz_3...z_n = b_1b_2...b_n$$

and $d(\varphi) = d(\psi)$.

□

Proposition 4.2.4. *Let $(G, \equiv_G, -1)$ be a pre-special group and φ, ψ and θ be forms on G. Then*

a - The direct sum of isometric forms is isometric.

b - The tensor product of isometric forms is isometric.

c - If G is a special group, then we also have the Witt cancellation:

$$\varphi \oplus \theta \equiv \psi \oplus \theta \Rightarrow \varphi \equiv \psi.$$

d - For all $a \in G$ and forms $\varphi_1, ..., \varphi_n$ on G,

$$a \in D_G(\oplus_{i=1}^n \varphi_i) \Leftrightarrow \begin{cases} \exists\, x_i \in D_G(\varphi_i),\ 1 \leq i \leq n, \\ \text{such that } a \in D_G(\langle x_1, ..., x_n \rangle) \end{cases}.$$

e - $\varphi \oplus \psi$ is isotropic iff there is $x \in G$ such that $x \in D_G(\varphi)$ and $-x \in D_G(\psi)$. In particular, if a is an element of G, $a \in D_G(\varphi)$ iff $\langle -a \rangle \oplus \varphi$ is isotropic.

Proof. a - Suppose that $\varphi_1, \varphi_2, \psi_1, \psi_2$ are forms over G such that $\varphi_1 \equiv \varphi_2$ and $\psi_1 \equiv \psi_2$. We prove that $\varphi_1 \oplus \psi_1 \equiv \varphi_2 \oplus \psi_2$ by induction on $n = \dim \varphi_1 = \dim \varphi_2$. If $n = 1$, then $\varphi_1 = \varphi_2 = \langle a \rangle$ for some $a \in G$. Let $\psi_1 = \langle c_1, ..., c_m \rangle$ and $\psi_2 = \langle d_1, ..., d_m \rangle$. The isometries $\langle a, c_1 \rangle \equiv \langle a, c_1 \rangle$, $\psi_1 \equiv \psi_1$ and $\psi_1 \equiv \psi_2$ show that $\langle a, c_1, ..., c_m \rangle \equiv \langle a, d_1, ..., d_m \rangle$, as required.

Assume that result true for $\dim \varphi_1 = \dim \varphi_2 = n$ and suppose $\varphi_1 = \langle a, a_1, ..., a_n \rangle$ and $\varphi_2 = \langle b, b_1, ..., b_n \rangle$. Let $x, y, \vec{z} = (z_2, ..., z_n)$ be witnesses to the isometry $\varphi_1 \equiv \varphi_2$, that is

$$\langle a, x \rangle \equiv \langle b, y \rangle,\ \langle a_1, ..., a_n \rangle \equiv \langle x, \vec{z} \rangle \text{ and } \langle b_1, ..., b_n \rangle \equiv \langle y, \vec{z} \rangle. \tag{*}$$

The isometries in (*) and the induction hypothesis give

$$\langle a_1, ..., a_n \rangle \oplus \psi_1 \equiv \langle x, \vec{z} \rangle \oplus \psi_1 \text{ and } \langle a_1, ..., a_n \rangle \oplus \psi_1 \equiv \langle x, \vec{z} \rangle \oplus \psi_2.$$

Hence, these isometries together with the first one in (*) yields

$$\langle a, a_1, ..., a_n \rangle \oplus \psi_1 \equiv \langle b, b_1, ..., b_n \rangle \oplus \psi_2$$

as desired.

b - Suppose that $\varphi_1, \varphi_2, \psi_1, \psi_2$ are forms over G such that $\varphi_1 \equiv \varphi_2$ and $\psi_1 \equiv \psi_2$. We prove that $\varphi_1 \otimes \psi_1 \equiv \varphi_2 \otimes \psi_2$ by induction on $n = \dim \varphi_1 = \dim \varphi_2$.

Let $n = 1$. Then $\varphi_1 = \varphi_2 = \langle a \rangle$ for some $a \in G$. Now, we proceed by induction on $m = \dim \psi_1 = \dim \psi_2$. Let $\psi_1 = \langle c_1, ..., c_m \rangle$ and $\psi_2 = \langle d_1, ..., d_m \rangle$. If $m = 1$ there is nothing to proof and if $m = 2$ the result holds by SG5. Assume that the result holds true for $(m-1)$ and let $x, y, \vec{z} = (z_2, ..., z_n)$ be witnesses to the isometry $\psi_1 \equiv \psi_2$, i.e,

$$\langle c_1, x \rangle \equiv \langle d_1, y \rangle,\ \langle c_2, ..., c_m \rangle \equiv \langle x, \vec{z} \rangle \text{ and } \langle d_2, ..., d_m \rangle \equiv \langle y, \vec{z} \rangle. \tag{**}$$

Multiplying all these isometries by a and using the induction hypothesis, we have

$$\langle ac_1, ax \rangle \equiv \langle ad_1, ay \rangle,\ \langle ac_2, ..., ac_m \rangle \equiv \langle ax, a\vec{z} \rangle \text{ and } \langle ad_2, ..., ad_m \rangle \equiv \langle ay, a\vec{z} \rangle,$$

and hence, $a\psi_1 \equiv a\psi_2$.

The general induction step follow by the argument in the case $n = 2$. So, let us prove

$$\langle a, b \rangle \equiv \langle c, d \rangle \Rightarrow \langle a, b \rangle \otimes \psi_1 \equiv \langle c, d \rangle \otimes \psi_2 \tag{4.3}$$

The argument is (again!) by induction on the dimension m of $\psi's$. If $m = 2$, say $\psi_1 = \langle c_1, c_2 \rangle \equiv \langle d_1, d_2 \rangle = \psi_2$, by preservation of isometry by sums and multiplication by an element of G we

have

$$\begin{aligned}\langle a,b\rangle \otimes \langle c_1,c_2\rangle &= a\langle c_1,c_2\rangle \oplus b\langle c_1,c_2\rangle \equiv a\langle d_1,d_2\rangle \oplus b\langle d_1,d_2\rangle = \langle a,b\rangle \otimes \langle d_1,d_2\rangle \\ &= d_1\langle a,b\rangle \oplus d_2\langle a,b\rangle \equiv d_1\langle c,d\rangle \oplus d_2\langle c,d\rangle = \langle c,d\rangle \otimes \langle d_1,d_2\rangle.\end{aligned}$$

Now, suppose that 4.3 holds for $\dim(\psi_1) = \dim(\psi_2) = m-1$. From (**) come

$$\langle a,b\rangle \otimes \langle c_1,x\rangle \equiv \langle c,d\rangle \otimes \langle d_1,y\rangle; \tag{4.4}$$
$$\langle a,b\rangle \otimes \langle c_2,...,c_m\rangle \equiv \langle a,b\rangle \otimes \langle x,z\rangle; \tag{4.5}$$
$$\langle c,d\rangle \otimes \langle d_2,...,d_m\rangle \equiv \langle c,d\rangle \otimes \langle y,z\rangle; \tag{4.6}$$
$$\langle a,b\rangle \otimes \langle \vec{z}\rangle \equiv \langle c,d\rangle \otimes \langle \vec{z}\rangle. \tag{4.7}$$

These isometries and the preservation of isometry by sums yields

$$\begin{aligned}\langle a,b\rangle \otimes \psi_1 &= c_1\langle a,b\rangle \oplus [\langle a,b\rangle \otimes \langle c_2,...,c_m\rangle] \\ &= c_1\langle a,b\rangle \oplus [\langle a,b\rangle \otimes \langle x,\vec{z}\rangle] \\ &= c_1\langle a,b\rangle \oplus x\langle a,b\rangle \oplus [\langle a,b\rangle \otimes \langle \vec{z}\rangle] \\ &= d_1\langle c,d\rangle \oplus y\langle c,d\rangle \oplus [\langle c,d\rangle \otimes \langle \vec{z}\rangle] \\ &= d_1\langle c,d\rangle \oplus [\langle c,d\rangle \otimes \langle y,\vec{z}\rangle] \\ &= d_1\langle c,d\rangle \oplus [\langle c,d\rangle \otimes \langle d_2,...,d_m\rangle] = \langle c,d\rangle \otimes \psi_2.\end{aligned}$$

Finally, we deal with the general case. By induction, let $\varphi_1 = \langle a,a_1,...,a_n\rangle$ and $\varphi_2 = \langle b,b_1,...,b_n\rangle$, $n \geq 3$. Let $x,y,\vec{z} = (z_2,...,z_n)$ be witnesses to the isometry $\varphi_1 \equiv \varphi_2$, i.e, elements satisfying (*). From the isometries in (**) we get, by induction hypothesis and the case $n = 2$

$$\langle a,x\rangle \otimes \psi_1 = a\psi_1 \oplus x\psi_1 \equiv \langle b,y\rangle \otimes \psi_2 = b\psi_2 \oplus y\psi_2; \tag{4.8}$$
$$\langle a_1,...,a_n\rangle \otimes \psi_1 \equiv \langle x,z\rangle \otimes \psi_1; \tag{4.9}$$
$$\langle b_1,...,b_n\rangle \otimes \psi_2 \equiv \langle y,z\rangle \otimes \psi_2; \tag{4.10}$$
$$\langle \vec{z}\rangle \otimes \psi_1 \equiv \langle \vec{z}\rangle \otimes \psi_2. \tag{4.11}$$

Then, we get

$$\begin{aligned}\varphi_1 \otimes \psi_1 &= \langle a,a_1,...,a_n\rangle \otimes \psi_1 \\ &= a\psi_1 \oplus [\langle a_1,...,a_n\rangle \otimes \psi_1] \\ &= a\psi_1 \oplus [\langle x,z\rangle \otimes \psi_1] \\ &= a\psi_1 \oplus x\psi_1 \oplus [\langle \vec{z}\rangle \otimes \psi_1] \\ &\equiv b\psi_2 \oplus y\psi_2 \oplus [\langle \vec{z}\rangle \otimes \psi_2] \\ &= b\psi_2 \oplus [\langle y,z\rangle \otimes \psi_2] \\ &\equiv b\psi_2 \oplus [\langle b_1,...,b_n\rangle \otimes \psi_2] \\ &= \langle b,b_1,...,b_n\rangle \otimes \psi_2 = \varphi_2 \otimes \psi_2.\end{aligned}$$

c - Let $n = \dim(\varphi) = \dim(\psi)$. First suppose that $\theta = \langle a\rangle$, $a \in G$. Then the hypothesis in this case reads $\langle a\rangle \oplus \varphi \equiv \langle a\rangle \oplus \psi$. Thus, there are $x,y,\vec{z} = (z_3,...,z_n) \in G$ such that $\langle a,x\rangle \equiv \langle a,y\rangle$, $\varphi \equiv \langle x,\vec{z}\rangle$ and $\psi \equiv \langle y,\vec{z}\rangle$. The first isometry tells us that $ax = ay$ and so $x = y$. But then the

transitivity of $\equiv$ yields $\varphi \equiv \psi$. To finish the proof, use induction on $\dim(\theta)$, noting that the isometry $\theta \oplus \varphi \equiv \theta \oplus \psi$ can be written as $\langle a\rangle \oplus \varphi' \equiv \langle a\rangle \oplus \psi'$, for suitable φ', ψ'.

d - It is enough to prove the statement for $n = 2$ and use induction. Therefore, we will prove that

$$a \in D_G(\varphi \oplus \psi) \Leftrightarrow \text{ there exist } x_1 \in D_G(\varphi) \text{ and } x_2 \in D_G(\psi) \text{ such that } a \in D_G(x_1, x_2). \quad (4.12)$$

($\Leftarrow$) Let $\dim(\varphi) = n$, $\dim(\psi) = m$, $b \in D_G(\varphi)$, $c \in D_G(\psi)$ and $a \in D_G(b, c)$. Then, there are $w, \vec{t} = (t_2, ..., t_n)$ and $\vec{a} = (a_2, ..., a_m)$ in G such that

$$\langle b, c\rangle \equiv \langle a, w\rangle,\ \langle b, \vec{t}\rangle \equiv \varphi \text{ and } \langle c, \vec{a}\rangle \equiv \psi.$$

But then,

$$\varphi \oplus \psi \equiv \langle b, \vec{t}\rangle \oplus \langle c, \vec{a}\rangle \equiv \langle b, c\rangle \oplus \langle \vec{t}, \vec{a}\rangle \equiv \langle a, z\rangle \oplus \langle \vec{t}, \vec{a}\rangle \equiv,$$

showing that $a \in D_G(\varphi \oplus \psi)$, hence $D_G(a, b) \subseteq D_G(\varphi \oplus \psi)$.

($\Rightarrow$) We use induction on $\dim(\varphi) = n$. If $\varphi = \langle b\rangle$ and $a \in \langle b\rangle \oplus \psi$, there is $\vec{t} = (t_1, ..., t_n)$ in G such that $\langle a, \vec{t}\rangle \equiv \langle b\rangle \oplus \psi$. This means that we can find x, y and $\vec{z} = (z_1, ..., z_m)$ in G such that (among other things), $\langle a, x\rangle \equiv \langle b, y\rangle$ and $\psi \equiv \langle y, \vec{z}\rangle$. Since $y \in D_G(\psi)$, this is exactly what was to be proved.

Now suppose $\varphi = \langle b, \vec{v}\rangle$, where $\vec{v} \in G^n$. If $a \in D_G(\varphi \oplus \psi)$, then there is $\vec{t} = (t_2, ..., t_l)$ in G, with $l = n + m + 1$, such that $\langle a, \vec{t}\rangle \equiv \langle b, \vec{v}\rangle \oplus \psi$. Just as before, there are x, y and $\vec{z} = (z_3, ..., z_l)$ in G such that $\langle a, x\rangle \equiv \langle b, y\rangle$ and $\langle y, \vec{z}\rangle \equiv \langle \vec{v}\rangle \oplus \psi$. By induction, since y is represented by $\langle \vec{v}\rangle \oplus \psi$, there are $u \in D_G(\langle \vec{v}\rangle)$ and $w \in D_G(\psi)$ such that $y \in D_G(u, w)$. Now note that we have $a \in D_G(b, y)$ and $y \in D_G(u, w)$.

By what was proven above, we may conclude that $a \in D_G(\langle b, u, w\rangle) = D_G(\langle b, u\rangle \oplus \langle w\rangle)$. Using the first step in the induction, we get the existence of $t \in D_G(b, u)$ such that $a \in D_G(t, w)$. But again, by the first part of the proof, $D_G(b, u) \subseteq D_G(\langle b\rangle \oplus \vec{v}) = D_G(\varphi)$, and the proof is complete.

e - If there is $x \in D_G(\varphi)$ such that $-x \in D_G(\psi)$, then there are $\vec{t} = \langle t_1, ..., t_n\rangle$ and $\vec{z} = \langle z_1, ..., z_m\rangle$ such that $\langle x, \vec{t}\rangle \equiv \varphi$ and $\langle -x, \vec{z}\rangle \equiv \psi$. But then

$$\varphi \oplus \psi \equiv \langle x, -x\rangle \oplus (\langle \vec{t}\rangle \oplus \langle \vec{z}\rangle) \equiv \langle 1, -1\rangle \oplus (\langle \vec{t}\rangle \oplus \langle \vec{z}\rangle),$$

i.e, $\varphi \oplus \psi$ is isotropic. For the converse, we proceed by induction on $\dim(\varphi) = n$. If $\varphi = \langle a\rangle$, then we have

$$\langle a\rangle \oplus \psi \equiv \langle 1, -1\rangle \oplus \theta \equiv \langle a, -a\rangle \oplus \theta,$$

and so cancelling a on both sides yields $\psi \equiv \langle -a\rangle \oplus \theta$, which shows that $-a \in D_G(\psi)$. By induction, write $\varphi = \langle a\rangle \oplus \gamma$, thus

$$\varphi \oplus \psi = \langle a\rangle \oplus \gamma \oplus \psi \equiv \langle 1, -1\rangle \oplus \theta \equiv \langle a, -a\rangle \oplus \theta,$$

which yields, by cancellation of a on both sides, $\gamma \oplus \psi \equiv \langle -a\rangle \oplus \theta$. By (d) above, there are $x \in D_G(\gamma)$ and $y \in D_G(\psi)$ such that $-a \in D_G(x, y)$, i.e, for some $z \in G$, $\langle -a, z\rangle \equiv \langle x, y\rangle$. Using SG1 and SG4, $\langle z, -y\rangle \equiv \langle a, x\rangle$. By (d), $-y \in D_G(\langle a\rangle \oplus \gamma) = D_G(\varphi)$, completing the proof.

□

Proposition 4.2.5. *Let $(G, \equiv_G, -1)$ be a pre-special group and φ, ψ and θ be forms on G. Then are equivalent:*

a - G is a reduced special group.

b - For all $x, a \in G$, if $x \in D_G(a, a)$ then $x = a$.

c - For any form ψ on G, $D_G(\psi \oplus \psi) = D_G(\psi)$.

d - For any form ψ on G, $\psi \oplus \psi$ isotropic $\Rightarrow$ ψ isotropic.

e - For all forms ψ, θ on G, $\psi \oplus \psi \equiv \theta \oplus \theta \Rightarrow \psi \equiv \theta$.

f - For any form ψ of even dimension on G, $\psi \oplus \psi$ hyperbolic $\Rightarrow$ ψ hyperbolic.

Proof. (a)$\Rightarrow$(b). If $x \in D_G(a, a)$, there exist $y \in G$ such that $\langle x, y\rangle \equiv \langle a, a\rangle$. By SG3, $xy = a^2 = 1$, so $xy = 1$, and $x = y$ (because G has exponent 2). Now, by SG5 and reduction we have

$$\langle x, x\rangle \equiv \langle a, a\rangle \Rightarrow \langle ax, ax\rangle \equiv \langle 1, 1\rangle \Rightarrow ax = 1 \Rightarrow x = a.$$

(b)$\Rightarrow$(c). Let $\psi = \langle a_1, ..., a_n\rangle$ and $x \in D_G(\psi \oplus \psi)$. Then $\psi \oplus \psi = \bigoplus_{i=1}^{n} \langle a_i, a_i\rangle$. Thus, by 4.2.4(c) there are $x_i \in D_G(a_i, a_i)$ such that $x \in D_G(\langle x_1, ..., x_n\rangle)$. By item (b), $x_i = a_i$ for all $i = 1, ..., n$, proving that $x \in D_G(\psi)$.

(c)$\Rightarrow$(d). Let $\psi' = \langle a_2, ..., a_n\rangle$. Then $\psi \oplus \psi = \langle a_1, a_1\rangle \oplus (\psi' \oplus \psi')$. Since $\psi \oplus \psi$ is isotropic, by 4.2.4(d), there is $x \in D_G(a_1, a_1)$ such that $-x \in D_G(\psi' \oplus \psi')$. By item (c), $x \in D_G(\langle a_1\rangle)$, so $x = a_1$ and $-a_1 = -x \in D_G(\psi')$. Invoking 4.2.4(d) again, we conclude that $\psi = \langle a_1\rangle \oplus \psi'$ is isotropic.

(d)$\Rightarrow$(e). Let ψ and ψ' as above and set $\theta = \langle b_1, ..., b_n\rangle$ with $\theta' = \langle b_2, ..., b_n\rangle$. We proceed by induction on n. Assume $\psi \oplus \psi \equiv \theta \oplus \theta$; then $\langle a_1, a_1\rangle \oplus (\psi' \oplus \psi') \equiv \langle b_1, b_1\rangle \oplus (\theta' \oplus \theta')$, which from

$$\langle a_1, a_1\rangle \oplus \langle -b_1, -b_1\rangle \oplus (\psi' \oplus \psi') \equiv \langle 1, -1\rangle \oplus \langle 1, -1\rangle \oplus (\theta' \oplus \theta'), \qquad (*)$$

i.e, the form $\langle 1, 1\rangle \otimes (\langle a_1, -b_1\rangle \oplus \psi')$ is isotropic. By item (d), the same is true of $\langle a_1, -b_1\rangle \oplus \psi' \equiv \langle -b_1\rangle \oplus \psi$. Thus, there is a form θ_0 of dimension $n - 1$ such that

$$\langle -b_1\rangle \oplus \psi \equiv \langle 1, -1\rangle \oplus \theta_0 \equiv \langle b_1, -b_1\rangle \oplus \theta_0, \qquad (**)$$

where we have used the preservation of isometry by sum and SG2. By Witt cancellation, $\psi \equiv \langle b_1\rangle \oplus \theta_0$. From (*) and (**) we also have

$$\begin{aligned} \langle 1, 1\rangle \otimes (\langle 1, -1\rangle \oplus \theta') &\equiv \langle 1, 1\rangle \otimes (\langle -b_1\rangle \oplus \psi) \\ &\equiv \langle 1, 1\rangle \otimes (\langle 1, -1\rangle \oplus \theta_0); \end{aligned}$$

cancelling out $\langle 1, 1\rangle \otimes \langle 1, -1\rangle$, gives $\langle 1, 1\rangle \otimes \theta' \equiv \langle 1, 1\rangle \otimes \theta_0$. By the induction hypothesis, $\theta' \equiv \theta_0$, which yields

$$\theta \equiv (\langle -b_1\rangle \oplus \theta') \equiv \langle -b_1\rangle \oplus \theta_0 \equiv \psi,$$

as desired.

(e)$\Rightarrow$(f). Assume that $\psi \oplus \psi$ is hyperbolic. Since $\dim(\psi)$ is even, say $2l$, our assumption comes down to

$$\psi \oplus \psi \equiv \bigoplus_{i=1}^{n} \langle 1, -1\rangle = (2l) \times \langle 1, -1\rangle \equiv \theta \oplus \theta$$

with $\theta = \bigoplus_{i=1}^{l} \langle 1, -1\rangle$. By item (e), $\psi \equiv \theta$ which means ψ hyperbolic.

(f)⇒(a). Assume that $\langle a,a\rangle \equiv \langle 1,1\rangle$. Then the form $\langle a,-1\rangle \oplus \langle a,-1\rangle$ is hyperbolic. By item (f), so is $\langle a,-1\rangle$, that is, $\langle a,-1\rangle \equiv \langle 1,-1\rangle$, which implies $a=1$ by SG3. □

Example 4.2.6 (Fan)**.** *Let G be a group of exponent 2 with a distinguished element $-1\neq 1$. For each $a\in G$, $a\neq -1$, define $G_a=\{1,a\}$, setting $G_{-1}=G$. We now define a relation $\equiv_{fan}$ on $G\otimes G$ by*

$$\langle a,b\rangle \equiv_{fan} \langle c,d\rangle \text{ iff } ab=cd \text{ and } ac\in G_{cd}. \tag{fan}$$

Indeed, $(G,\equiv_{fan},-1)$ is a reduced special group with $D_G(1,a)=G_a$. We will make a proof of this in our second functorial picture, in theorem 4.3.1.

Example 4.2.7. *Consider the multiplicative group $\mathbf{2}=\{\pm 1\}$ with -1 as the distinguished element. By the previous example, define for $a,b,c,d\in\mathbf{2}$*

$$\langle a,b\rangle \equiv_{fan} \langle c,d\rangle \text{ iff } a+b=c+d \,(\text{computed in } \mathbb{Z}).$$

With this structure, $\{\pm 1\}$ is a reduced special group with $D(1,1)=\{1\}$ and $D(1,-1)=\mathbf{2}$.

If t is a form over $\mathbf{2}$ of dimension n (i.e, a sequence of 1's and -1's of length $n\geq 1$), let $p_t=$ number of 1's and $n_t=$ number of -1's in t. Then $p_t+n_t=n$. If s,t are forms of dimension n in $\mathbf{2}$, then the definition of isometry of n-forms and induction, yields

$$s\equiv_{fan} t \text{ iff } \sum_{i\leq n} s(i)=\sum_{i\leq n} t(i) (\text{in } \mathbb{Z}) \text{ iff } p_s=p_t \text{ and } n_s=n_t.$$

This is the only structure of reduced (pre-)special group on $\mathbf{2}$, with $1\neq -1$, to be indicated by $\mathbb{Z}_2$.

Example 4.2.8 (The trivial special relation)**.** *Let G be a group of exponent 2 and -1 any element of G distinct from 1. For $a,b,c,d\in G$ define*

$$\langle a,b\rangle \equiv_t \langle c,d\rangle \text{ iff } ab=cd.$$

Is an immediate consequence of this that $(G,\equiv_t,-1)$ is a pre-special group. For SG6, we will proof that For forms $\varphi=\langle a_1,...,a_n\rangle$ and $\psi=\langle b_1,...,b_n\rangle$ on G,

$$\varphi\equiv_t\psi \text{ iff } d(\varphi)=d(\psi).$$

Of course, follows by Lemma 4.2.3(b) that $\varphi\equiv_t\psi$ implies the equality of discriminants. For the converse, we use induction on $n\geq 2$, observing that for $n=2$ the equality of discriminants is the definition of $\equiv_t$.

Assume $n\geq 3$ and that $d(\varphi)=d(\psi)$. Set $\alpha=d(\langle a_2,...,a_n\rangle)$ and $\beta=d(\langle b_2,...,b_n\rangle)$. Let $\vec{z}=(z_3,...,z_n)=(1,...,1)$. Then, using the induction hypothesis,

i - $a_1\alpha=b_1\beta$ *yields* $\langle a_1,\alpha\rangle\equiv_t\langle b_1,\beta\rangle$;

ii - $\alpha d(\langle\vec{z}\rangle)=\alpha$ *yields* $\langle a_2,...,a_n\rangle\equiv_t\langle\alpha,\vec{z}\rangle$;

iii - $\beta d(\langle\vec{z}\rangle)=\beta$ *yields* $\langle b_2,...,b_n\rangle\equiv_t\langle\beta,\vec{z}\rangle$.

The three isometries above imply $\varphi\equiv_t\psi$, as desired. In particular, $\equiv_t$ is transitive. We refer to the relation $\equiv_t$ as the trivial special group structure on G, denoting it by G_t.

It is straightforward to verify that G_t is never reduced, all binary forms are universal and all forms of dimension ≥ 3 are isotropic.

Example 4.2.9 (Extension)**.** *Let $(G, \equiv, -1)$ be a SG and Δ be a group of exponent 2. Write $G[\Delta]$ for the group $G \times \Delta$ with its usual (coordinate-wise) group structure, with $\mathbb{1} = (1,1)$ as identity and $-\mathbb{1} = (-1,1)$ as distinguished element. We write $g \cdot \delta$, instead of (g,δ), for a typical element of $G[\Delta]$. For each $g \cdot \delta$ in $G[\Delta]$ we define a subgroup $E_{g\cdot\delta}$ of $G[\Delta]$ as follows:*

$$E_{g\cdot\delta} = \begin{cases} D_G(1,g) \times \{1\} \text{ if } g \neq -1 \text{ and } \delta = 1; \\ G[\Delta] \text{ if } g = -1 \text{ and } \delta = 1; \\ \{\mathbb{1}, g\cdot\delta\} \text{ if } \delta \neq 1 \end{cases} \tag{ext}$$

Define a relation $\equiv_{ext}$ on $G[\Delta] \times G[\Delta]$ by

$$(g_1\cdot\delta_1, g_2\cdot\delta_2) \equiv_{ext} (h_1\cdot\eta_1, h_2\cdot\eta_2) \Leftrightarrow \begin{cases} g_1g_2 = h_1h_2 \text{ and } \delta_1\delta_2 = \eta_1\eta_2 \\ h_1g_1\cdot\eta_1\delta_1 \in E_{g_1g_2\cdot\delta_1\delta_2}. \end{cases}$$

Lemma 4.2.10. *$(G[\Delta], \equiv_{ext}, \mathbb{1})$ is a special group that is reduced iff G is reduced.*

Proof. We will verify that $\equiv_{ext}$ is a special relation on $G[\Delta]$:

SG 0 - $\langle g_1\cdot\delta_1, g_2\cdot\delta_2\rangle \equiv_{ext} \langle g_1\cdot\delta_1, g_2\cdot\delta_2\rangle$ since $g_1g_1\cdot\delta_1\delta_1 = \mathbb{1} \in E_{g_1g_2\cdot\delta_1\delta_2}$. If $(g_1\cdot\delta_1, g_2\cdot\delta_2) \equiv_{ext} (h_1\cdot\eta_1, h_2\cdot\eta_2)$ then $g_1g_2 = h_1h_2$, $\delta_1\delta_2 = \eta_1\eta_2$ and $h_1g_1\cdot\eta_1\delta_1 \in E_{g_1g_2\cdot\delta_1\delta_2} = E_{h_1h_2\cdot\eta_1\eta_2}$, so $(h_1\cdot\eta_1, h_2\cdot\eta_2) \equiv_{ext} (g_1\cdot\delta_1, g_2\cdot\delta_2)$. Now, suppose $(g_1\cdot\delta_1, g_2\cdot\delta_2) \equiv_{ext} (h_1\cdot\eta_1, h_2\cdot\eta_2)$ and $(h_1\cdot\eta_1, h_2\cdot\eta_2) \equiv_{ext} (l_1\cdot\theta_1, l_2\cdot\theta_2)$. Then $g_1g_2 = h_1h_2 = l_1l_2$ and $\delta_1\delta_2 = \eta_1\eta_2 = \theta_1\theta_2$. Since $g_1h_1\cdot\delta_1\eta_1 \in E_{g_1g_2\cdot\delta_1\delta_2} = E_{l_1l_2\cdot\theta_1\theta_2}$ and $h_1l_1\cdot\eta_1\theta_1 \in E_{h_1h_2\cdot\eta_1\eta_2} = E_{l_1l_2\cdot\theta_1\theta_2}$, we have

$$g_1l_1\cdot\delta_1\theta_1 = (g_1h_1\cdot\delta_1\eta_1)(h_1l_1\cdot\eta_1\theta_1) \in E_{l_1l_2\cdot\theta_1\theta_2}.$$

This proves that $\equiv_{ext}$ is an equivalence relation.

SG 1 - $(g_1\cdot\delta_1, g_2\cdot\delta_2) \equiv_{ext} (g_2\cdot\delta_2, g_1\cdot\delta_1)$ is just consequence of $g_1g_2\cdot\delta_1\delta_2 \in E_{g_1g_2\cdot\delta_1\delta_2}$.

SG 2 - $(g\cdot\delta, -g\cdot\delta) \equiv_{ext} (\mathbb{1}, -\mathbb{1})$ is just consequence of $g\cdot\delta \in E_{-\mathbb{1}}$.

SG 3 - Follow from the definition of $\equiv_{ext}$.

SG 4 - Let $(g_1\cdot\delta_1, g_2\cdot\delta_2) \equiv_{ext} (h_1\cdot\eta_1, h_2\cdot\eta_2)$. Then $g_1g_2 = h_1h_2$, $\delta_1\delta_2 = \eta_1\eta_2$ and $g_1h_1\cdot\delta_1\eta_1 \in E_{g_1g_2\cdot\delta_1\delta_2}$. Of course, we have $-g_1h_1 = -g_2h_2$ and $-\delta_1\eta_1 = -\delta_2\eta_2$. Then, we just need to prove that $-g_1g_2\cdot\delta_1\delta_2 \in E_{-g_1h_1\cdot\delta_1\eta_1}$. We divide this in cases:

Case 1: $\delta_1\delta_2 \neq 1$. In this case, $E_{g_1g_2\cdot\delta_1\delta_2} = \{\mathbb{1}, g_1g_2\cdot\delta_1\delta_2\}$. Then $g_1h_1\cdot\delta_1\eta_1 = \mathbb{1}$ or $g_1h_1\cdot\delta_1\eta_1 = g_1g_2\cdot\delta_1\delta_2$. In both cases we have $-g_1g_2\cdot\delta_1\delta_2 \in E_{-g_1h_1\cdot\delta_1\eta_1} = \{\mathbb{1}, -g_1h_1\cdot\delta_1\eta_1\}$, since $\eta_1\eta_2 \neq 1$ too.

Case 2: $\delta_1\delta_2 = 1$ and $g_1g_2 = -1$. Then $-g_1g_2\cdot\delta_1\delta_2 = \mathbb{1} \in E_{-g_1h_1\cdot\delta_1\eta_1}$.

Case 3: $\delta_1\delta_2 = 1$ and $g_1g_2 \neq -1$. From $g_1h_1\cdot\delta_1\eta_1 \in E_{g_1g_2\cdot\delta_1\delta_2}$ we obtain $\delta_1\eta_1 = 1$ and $g_1h_1 \in D_G(1, g_1g_2)$. So there exits $t \in G$ such that $\langle 1, g_1g_2\rangle \equiv_G \langle g_1h_1, t\rangle$. From SG4 on G, we have $\langle 1, -g_1h_1\rangle \equiv_G \langle -g_1g_2, t\rangle$, then $-g_1g_2 \in D_G(1, -h_1h_2)$. This imply that $-g_1g_2\cdot 1 \in E_{-g_1h_1\cdot 1}$.

SG 5 - Let $(g_1\cdot\delta_1, g_2\cdot\delta_2) \equiv_{ext} (h_1\cdot\eta_1, h_2\cdot\eta_2)$. Then

$$g_1g_2 = h_1h_2 \text{ and } \delta_1\delta_2 = \eta_1\eta_2 \Rightarrow (xg_1)(xg_2) = (xh_1)(xh_2) \text{ and } (\theta\delta_1)(\theta\delta_2) = (\theta\eta_1)(\theta\eta_2)$$

and

$$g_1h_1 \cdot \delta_1\eta_1 \in E_{g_1g_2\cdot\delta_1\delta_2} \Rightarrow (xg_1)(xh_1)\cdot(\theta\delta_1)(\theta\eta_1) \in E_{(xg_1)(xg_2)\cdot(\theta\delta_1)(\theta\delta_2)}.$$

So $((x\cdot\theta)(g_1\cdot\delta_1),(x\cdot\theta)(g_2\cdot\delta_2)) \equiv_{ext} ((x\cdot\theta)(h_1\cdot\eta_1),(x\cdot\theta)(h_2\cdot\eta_2))$.

SG 6 - We use a characterization for SG3 that we will prove in theorem 4.2.16: in a psg $(G,\equiv,-1)$, $\equiv$ is 3-transitive iff for all For all 3-forms φ and all $b_1,b_2,b_3 \in G$,

$$\varphi \equiv \langle b_1,b_2,b_3\rangle \text{ imples } \varphi \equiv \langle b_2,b_1,b_3\rangle.$$

Now, let $\varphi = \langle a_1\cdot\delta_1, a_2\cdot\delta_2, a_3\cdot\delta_3$ and suppose $\varphi \equiv_{ext} \langle b_1\cdot\eta_1, b_2\cdot\eta_2, b_3\cdot\eta_3\rangle$. Then, there exist $x\cdot\delta, y\cdot\eta, z\cdot\theta \in G[\Delta]$ such that

$$\begin{aligned}\langle a_1\cdot\delta_1, x\cdot\delta\rangle \equiv_{ext} \langle b_1\cdot\eta_1, y\cdot\eta\rangle, \langle a_2\cdot\delta_2, a_3\cdot\delta_3\rangle \equiv_{ext} \langle x\cdot\delta, z\cdot\theta\rangle \text{ and}\\ \langle b_2\cdot\eta_2, b_3\cdot\eta_3\rangle \equiv_{ext} \langle y\cdot\eta, z\cdot\theta\rangle.\end{aligned} \tag{4.13}$$

Lets keep in mind that we want to prove

$$\begin{aligned}\langle a_1\cdot\delta_1, a\cdot\alpha\rangle \equiv_{ext} \langle b_2\cdot\eta_2, b\cdot\beta\rangle, \langle a_2\cdot\delta_2, a_3\cdot\delta_3\rangle \equiv_{ext} \langle a\cdot\alpha, c\cdot\gamma\rangle \text{ and}\\ \langle b_1\cdot\eta_1, b_3\cdot\eta_3\rangle \equiv_{ext} \langle b\cdot\beta, c\cdot\gamma\rangle,\end{aligned} \tag{4.14}$$

for some $a\cdot\alpha, b\cdot\beta, c\cdot\gamma \in G[\Delta]$. Now, we have five cases to deal with:

Case 1: $\delta=\eta=\theta$**.** For this case, we use the following fact:

Fact 4.2.11. *Let G be a psg and Δ be a group of exponent 2. Given $\varphi = \langle a_1\cdot\delta_1,...,a_n\cdot\delta_n\rangle$, $\psi = \langle b_1\cdot\eta_1,...,b_n\cdot\eta_n\rangle$ be forms on $G[\Delta]$, then*

$$\varphi \equiv_{ext} \psi \Rightarrow \delta_1...\delta_n = \eta_1...\eta_n \text{ and } \langle a_1,...,a_n\rangle \equiv_G \langle b_1,...,b_n\rangle.$$

Proof. We prove by induction on n. Let $n=2$ and suppose that $\langle a_1\cdot\delta_1, a_2\cdot\delta_2\rangle \equiv_{ext} \langle b_1\cdot\eta_1, b_2\cdot\eta_2\rangle$. We already have $\delta_1\delta_2 = \eta_1\eta_2$ and $a_1a_2 = a_1a_2$, so the discriminant part is done. Of course, the definition of $\equiv_{ext}$ yield $a_1b_1\cdot\delta_1\eta_1 \in E_{a_1a_2\cdot\delta_1\delta_2}$. Now, to prove that $\langle a_1,a_2\rangle \equiv_G \langle b_1,b_2\rangle$, we divide the argument in cases:

Case 1: $\delta_1\delta_2 \neq 1$. Then $E_{a_1a_2\cdot\delta_1\delta_2} = \{\mathbb{1}, a_1a_2\cdot\delta_1\delta_2\}$, and $a_1b_1\cdot\delta_1\eta_1 = \mathbb{1}$ or $a_1b_1\cdot\delta_1\eta_1 = a_1a_2\cdot\delta_1\delta_2$. Then $a_1b_1 = 1$ or $a_1b_1 = a_1a_2$ so $b_1 = a_1$ and $b_2 = a_2$ or $b_1 = a_2$ and $b_2 = a_1$. In both cases we have $\langle a_1,a_2\rangle \equiv_G \langle b_1,b_2\rangle$.

Case 2: $\delta_1\delta_2 = 1$ and $a_1a_2 = -1$. Then $b_1b_2 = -1$, $a_2 = -a_1$ and $b_2 = -b_1$. By SG2 on G, we have $\langle a_1,-a_1\rangle \equiv_G \langle 1,-1\rangle \equiv_G \langle b_1,-b_1\rangle$.

Case 3: $\delta_1\delta_2 = 1$ and $a_1a_2 \neq -1$. From $a_1b_1\cdot\delta_1\eta_1 \in E_{a_1a_2\cdot\delta_1\delta_2}$ we get $a_1b_1 \in D_G(1,g_1g_2)$. By 4.2.3(a) we obtain $\langle a_1,a_2\rangle \equiv_G \langle b_1,b_2\rangle$.

Now, suppose the assertion valid for $n-1$ and let $\varphi = \langle a_1\cdot\delta_1,...,a_n\cdot\delta_n\rangle$ and $\psi = \langle b_1\cdot\eta_1,...,b_n\cdot\eta_n\rangle$. By definition. $\varphi \equiv_{ext} \psi$ iff there exists $x\cdot\delta, y\cdot\eta, z_3\cdot\theta_3,...,z_n\cdot\eta_n \in G[\Delta]$ such that

$$\begin{aligned}\langle a_1\cdot\delta_1, x\cdot\delta\rangle &\equiv_{ext} \langle b_1\cdot\eta_1, y\cdot\eta\rangle\\ \langle a_2\cdot\delta_2,...,a_n\cdot\delta_n\rangle &\equiv_{ext} \langle x\cdot\delta, z_3\cdot\theta_3,...,z_n\cdot\eta_n\rangle\\ \langle b_2\cdot\eta_2,...,b_n\cdot\eta_n\rangle &\equiv_{ext} \langle y\cdot\eta, z_3\cdot\theta_3,...,z_n\eta_n\rangle\end{aligned}$$

By induction hypothesis, this imply $\delta_1\delta = \eta_1\eta$, $\delta_2...\delta_n = \theta_2...\theta_n = \eta_2...\eta_n$ and

$$\begin{aligned}\langle a_1, x\rangle &\equiv_G \langle b_1, y\rangle\\ \langle a_2, ..., a_n\rangle &\equiv_G \langle x, z_3, ..., z_n\rangle\\ \langle b_2, ..., b_n\rangle &\equiv_G \langle y, z_3, ..., z_n\rangle\end{aligned}$$

i.e, $\delta_1...\delta_n = \eta_1...\eta_n$ and $\langle a_1, ..., a_n\rangle \equiv_G \langle b_1, ..., b_n\rangle$. □

Now, lets return to the case $\delta = \eta = \theta$. From the fact, we have 4.13 imply $\langle a_1, a_2, a_3\rangle \equiv_G \rangle b_1, b_2, b_3\rangle$, and since G is a special group, we conclude $\langle a_1, a_2, a_3\rangle \equiv_G \langle b_2, b_1, b_3\rangle$. Therefore, exists $a, b, c \in G$ such that

$$\begin{aligned}\langle a_1, a\rangle \equiv_G \langle b_2, b\rangle, &\langle a_2, a_3\rangle \equiv_G \langle a, c\rangle \text{ and}\\ &\langle b_2, b_3\rangle \equiv \langle b, c\rangle.\end{aligned} \tag{4.15}$$

From 4.13 again, we get

$$\begin{aligned}\langle a_1 \cdot \delta_1, x \cdot \theta\rangle \equiv_{ext} \langle b_1 \cdot \eta_1, y \cdot \theta\rangle, \langle a_2 \cdot \delta_2, a_3 \cdot \delta_3\rangle \equiv_{ext} \langle x \cdot \theta, z \cdot \theta\rangle \text{ and}\\ \langle b_2 \cdot \eta_2, b_3 \cdot \eta_3\rangle \equiv_{ext} \langle y \cdot \theta, z \cdot \theta\rangle.\end{aligned} \tag{4.16}$$

Then $\delta_2\delta_3 = \eta_2\eta_3 = 1$. Moreover, $a_1b_1 \cdot \delta_1\eta_1 \in E_{a_1x\cdot\delta_1\theta}$, $a_2x \cdot \delta_2\theta \in E_{a_2a_3\cdot 1}$ and $b_2y \cdot \eta_2\theta \in E_{b_2b_3\cdot 1}$. Therefore, $\delta_1 = \eta_1 = \lambda$ and

$$\delta = \delta_2 = \delta_3 = \eta = \eta_2 = \eta_3 = \theta.$$

After this, we have two cases: $\lambda = \theta$ and $\lambda \neq \theta$. If $\lambda = \theta$, let a, b, c as in 4.15 and set $\alpha = \beta = \gamma = \theta$ to obtain 4.14.

If $\lambda \neq \theta$, from $a_1b_1 \cdot 1 \in E_{a_1x\cdot\lambda\theta}$, we obtain $a_1b_1 \cdot 1 \in \{\not\Vdash, a_1x \cdot \lambda\delta\}$. Since $\lambda\delta \neq 1$, we have $a_1 = b_1$. This implies $x = y$, and by 4.16 and transitivity of $\equiv_{ext}$ on 2-forms (SG0), we have $\langle a_2 \cdot \delta_2, a_3 \cdot \delta_3\rangle \equiv_{ext} \langle b_2 \cdot \eta_2, b_3 \cdot \eta_3\rangle$. Then

$$\begin{aligned}\langle a_1 \cdot \lambda, b_2 \cdot \theta\rangle \equiv_{ext} \langle b_2 \cdot \theta, a_1 \cdot \lambda\rangle, \langle a_2 \cdot \delta_2, a_3 \cdot \delta_3\rangle \equiv_{ext} \langle b_2 \cdot \eta_2, b_3 \cdot \eta_3\rangle \text{ and}\\ \langle b_1 \cdot \lambda, b_3 \cdot \theta\rangle \equiv_{ext} \langle a_1 \cdot \lambda, b_3 \cdot \theta\rangle.\end{aligned}$$

Setting $a = b_2$, $b = a_1$, $c = b_3$ and $\alpha = \theta$, $\beta = \lambda$, $\gamma = \theta$ we get 4.14.

Case 2: $\delta = \theta$**,** $\delta \neq \eta$**.** From 4.13 we get

$$\begin{aligned}\langle a_1 \cdot \delta_1, x \cdot \delta\rangle \equiv_{ext} \langle b_1 \cdot \eta_1, y \cdot \eta\rangle, \langle a_2 \cdot \delta_2, a_3 \cdot \delta_3\rangle \equiv_{ext} \langle x \cdot \delta, z \cdot \delta\rangle \text{ and}\\ \langle b_2 \cdot \eta_2, b_3 \cdot \eta_3\rangle \equiv_{ext} \langle y \cdot \eta, z \cdot \delta\rangle.\end{aligned} \tag{4.17}$$

Then $a_2x \cdot \delta_2\delta \in E_{xz\cdot 1}$ and since $\eta\delta \neq 1$, $b_2y \cdot \eta_2\eta \in E_{b_2b_3\cdot\eta_2\eta_3} = \{\mathbb{1}, b_2b_3 \cdot \eta_2\eta_3\}$.

If $b_2y \cdot \eta_2\eta = \mathbb{1}$, we get $y = b_2$, $\eta = \eta_2$, $z = b_3$ and $\delta = \eta_3$. Now, the isometries in 4.17 is rewritten as

$$\begin{aligned}\langle a_1 \cdot \delta_1, x \cdot \eta_3\rangle \equiv_{ext} \langle b_1 \cdot \eta_1, b_2 \cdot \eta_2\rangle, \langle a_2 \cdot \delta_2, a_3 \cdot \delta_3\rangle \equiv_{ext} \langle x \cdot \eta_3, b_3 \cdot \eta_3\rangle \text{ and}\\ \langle b_2 \cdot \eta_2, b_3 \cdot \eta_3\rangle \equiv_{ext} \langle b_2 \cdot \eta_2, b_3 \cdot \eta_3\rangle.\end{aligned} \tag{4.18}$$

Then, setting $a = x$, $b = b_1$, $c = b_3$ and $\alpha = \eta_3$, $\beta = \eta_1$, $\gamma = \eta_3$ we obtain the isometries in 4.14.

If $b_2y \cdot \eta_2\eta = b_2b_3 \cdot \eta_2\eta_3$, we get $y = b_3$, $\eta = \eta_3$, $z = b_2$ and $\delta = \delta_2$. Then, the isometries in 4.17 is rewritten as

$$\langle a_1 \cdot \delta_1, x \cdot \eta_3\rangle \equiv_{ext} \langle b_1 \cdot \eta_1, b_3 \cdot \eta_3\rangle, \langle a_2 \cdot \delta_2, a_3 \cdot \delta_3\rangle \equiv_{ext} \langle x \cdot \eta_2, b_2 \cdot \eta_2\rangle \text{ and}$$
$$\langle b_2 \cdot \eta_2, b_3 \cdot \eta_3\rangle \equiv_{ext} \langle b_3 \cdot \eta_3, b_2 \cdot \eta_2\rangle. \tag{4.19}$$

Now, setting $a = b_2$, $b = a_1$, $c = x$ and $\alpha = \eta_2$, $\beta = \delta_1$, $\gamma = \eta_2$ we obtain the isometries in 4.14.

Case 3: $\eta = \theta$**,** $\eta \neq \delta$**.** Similar to case 2.

Case 4: $\delta \neq \theta$**,** $\eta \neq \theta$**.** Here, the argument holds for both $\delta = \eta$ and $\delta \neq \eta$. From 4.13 we obtain $a_2x \cdot \delta_2\delta \in E_{a_2a_3 \cdot \delta_2\delta_3}$ and $b_2y \cdot \eta_2\eta \in E_{b_2b_3 \cdot \eta_2\eta_3}$. Since $\delta \neq \theta$ and $\eta \neq \theta$, we have $\delta_2\delta_3, \eta_2\eta_3 \neq 1$. Then $a_2x \cdot \delta_2\delta \in \{\mathbb{1}, a_2a_3 \cdot \delta_2\delta_3\}$ and $b_2y \cdot \eta_2\eta \in \{\mathbb{1}, b_2b_3 \cdot \eta_2\eta_3\}$.

If $a_2x \cdot \delta_2\delta = \mathbb{1} = b_2y \cdot \eta_2\eta$, we obtain $x = a_2$, $\delta = \delta_2$, $y = b_2$, $\eta = \eta_2$ and from isometries in 4.13, $a_3 = z = b_3$ and $\delta_3 = \theta = \eta_3$. Then setting $a = a_2$, $b = b_1$, $c = b_3 = a_3$ and $\alpha = \delta_2$, $\beta = \eta_1$, $\gamma = \eta_3$ we obtain the isometries in 4.14.

If $a_2x \cdot \delta_2\delta = \mathbb{1}$ and $b_2y \cdot \eta_2\eta = b_2b_3 \cdot \eta_2\eta_3$, we obtain $x = a_2$, $\delta = \delta_2$, $y = b_3$, $\eta = \eta_3$ and from isometries in 4.13, $z = a_3 = b_2$ and $\theta = \delta_3 = \eta_2$. Then setting $a = a_3 = b_2$, $b = a_1$, $c = a_2$ and $\alpha = \delta_3 = \eta_2$, $\beta = \delta_1$, $\gamma = \delta_2$ we obtain the isometries in 4.14.

If $a_2x \cdot \delta_2\delta = a_2a_3 \cdot \delta_2\delta_3$ and $b_2y \cdot \eta_2\eta = \mathbb{1}$, we obtain $x = a_3$, $\delta = \delta_3$, $y = b_2$, $\eta = \eta_2$ and from isometries in 4.13, $z = a_2 = b_3$ and $\theta = \delta_2 = \eta_3$. Then setting $a = a_3$, $b = a_1$, $c = a_2 = b_3$ and $\alpha = \delta_3$, $\beta = \eta_1$, $\gamma = \delta_2 = \eta_3$ we obtain the isometries in 4.14.

If $a_2x \cdot \delta_2\delta = a_2a_3 \cdot \delta_2\delta_3$ and $b_2y \cdot \eta_2\eta = b_2b_3 \cdot \eta_2\eta_3$, we obtain $z = a_2 = b_2$ and $\theta = \delta_2 = \eta_2$. Then setting $a = a_2 = b_2$, $b = a_1$, $c = a_3$ and $\alpha = \delta_2 = \eta_2$, $\beta = \delta_1$, $\gamma = \delta_3$ we obtain the isometries in 4.14.

Finally, the last assertion on the lemma is just the fact that

$$\langle a \cdot \theta, a \cdot \theta \equiv_{ext} \langle \mathbb{1}, \mathbb{1}\rangle \text{ iff } \langle a, a\rangle \equiv_G \langle 1, 1\rangle.$$

□

Definition 4.2.12. *A map* $(G, \equiv_G, -1) \xrightarrow{f} (H, \equiv_H, -1)$ *between PSG's is a morphism of PSG's or PSG-morphism if* $f : G \to H$ *is a homomorphism of groups,* $f(-1) = -1$ *and for all* $a, b, c, d \in G$

$$\langle a, b\rangle \equiv_G \langle c, d\rangle \Leftrightarrow \langle f(a), f(b)\rangle \equiv_H \langle f(c), f(d)\rangle$$

A morphism of special groups or SG-morphism is a PSG-morphism between the correspondents PSG's. f *will be an isomorphism if is bijective and* f, f^{-1} *are PSG-morphisms.*

If $\varphi = \langle a_1, ..., a_n\rangle$ is a form on G, the image form by f is denoted $f \star \varphi = \langle f(a_1), ..., f(a_n)\rangle$. Special groups (and reduced special groups) and their morphisms are categories, denoted respectively by $\mathcal{SG}$ and $\mathcal{RSG}$.

Lemma 4.2.13. *Let* $(G, \equiv_G, -1), (H, \equiv_H, -1)$ *be psg's and* φ, ψ *be* n *forms on* G*. Then*

a - A map $f : G \to H$ is a SG-morphism iff its a group homomorphism such that $f(-1) = -1$ and satisfies

$$\forall\, a \in G,\ f(D_G(1,a)) \subseteq D_H(1, f(a)). \tag{D}$$

b - A map $\sigma : G \to \mathbb{Z}_2$ is a morphism of psg's iff it is a group homomorphism taking -1 to -1 and satisfying

$$\forall\, a \in G,\ a \in Ker(\sigma) \Rightarrow D_G(1,a) \subseteq Ker(\sigma). \tag{Ker}$$

Moreover, if $f : G \to H$ is a morphism of psg's and $\sigma : H \to \mathbb{Z}_2$ is a group homomorphism satisfying [Ker], the same is true $\sigma \circ f : G \to \mathbb{Z}_2$.

c - If $f : G \to H$ is a morphism of special groups and φ, ψ are forms on G of the same dimension, then $\varphi \equiv_G \psi$ implies $f \star \varphi \equiv_H f \star \psi$.

Proof.

a - Suppose that f is a morphism and $b \in D_G(1,a)$. Then there is $u \in G$ such that $\langle b, u\rangle \equiv_G \langle 1, a\rangle$. Since f is a morphism, $\langle f(b), f(u)\rangle \equiv_H \langle 1, f(a)\rangle$, and so $f(b) \in D_H(1, f(a))$. Conversely, assume that f is a group homomorphism, taking -1 to -1 and satisfying [D]. Let a, b, c, d be elements of G such that $\langle a, b\rangle \equiv_G \langle c, d\rangle$. Then $ab = cd$ and $ac \in D_G(1, cd)$. Since $f(ab) = f(a)f(b) = f(c)f(d) = f(cd)$, to prove that f is a morphism of special groups, it is enough to verify (by 4.2.3(a)) that $f(ac) \in D_H(1, f(cd))$. But this comes directly from [D].

b - Follow by the fact that in this case, condition [D] is equivalent to [Ker].

c - Follow by induction on the dimension of φ and ψ with the fact that the result being true for forms of dimension 2 by definition.

□

4.2.2 Caracterization of Special Groups

In this section, we present a useful set of equivalent conditions for a pre-special group to be a special group.

If G is a group of exponent 2, $\varphi = \langle a_1, ..., a_n\rangle$ is a n-form over G and $\sigma \in S_n$, write φ^σ for the n-form $\varphi^\sigma = \langle a_{\sigma(1)}, ..., a_{\sigma(n)}\rangle$.

Lemma 4.2.14. *Let $(G, \equiv, -1)$ be a pre-special group. Let a, b, c, x, y be elements of G and φ, ψ forms over G. Assume that $\langle a, b\rangle \equiv \langle x, y\rangle$. Then*

a - $\varphi \equiv \psi\langle a, b\rangle \Rightarrow \varphi \equiv \psi\langle x, y\rangle$.

b - For all $\sigma \in S_3$, $\langle a, b, c\rangle \equiv \langle x, y, c\rangle^\sigma$.

Proof.

a - By induction on $\dim(\psi)$. Write $\varphi = \langle z\rangle \oplus \varphi_1$. If $\dim(\psi) = 1$, then $\psi = \langle\alpha\rangle$ and we must show that

$$\varphi \equiv \langle\alpha, a, b\rangle \Rightarrow \varphi \equiv \langle\alpha, x, y\rangle.$$

Then, there are $\gamma, \delta, \mu \in G$, such that

$$\langle z, \gamma\rangle \equiv \langle\alpha, \delta\rangle,\ \varphi_1 \equiv \langle\gamma, \mu\rangle \text{ and } \langle a, b\rangle \equiv \langle\delta, \mu\rangle.$$

The third isometry and $\langle a,b\rangle \equiv \langle x,y\rangle$ yield $\langle x,y\rangle \equiv \langle \delta,\mu\rangle$ which, together with the first two isometries, implies $\varphi \equiv \langle \alpha,x,y\rangle$.

Assume the result true for $\dim(\psi) = n-1$ and that $\psi = \langle y_1,...,y_n\rangle$. Then $\varphi \equiv \psi \oplus \langle a,b\rangle$ means that there are $\gamma,\delta,\mu_3,...,\mu_{n+2} \in G$ such that

$$\langle z,\gamma\rangle \equiv \langle y_1,\delta\rangle; \varphi_1 \equiv \langle \gamma,\mu_3,...,\mu_{n+2}\rangle; \tag{4.20}$$

$$\langle y_2,...,y_n\rangle \oplus \langle a,b\rangle \equiv\rangle \delta,\mu_3,...,\mu_{n+2}\rangle. \tag{4.21}$$

By the induction hypothesis, $\langle \delta,\mu_3,...,\mu_{n+2}\rangle \equiv \langle y_2,...,y_n\rangle \oplus \langle x,y\rangle$. But this isometry, and the first two isometries above, show that $\varphi \equiv \psi \oplus \langle x,y\rangle$.

b - By item (a) it is sufficient to verify that $\theta = \langle a,b,c\rangle$ is isometric to $\langle x,y,c\rangle$, $\langle y,x,c\rangle$ and $\langle c,x,y\rangle$. That the first two are isometric to θ follows directly from the preservation of $\equiv$ by sum and the hypothesis that $\langle a,b\rangle \equiv \langle x,y\rangle$ (and $\langle a,b\rangle \equiv \langle y,x\rangle$ by SG1). For the remaining permutation, observe that the isometries

$$\langle a,c\rangle \equiv \langle c,a\rangle,\ \langle b,c\rangle \equiv \langle c,b\rangle \text{ and } \langle x,y\rangle \equiv \langle a,b\rangle,$$

shows that $\theta \equiv \langle c,x,y\rangle$.

□

Two forms $\varphi = \langle a_1,...,a_n\rangle$, $\psi = \langle b_1,...,b_n\rangle$, over the psg G are said to be *simply equivalent*, if there are i,j (not necessary distinct) such that

i - $\langle a_i,a_j\rangle \equiv \langle b_i,b_j\rangle$;

ii - $a_k = b_k$, whenever k is distinct from i and j.

We say that φ,ψ are *chain-equivalent*, written $\varphi \approx \psi$, if there is a sequence of n-forms $\varphi_0,\varphi_1,...,\varphi_m$, such that $\varphi_0 = \varphi$, $\varphi_m = \psi$, and φ_k is simply equivalent to φ_{k+1} for $0 \le k \le m-1$.

Lemma 4.2.15. *Chain-equivalence is an equivalence relation. Moreover, if φ,ψ are n-forms over G and c is an element of G, then:*

a - $\varphi \approx \psi$ *iff* $\forall\, \sigma \in S_n$, $\varphi \approx \psi^\sigma$.

b - *If* $\varphi \approx \psi$ *implies* $\langle c\rangle \oplus \varphi \approx \langle c\rangle \oplus \psi$.

c - $\varphi \equiv \psi$ *implies* $\varphi \approx \psi$.

Proof. The fact that $\approx$ is an equivalence relation is straightforward. Note that a form ψ is simply equivalent to ψ^τ, where τ is a transposition in S_n.

a - Consequence of the fact that $\approx$ is transitive and that S_n is generated by transpositions.

b - Note that if φ is simply equivalent to ψ the same is true of $\langle c\rangle \oplus \varphi$ and $\langle c\rangle \oplus \psi$. So, any chain connecting φ and ψ becomes, adding $\langle c\rangle$ to each term, a chain connecting $\langle c\rangle \oplus \varphi$ to $\langle c\rangle \oplus \psi$.

c - By induction on dimension of φ, noting that for 2-forms there is nothing to prove. So suppose the result true for forms of dimension n and let $\varphi = \langle a\rangle \oplus \theta_0$ and $\psi = \langle b\rangle \oplus \theta_1$, where $\dim(\theta_0) = \dim(\theta_1) = n$. If $\varphi \equiv \psi$, there are $x,y,\vec{z} = (z_1,...,z_n) \in G$ such that

$$\langle a,x\rangle \equiv \langle b,y\rangle,\ \theta_0 \equiv \langle x,\vec{z}\rangle \text{ and } \theta_1 \equiv \langle y,\vec{z}\rangle.$$

By the induction hypothesis, the last two isometries yields $\theta_0 \approx \langle x, \vec{z}\rangle$ and $\theta_1 \approx \langle y, \vec{z}\rangle$. By item (b),

$$\varphi = \langle a\rangle \oplus \theta_0 \approx \langle a, x, \vec{z}\rangle \text{ and } \psi = \langle b\rangle \oplus \theta_1 \approx \langle b, y, \vec{z}\rangle.$$

Since $\approx$ is an equivalence relation and $\langle a, x, \vec{z}\rangle \approx \langle b, y, \vec{z}\rangle$ (because $\langle a, x\rangle \equiv \langle b, y\rangle$), we conclude $\varphi \approx \psi$, as desired.

□

The following result is very useful in verifying that a psg is a special group. It is interesting to know that it can be presented at an early stage in the development of the theory of special groups.

Theorem 4.2.16. *Let $(G, \equiv, -1)$ be a pre-special group. The following are equivalent:*

a - $\equiv$ is 3-transitive (i.e, transitive for 3-forms, and hence G is a special group).

b - $\equiv$ is transitive (i.e, transitive for n-forms for all $n \geq 2$).

c - For all $n \geq 2$, for all n-forms φ, ψ over G and all $\sigma \in S_n$,

$$\varphi \equiv \psi \text{ implies } \varphi \equiv \psi^\sigma.$$

d - For all $n \geq 2$, for all n-forms φ, ψ over G,

$$\varphi \equiv \psi \text{ iff } \varphi \approx \psi.$$

e - For all 3-forms φ and all $b_1, b_2, b_3 \in G$,

$$\varphi \equiv \langle b_1, b_2, b_3\rangle \text{ imples } \varphi \equiv \langle b_2, b_1, b_3\rangle.$$

Proof. (1)⇒(2). By induction on the dimension, which, when 2 or 3 are taken care of by assumption. Assume that $\langle a_1, ..., a_n\rangle \equiv \langle b_1, ..., b_n\rangle = \psi$ and $\psi \equiv \langle c_1, ..., c_n\rangle$, and that $\equiv$ is transitive on forms of dimension $n - 1 \geq 3$. The hypotheses yield $\alpha, \beta, \gamma, \delta, y_i, z_i \in G$, $3 \leq i \leq n$, such that (I) and (II) below hold true

$$\langle a_1, \alpha\rangle \equiv \langle b_1, \beta\rangle,\ \langle a_2, ..., a_n\rangle \equiv \langle \alpha, \vec{y}\rangle \text{ and } \langle b_2, ..., b_n\rangle \equiv \langle \beta, \vec{y}\rangle; \tag{I}$$

$$\langle b_1, \gamma\rangle \equiv \langle c_1, \delta\rangle,\ \langle b_2, ..., b_n\rangle \equiv \langle \gamma, \vec{z}\rangle \text{ and } \langle c_2, ..., c_n\rangle \equiv \langle \delta, \vec{z}\rangle, \tag{II}$$

where $\vec{y} = \langle y_3, ..., y_n\rangle$ and $\vec{z} = \langle z_3, ..., z_n\rangle$. By induction, $\equiv$ is transitive on $(n-1)$-forms, and so, $\langle \beta, \vec{y}\rangle \equiv \langle \gamma, \vec{z}\rangle$, since both are isometric to $b_2, ..., b_n\rangle$. Thus, there are $x, t, y.\vec{t} = \langle t_4, ..., t_n\rangle \in G$ such that

$$\langle \beta, x\rangle \equiv \langle \gamma, y\rangle,\ \langle \vec{y}\rangle \equiv \langle x, \vec{t}\rangle \text{ and } \langle \vec{z}\rangle \equiv \langle y, \vec{t}\rangle. \tag{III}$$

Now, by the preservation of isometry by sum, the first isometry in (I), (II) and (III) as well as 3-transitivity, we may write

$$\begin{aligned}\langle a_1, \alpha, x\rangle &= \langle a_1, \alpha\rangle \oplus \langle x\rangle \equiv \langle b_1, \beta\rangle \oplus \langle x\rangle \equiv \langle b_1\rangle \oplus \langle \beta, x\rangle \\ &\equiv \langle b_1\rangle \oplus \langle \gamma, y\rangle \equiv \langle b_1, \gamma\rangle \oplus \langle y\rangle \equiv \langle c_1, \delta\rangle \oplus \langle y\rangle = \langle c_1, \delta, y\rangle.\end{aligned}$$

Therefore, there are $u, v, w \in G$ such that

$$\langle a_1, u\rangle \equiv \langle c_1, v\rangle,\ \langle \alpha, x\rangle \equiv \langle u, w\rangle \text{ and } \langle \delta, y\rangle \equiv \langle v, w\rangle. \tag{IV}$$

The preservation of isometry by sum, the transitivity of $\equiv$ for $(n-1)$-forms, the second and the third isometry in (I) and (II), respectively, together with the last two in (III) and (IV), yield

$$\langle a_2, ..., a_n\rangle \equiv \langle \alpha, \vec{y}\rangle \equiv \langle \alpha, x, \vec{t}\rangle \equiv \langle u, w, \vec{t}\rangle \text{ and}$$
$$\langle c_2, ..., c_n\rangle \equiv \langle \delta, \vec{z}\rangle \equiv \langle \delta, y, \vec{t}\rangle \equiv \langle v, w, \vec{t}\rangle,$$

isometries which, together with the first one in (IV), prove that $\langle a_1, ..., a_n\rangle \equiv \langle c_1, ..., c_n\rangle$.

(2)⇒(3). By induction on dimension; for 2-forms, the conclusion follows from SG1. Let $\sigma \in S_n$, $\varphi = \langle a\rangle \oplus \varphi_1$ and $\psi = \langle b_1, ..., b_n\rangle$.

Case A. $\sigma(1) = 1$.

We may write $\psi^\sigma = \langle b_1\rangle \oplus \langle b_2, ..., b_n\rangle^\sigma$; moreover from $\varphi \equiv \psi$ we get $\alpha, \beta, \vec{y} = \langle y_3, ..., y_n\rangle \in G$ such that

$$\langle a, \alpha\rangle \equiv \langle b_1, \beta\rangle,\ \varphi_1 \equiv \langle \alpha, \vec{y}\rangle \text{ and } \langle b_2, ..., b_n\rangle \equiv \langle \beta, \vec{y}\rangle. \tag{V}$$

By induction, $\langle b_2, ..., b_n\rangle^\sigma \equiv \langle \beta, \vec{y}\rangle$ and this, together with the first two isometries in (V), yield $\varphi \equiv \langle b_1\rangle \oplus \langle b_2, ..., b_n\rangle^\sigma = \psi^\sigma$.

Case B. σ is a 2-cycle $(1, i)$ for some $i \geq 2$.

From $\varphi \equiv \psi$ we get the isometries in (V). Let $\vec{b} = \{b_k : k \neq 1, i\}$. By the induction hypothesis and the third isometry in (V), $\langle \beta, \vec{y}\rangle \equiv \langle b_i, \vec{b}\rangle$, and so it follows that $\langle \beta, \vec{y}, b_1\rangle \equiv \langle b_i, \vec{b}, b_1\rangle$.

Case A and the preservation of isometry by sum yield the following sequence of isometries:

$$\langle \beta, \vec{y}, b_1\rangle \equiv \langle \beta, b_1, \vec{y}\rangle = \langle \beta, b_1\rangle \oplus \langle \vec{y}\rangle \equiv \langle b_1, \beta\rangle \oplus \langle \vec{y}\rangle$$
$$\equiv \langle a, \alpha\rangle \oplus \langle \vec{y}\rangle = \langle a\rangle \oplus \langle \alpha, \vec{y}\rangle \equiv \varphi.$$

Since $\equiv$ is transitive, we get $\varphi \equiv \langle \beta, \vec{y}, b_1\rangle$, and thus, $\varphi \equiv \langle b_i, \vec{b}, b_1\rangle$. We may apply Case A once more to put b_1 in its desired place, preserving isometry, getting $\langle b_i, \vec{b}, b_1\rangle \equiv \psi^\sigma$. The transitivity of $\equiv$ now yields $\varphi \equiv \psi^\sigma$, concluding the proof of Case B.

Cases A and B show that $\varphi \equiv \psi$ implies $\varphi \equiv \psi^\sigma$, for any transposition $\sigma \in S_n$. Since $\equiv$ is assumed transitive and S_n is generated by transpositions, we conclude the desired implication for all $\sigma \in S_n$.

(3)⇒(4). By Lemma 4.2.15(c) it is enough to verify that $\varphi \approx \psi$ implies $\varphi \equiv \psi$.

We first verify that simple equivalence implies isometry. If φ is simply equivalent to ψ, then there are $a, b, x, y, \vec{z} \in G$ and permutations $\sigma, \tau \in S_n$, such that $\varphi^\sigma = \langle \vec{z}, a, b\rangle$ and $\psi^\tau = \langle \vec{z}, x, y\rangle$, with $\langle a, b\rangle \equiv \langle x, y\rangle$. By Lemma 4.2.14(a), $\varphi^\sigma \equiv \psi^\tau$, and so (3) guarantees that $\varphi \equiv \psi$, because $(\varphi^\sigma)^{\sigma^{-1}} = \varphi$, for all $\sigma \in S_n$ and all forms φ over G.

We use induction on the length l of chains φ_i, $0 \leq i \leq l$, which witness $\varphi \approx \psi$. If $l = 1$, φ is simply equivalent to ψ and we have already remarked that (with (3)) $\varphi \equiv \psi$. Suppose the result true for chains of lenght l and that φ_i, $0 \leq i \leq l+1$, is a chain connecting $\varphi = \varphi_0$ and $\psi = \varphi_{l+1}$. By induction, $\varphi \equiv \varphi_l$ with φ_l simply equivalent to ψ. Thus, just as above, there are $\sigma, \tau \in S_n$ and $a, b, x, y, \vec{z} \in G$ such that

$$\varphi_l^\sigma = \langle \vec{z}\rangle \oplus \langle a, b\rangle \text{ and } \psi^\tau = \langle \vec{z}\rangle \oplus \langle x, y\rangle,$$

with $\langle a, b\rangle \equiv \langle x, y\rangle$. By (3), $\varphi \equiv \psi_l^\sigma = \langle \vec{z}\rangle \oplus \langle a, b\rangle$. By Lemma 4.2.14(a), $\varphi \equiv \langle \vec{z}\rangle \oplus \langle x, y\rangle = \psi^\tau$. Another application of (3) gives $\varphi \equiv \psi$, as desired.

(4)⇒(5). This is a special case of Lemma 4.2.14(b).

(5)⇒(1). We show that if φ, ψ are 3-forms over G, then

$$\forall\, \sigma \in S_3,\ \varphi \equiv \psi \text{ implies } \varphi \equiv \psi^\sigma.$$

Once this is proven, then, exactly as in the proof of (3)⇒(4), we have that for all 3-forms φ, ψ, $\varphi \equiv \psi \Leftrightarrow \varphi \approx \psi$. Since $\approx$ is transitive, the same will be true of $\equiv$.

Let $\psi = \langle b_1, b_2, b_3\rangle$, $\sigma \in S_3$, and assume that $\varphi \equiv \psi$.

i - $\sigma(1) = 1$. Since $\langle b_2, b_3\rangle \equiv \langle b_3, b_2\rangle$ (SG1), it follows from Lemma 4.2.14(a) that $\varphi \equiv \psi$ implies $\varphi \equiv \psi^\sigma$.

ii - $\sigma(1) = 2$. In this case we have $\psi^\sigma = \langle b_2, b_i, b_j\rangle$, $\{i, j\} = \{1, 3\}$. If $i = 1$, the desired isometry follows directly from (5). If $i = 3$, using (5) and (i) in succession, we getting

$$\varphi \equiv \psi \Rightarrow \varphi \equiv \langle b_2, b_1, b_3\rangle \Rightarrow \varphi \equiv \langle b_2, b_3, b_1\rangle,$$

as needed.

iii - $\sigma(1) = 3$. By (i) above, we have $\varphi \equiv \langle b_1, b_3, b_2\rangle$; by (5), we can exchange b_1 and b_3 to get $\varphi \equiv \langle b_3, b_1, b_2\rangle$. Now, case (i) can be applied again, to get $\varphi \equiv \psi^\sigma$.

□

Corollary 4.2.17. *Let $(G, \equiv, -1)$ be a pre-special group. Let φ and ψ be forms over G and $a, b, x, y \in G$. The following are equivalent:*

a - G is a special group.

b - For all forms φ, ψ over G and all $a, b, x, y \in G$

$$\varphi \equiv \langle a, b\rangle \oplus \psi \text{ and } \langle a, b\rangle \equiv \langle x, y\rangle \Rightarrow \varphi \equiv \langle x, y\rangle \oplus \psi.$$

c - For all 3-forms φ, ψ over G and all $a, b, c, x, y \in G$

$$\varphi \equiv \langle a, b, c\rangle \text{ and } \langle a, b\rangle \equiv \langle x, y\rangle \Rightarrow \varphi \equiv \langle x, y, c\rangle.$$

Proof. That (a) implies (b) follows from Lemma 4.2.14(a) and the fact that G satisfies condition (3) in theorem 4.2.16. (b) implies (c) making $\psi = \langle c\rangle$. It remains to prove that (c) implies (a). We verify that, in fact, (c) implies condition (5) of theorem 4.2.16.

Assume that $\langle u, v, w\rangle \equiv \langle a, b, c\rangle$. Hence, there are α, β, γ in G such that

$$\langle u, \alpha\rangle \equiv \langle a, \beta\rangle,\ \langle v, w\rangle \equiv \langle \alpha, \gamma\rangle \text{ and } \langle b, c\rangle \equiv \langle \beta, \gamma\rangle. \qquad (*)$$

By 4.2.14(b), from $\langle u, \alpha\rangle \equiv \langle a, \beta\rangle$, we get $\langle \gamma, a, \beta\rangle \equiv \langle u, \alpha, \gamma\rangle$. Lemma 4.2.14(a) (with $\langle \gamma, a, \beta\rangle = \varphi$ and $\langle u\rangle = \psi$) and the second isometry in (*) also yield $\langle \gamma, a, \beta\rangle \equiv \langle u, v, w\rangle$. Since $\langle a, \beta\rangle \equiv \langle \beta, a\rangle$, 4.2.14(a) once again (this time with $\langle u, v, w\rangle = \varphi$ and $\langle \gamma\rangle = \psi$), implies $\langle u, v, w\rangle \equiv \langle \gamma, \beta, a\rangle$. Now, (c) and the third isometry in (*) yield $\langle u, v, w\rangle \equiv \langle b, c, a\rangle$, and yet another application of 4.2.14(a) gives $\langle u, v, w\rangle \equiv \langle b, a, c\rangle$, as desired. □

The usual construction of the Witt ring of a field can be carried out, in almost identical terms, for special groups as well.

Let $(G, \equiv_G, -1)$ be a special group (not necessarily reduced). Two forms φ, ψ over G are called *Witt-equivalent* (over G), written $\varphi \approx_G \psi$, if there are integers $n, m \geq 0$ such that

$$\varphi \oplus n\langle 1, -1\rangle \equiv_G \psi \oplus m\langle 1, -1\rangle.$$

We have that $\approx_G$ is an equivalence relation on forms over G, compatible with (and coarser than) the isometry relation $\equiv_G$.

We denote by $W(G)$ the set of equivalence classes of forms over G under Witt-equivalence, and by $\overline{\varphi}$ the Witt-equivalence class of the form φ. The following proposition summarizes the basic properties of this construction. The proof follow the same line as the arguments made in chapters 1 and 3.

Proposition 4.2.18. *Let G be a special group and let φ, ψ be forms over G.*

a - Witt-equivalence is a congruence with respect to sum and product of forms.

b - With the operations $\overline{\varphi} + \overline{\psi} = \overline{\varphi \oplus \psi}$ and $\overline{\varphi}\overline{\psi} = \overline{\varphi \otimes \psi}$, $W(G)$ is a commutative ring having as zero the class of hyperbolic forms and $\overline{\langle 1\rangle}$ as multiplicative identity.

c - The set $I(G)$ of (classes of) even dimensional forms is a maximal ideal in $W(G)$ (called the fundamental ideal of $W(G)$). Moreover $W(G)/I(G)$ is the two element field.

d - For $n \geq 1$, the n^{th} power of $I(G)$, denoted $I^n(G)$ is generated, as an abelian group, by the multiplies of Pfister forms of degree n, that is, every element of $I^n(G)$ is Witt-equivalent to a linear combination $\oplus_{i=1}^{k} a_i\varphi_i$ of Pfister forms φ_i of degree n, with coefficients $a_i \in G$.

4.2.3 Fields and Special Groups

In this section, we shall present a proof that the usual quadratic form theories over fields of characteristic distinct from 2 – reduced and not necessarily reduced – yield special groups. These examples are of course, at the root of the concept of special group.

Let F be a field with $\mathrm{char}(F) \neq 2$, which will remain fixed in what follow. We set $F(G) = \dot{F}/\dot{F}^2$ and in the case F be formally real, we define $G_{red}(F) = \dot{F}/\sum \dot{F}^2$. Of course, both $G(F)$ and $G_{red}(F)$ are groups of exponent 2.

We wish to show that the usual notion of isometry in $G(F)$ and in $G_{red}(F)$ yield special groups, the latter always reduced. To this end, we introduce the following:

Definition 4.2.19. *Let T be a subset of $\dot{F}$ and write $T^* = T \cup \{0\}$.*

a - If $a, b \in \dot{F}$,

$$D_T(a, b) = \{t \in \dot{F} : t = ap + bq \text{ for some } p, q \in T^*\}$$

is the set of elements represented by $\langle a, b\rangle$ over T. $\{a, b\} \subseteq D_T(a, b)$ is immediate.

b - T is a SG-subgroup of F iff it satisfies the following conditions:

i - T is a proper subgroup of the multiplicative group $\dot{F}$;

ii - $\dot{F}^2 \subseteq T$;

iii - For all $a \in \dot{F}$, $D_T(1, a)$ is a subgroup of $\dot{F}$.

Since T is a subgroup of $\dot{F}$, for all $p \in \dot{F}$, $p \in T$ iff $1/p \in T$.

We now show that squares, sums of squares and pre-orderings are examples of SG-subgroups.

Lemma 4.2.20. *With notation as above, let T be a subgroup of $\dot{F}$, containing $\dot{F}^2$ and satisfying:*

$$\begin{gathered}\forall\, p,q,u,v \in T \text{ and } \forall\, a \in \dot{F}\, \exists\, x \in F \text{ such that} \\ (pua^2 + qv - xa) \in T^* \text{ and } (pv + qu + x) \in T^*.\end{gathered} \tag{CS}$$

Then T is a SG-subgroup of F. In particular, $\dot{F}^2$ is a SG-subgroup of F and if F is formally real, $\sum \dot{F}^2$ and pre-orders are SG-subgroups of F.

Proof. For $s,t \in D_T(1,a)$ we must show that $1/s$ and st are in $D_T(1,a)$. We may write

$$s = pq + q \text{ and } t = ua + v, \tag{I}$$

with $p,q,u,v \in T^*$. Dividing the first equation by $1/s^2 \in T$ shows that $1/s \in D_T(1,a)$. To verify that $st \in D_T(1,a)$, consider the product of the equations in (I), namely

$$st = pua^2 + qv + (pv + qu)a. \tag{II}$$

Then, (II) implies that if any one of p,q,u,v is zero, then $st \in D_T(1,a)$. Assume then, that all these coefficients are in T. By (CS), there is $x \in F$ such that

$$\begin{aligned} st &= pua^2 + qv - xa + xa + (pv + qu)a = \\ &= \underbrace{(pua^2 + qv - xa)}_{\alpha} + \underbrace{pv + qu + x}_{\beta}\, a, \end{aligned}$$

with $\alpha, \beta \in T^*$, and hence $D_T(1,a)$ is a subgroup of $\dot{F}$.

If T is closed under sums (as is the case of a pre-order or of $\sum \dot{F}^2$), then it satisfies (CS) with $x = 0$, for all $a \in \dot{F}$. If $T = \dot{F}^2$, then $p = p_1^2$, $q = q_1^2$, $u = u_1^2$ and $v = v_1^2$; we take $x = 2(p_1 q_1 u_1 v_1)$ to prove (CS) for all $a \in \dot{F}$. For instance, $pua^2 + qv - xa = (p_1 u_1 a - q_1 v_1)^2$. □

Let T be a fixed (but otherwise arbitrary) SG-subgroup of F. Let $G_T(F) = \dot{F}/T$ be the exponent-2 quotient of $\dot{F}$ by T; write a_T for the class of $a \in \dot{F}$ in $G_T(F)$. For $a,b \in \dot{F}$ we have

$$a_T = b_T \text{ iff } a,b \in T \text{ iff } \exists\, p \in T \text{ such that } b = ap. \tag{*}$$

Lemma 4.2.21. *With the notation above, let a,b,c,d,t be elements of $\dot{F}$. Then*

a - $t \in D_T(a,b) \Rightarrow t_T \subseteq D_T(a,b)$.

b - $tD_T(a,b) = D_T(ta,tb)$.

c - $a_T = c_T$ and $b_T = d_T \Rightarrow D_T(a,b) = D_T(c,d)$.

Proof. For item (a), let $t \in D_T(a,b)$. Then, $t = ap + bq$ for some $p,q \in \dot{T}$. If $w \in t_T$, by (*) above, $w = tx$, for some $x \in T$. Then

$$w = tx = (ap + bq)x = a(px) + b(qx), \text{ with } px, qx \in \dot{T}.$$

This implies $w \in D_T(a,b)$, as desired.

Itens (b) and (c) are immediate consequence of $T + T \subseteq T$, $T \cdot T \subseteq T$ and (*) above. □

We now define a relation $\equiv$ on $G_T(F) \times G_T(F)$ by

$$\langle a_T, b_T \rangle \equiv \langle c_T, d_T \rangle \text{ iff } (ab)_T = (cd)_T \text{ and } D_T(a,b) = D_T(c,d).$$

When T is $\dot{F}^2$ or a pre-order, this relation is precisely the isometry of 2-forms in the non-reduced or reduced theory of quadratic forms, respectively.

Proposition 4.2.22. *If $a, b, c, d, t \in \dot{F}$, then*

a - $t \in D_T(a,b)$ *iff* $D_T(t,abt) = D_T(a,b)$ *iff* $\langle t_T, (abt)_T\rangle \equiv \langle a_T, b_T\rangle$.

b - $\langle a_T, b_T\rangle \equiv \langle c_T, d_T$ *iff* $\begin{cases} (ab)_T = (cd)_T \\ \text{and} \\ D_T(a,b) \cap D_T(c,d) \neq \emptyset. \end{cases}$

Proof.

a - One should keep in mind that $\dot{F}^2 \subseteq T$. To prove (a) it is enough to verify that

$$t \in D_T(a,b) \text{ implies } D_T(t,abt) = D_T(a,b),$$

the other implications coming directly from the definition of $\equiv$. We first note that if $x \in D_T(1,y)$, then

$$D_T(x,xy) = xD_T(1,y) = D_T(1,y). \tag{4.22}$$

To verify this, since $D_T(1,y)$ is a subgroup of $\dot{F}$, if $x \in D_T(1,y)$, then $1/x \in D_T(1,y)$ and we have $xD_T(1,y) \subseteq D_T(1,y)$ and $1/xD_T(1,y) \subseteq D_T(1,y)$, relations which, together with Lemma 4.2.21(b), prove $xD_T(1,y) = D_T(1,y)$, verifying 4.22.

If $t \in D_T(a,b)$, then $at \in D_T(1,ab)$ and so, by 4.22, $D_T(ta,(tab)a) = D_T(1,ab)$. Thus, we have

$$\begin{aligned} D_T(a,b) = D_T(a,ba^2) &= aD_T(1,ab) = aD_T(ta,(tab)a) \\ &= D_T(ta^2,(tab)a^2) = D_T(t,abt), \end{aligned}$$

which proves (a).

b - We only need to prove $\Leftarrow$. If $t \in D_T(a,b) \cap D_T(c,d)$ we have

$$D_T(a,b) = D_T(t,abt) \text{ and } D_T(t,cdt) = D_T(c,d).$$

Since $(ab)_T = (cd)_T$, we get $(abt)_T = (cdt)_T$ and so, by Lemma 4.2.21(c), $D_T(t,abt) = D_T(t,cdt)$, proving that $D_T(a,b) = D_T(c,d)$ and that $\langle a_T, b_T\rangle \equiv \langle c_T, d_T\rangle$.

□

We take as distinguished element $-1 \in G_T(F)$ the class of $-1 \in \dot{F}$, $(-1)_T$. We now prove

Theorem 4.2.23. *If T is a SG-subgroup of a field F of characteristic $\neq 2$, then $(G_T(F), \equiv, -1)$ is a special group, which is reduced iff T is closed under sums..*

Proof. We have to verify conditions [SG0]-[SG6] in definition 4.2.1. Both [SG0] and [SG1] are straightforward. The validity of [SG3] is required in the very definition of $\equiv$, while [SG5] follows from Lemma 4.2.21(b). It remains to verify that [SG2], [SG4] and [SG6]. Although is a consequence of [SG4], the former will be used in the proof of the latter.

SG2 - Note that if $a \in \dot{F}$, then there are $x, y \in F$ such that $a = x^2 - y^2$: just take $x = (1+a)/2$ and $y = (1-a)/2$. This shows that $a \in D_T(1,-1) \cap D_T(a,-a)$. Since the discriminant of $\langle a, -a\rangle$ is the same as that of $\langle 1, -1\rangle$ modulo T, 4.2.22(c) yields $\langle a, -a\rangle \equiv \langle 1, -1\rangle$.

SG4 - By hypothesis, we have $a_T b_T = c_T d_T$ and $D_T(a,b) = D_T(c,d)$. Since the discriminant equation implies $a_T(-c_T) = (-b_T)d_T$, it is sufficient to verify, by proposition 4.2.22(c), that $D_T(a,-c) \cap D_T(-b,d) \neq \emptyset$.

First observe that if $b_T = d_T$, then $a_T = c_T$, and [SG2] yields the desired conclusion. We assume, therefore, that $b_T \neq d_T$. Since $b \in D_T(c,d)$, there are $p, q \in T^*$ such that

$$b = cp + dq;$$

note that $p \neq 0$, otherwise, $b_T = d_T$. But then we may write

$$-c = d(q/p) - n(1/p),$$

and $-c \in D_T(-b,d)$. Since $-c$ is also in $D_T(a,-c)$, we have verified [SG4] and thus, that $(G_T(F), \equiv, -1)$ is a pre-special group.

SG6 - By condition (e) in theorem 4.2.16, it is enough to show that

$$\langle a_T, b_T, c_T\rangle \equiv \langle x_T, y_T, z_T\rangle \text{ implies } \langle a_T, b_T, c_T\rangle \equiv \langle y_T, x_T, z_T\rangle.$$

The antecedent of the above implication means that there are $\alpha, \beta, \gamma \in \dot{F}$ such that

$$\langle a_T, \alpha_T\rangle \equiv \langle x_T, \beta_T\rangle,\ \langle b_T, c_T\rangle \equiv \langle \alpha_T, \gamma_T\rangle \text{ and } \langle y_T, z_T\rangle \equiv \langle \beta_T, \gamma_T\rangle. \tag{4.23}$$

From the first isometry in 4.23 we get $a \in D_T(x,\beta)$, while the last one implies $\beta \in D_T(y,z)$. Thus, there are $p_a, q_a, p_\beta, q_\beta$ in T^* such that the equations below hold true:

$$a = xp_a + \beta q_a \tag{4.24}$$

$$\beta = yp_\beta + zq_\beta \tag{4.25}$$

Substituting equation 4.25 in 4.24, we arrive at

$$\begin{aligned} a &= xp_a + \beta q_a = xp_a + q_a(yp_\beta + zq_\beta) \\ &= xp_a + yp_\beta q_a + zq_\beta q_a = yp_\beta q_a + (xp_a + zq_\beta q_\alpha). \end{aligned}$$

Now define

$$v = xp_a + zq_\beta q_\alpha. \tag{4.26}$$

Then,

$$a = yp_\beta q_a + v. \tag{4.27}$$

We discuss two cases:

Case I: $v = 0$**.** Then, from 4.27, we have $a_T = y_T$. Consequently, the third isometry in 4.23 can be written as $\langle a_T, z_T\rangle \equiv \langle \beta_T, \gamma_T\rangle$. This isometry, the first one in 4.23 and SG4 yield

$$\langle x_T, -\alpha_T\rangle \equiv \langle a_T, -\beta_T\rangle \equiv \langle -z_T, \gamma_T\rangle,$$

and so, $\langle x_T, -\alpha_T\rangle \equiv \langle -z_T, \gamma_T\rangle$. Another application of SG4 yields $\langle x_T, z_T\rangle \equiv \langle \alpha_T, \gamma_T\rangle$, which

together with the second isometry in 4.23, gives $\langle x_T, z_T\rangle \equiv \langle b_T, c_T\rangle$. Then we have

$$\langle a_T, x_T\rangle \equiv \langle a_T, x_T\rangle,\ \langle b_T, c_T\rangle \equiv \langle x_T, z_T\rangle \text{ and } \langle x_T, z_T\rangle \equiv \langle x_T, z_T\rangle,$$

which shows that $\langle a_T, b_T, c_T\rangle \equiv \langle a_T, x_T, z_T\rangle$, as required.

Case II: $v \neq 0$**.** Equation 4.27 implies $a \in D_T(y, v)$, while 4.26 yields $v \in D_T(x, z)$. Therefore, proposition 4.2.22(a) gives

$$\langle a_T, (vay)_T\rangle \equiv \langle y_T, v_T\rangle \text{ and } \langle v_T, (vxz)_T\rangle \equiv \langle x_T, z_T\rangle.$$

These isometries imply that, to prove $\langle a_T, b_T, c_T\rangle \equiv \langle y_T, x_T, z_T\rangle$, it is enough to verify that $\langle (vay)_T, (vxz)_T\rangle \equiv \langle b_T, c_T\rangle$. Since the discriminant of these forms in $G_T(F)$ are the same, by proposition 4.2.22, they are isometric iff $D_T(vay, vxz) = D_T(b, c)$. From the isometries in 4.23 we get $\alpha_T = (ax\beta)_T$, $\gamma_T = (yz\beta)_T$ and $D_T(b, c) = D_T(\alpha, \gamma)$. By lemma 4.2.21(c) we conclude $D_T(b, c) = D_T(ax\beta, yz\beta)$.

Hence, what is need is equivalent to $D_T(ax\beta, yz\beta) = D_T(vay, vxz)$. Since the discriminants are the same, it is enough to prove $ax\beta \in D_T(vay, vxz)$. Multiplying this relation through by axv, we arrive at yet another equivalent condition, namely

$$v\beta \in D_T(xy, az),$$

which we shall now verify. Equations 4.25, 4.26 and 4.24 yield, with $t = zq_\beta$,

$$\begin{aligned} v\beta &= (xp_a + tq_a)(yp_\beta + t) = xyp_ap_\beta + txp_a + typ_\beta q_a + t^2q_a = \\ &= xyp_ap_\beta + t(xp_a + yp_\beta q_a + tq_q) = \\ &= xyp_ap_\beta + t(xp_a + q_a(yp_\beta + t)) = \\ &= xyp_ap_\beta + t(xp_a + \beta q_a) = \\ &= xyp_ap_\beta + ta = xyp_ap_\beta + azq_\beta, \end{aligned}$$

showing that $v\beta \in D_T(xy, az)$ and concluding the verification of SG6.

Regarding reduction, note that $\langle a_T, a_T\rangle \equiv \langle 1, 1\rangle$ iff a is a sum of elements of T; □

In recent book of Dickmann and Miraglia [DM15], they extend the classical algebraic theory of quadratic forms over fields to a broad class of commutative rings with unit (of course, which was mediated by the theory of special groups). The context is of a ring A of characteristic not 2, with $-1 \notin \sum A^2$ and $2 \in \dot{A}$.

Given a such ring A and a preordering T on A[4], they define that two n-dimensional forms $\varphi = a_1X_1^2 + ... + a_nX_n^2$, $\psi = b_1X_1^2 + ... + b_nX_n^2$ with $a_i, b_i \in \dot{A}$ are T-isometric, $\varphi \approx_T \varphi$ if there is a sequence $\varphi_0, \varphi_1, ..., \varphi_k$ of n-dimensional diagonal forms over $\dot{A}$, such that $\varphi = \varphi_0$, $\psi = \varphi_k$ and for every $1 \leq i \leq k$, φ_i is either isometric to φ_{i-1} in the usual sense that there is a matrix $M \in \mathrm{GL}_n(A)$ such that $\varphi_i = M\varphi_{i-1}M^t$ or there are $t_1, ..., t_n \in \dot{T}$ such that $\varphi_i = \langle t_1x_1, ..., t_nx_n\rangle$ and $\varphi_{i-1} = \langle x_1, ..., x_n\rangle$. Value representation relation D_T on (A, T) is given by: for $a, b_1, ..., b_n \in \dot{A}$,

$$a \in D_T^v(b_1, ..., b_n) \Leftrightarrow \exists\, t_1, ..., t_n \in T \text{ such that } a = \sum_{i=1}^{n} t_ib_i.$$

[4]We will see later that A is preordered if and only if $-1 \notin \sum A^2$.

Given a preordered ring (A,T), they associate a structure $G_T(A)$, whose domain is $\dot{A}/\dot{T}$, endowed with the product operation induced by $\dot{A}$, togheter with a binary isometry relation $\equiv_{G_T(A)}$, defined on ordered pairs of elements of $\dot{A}/\dot{T}$, and having $-1 = -1/\dot{T}$ as distinguished element. The structure $(G_T(A), \equiv_{G_T(A)}, -1)$ is not quite a special group, but satisfy SG0, SG1, SG2, SG3 and SG5. They observed that the ring-theoretic approach, based on the definition of n-isometry and the formal approach via $G_T(A)$, though related, are far from identical.

Beside this, they called **T-faithfully quadratic** any preordered ring (A,T) such that $G_T(A)$ is a special group and T-isometry and value representation in (A,T) are faithfully coded by the corresponding formal notions in $G_T(A)$. After this brilliant idea, they was able to replicate most of the consequences of the theory of special groups in field theory in this extended ring-theoretic context.

4.2.4 Pfister Forms and Saturated Subgroups

Definition 4.2.24. *Let G be a special group. A Pfister form over G is a quadratic form φ of the type $\otimes_{i=1}^{n}\langle 1, a\rangle_i$, where $n \geq 1$ and $a_1, ..., a_n \in G$, or the form $\langle 1\rangle$. In the first case, the integer n is called the degree of φ and written $\deg(\varphi)$; alson $\deg(\langle 1\rangle) = 0$. If the coefficients of φ happen to belong to a subgroup Δ of G, we say that φ is Pfister over Δ.*

Since a Pfister form φ contains 1 as a coefficient, we may write φ as $\langle 1\rangle \oplus \varphi'$; φ' is called *pure subform* of φ.

Proposition 4.2.25 (Basic properties of Pfister forms)**.** *Let G be a special group, $\varphi = \langle\langle a_1, ..., a_n\rangle\rangle$ a Pfister form over G of degree $n \geq 1$ and $b \in G$. Recall that φ' is the pure sub-form of φ. Then:*

i - $b \in D_G(1, a_1) \Rightarrow \langle\langle a_1, a_2\rangle\rangle \equiv_G \langle\langle a_1, a_2 b\rangle\rangle$.

ii - $b \in D_G(a_1, a_2) \Rightarrow \langle\langle a_1, a_2\rangle\rangle \equiv_G \langle\langle b, a_1 a_2\rangle\rangle$.

iii - $\langle\langle a_1 b, ..., a_n b\rangle\rangle \equiv_G \langle\langle 1, a_1 b\rangle\rangle \otimes \langle\langle a_1 a_2, ..., a_1 a_n\rangle\rangle$.

iv - *If $b \in D_G(\varphi')$, then $\varphi \equiv_G \langle\langle b, b_2, ..., b_n\rangle\rangle$, with $b_2, ..., b_n \in G$.*

v - *An isotropic Pfister form is hyperbolic.*

vi - $D_G(\varphi) = \{x \in G : x\varphi \equiv_G \varphi\}$. *Hence $D_G(\varphi)$ is a subgroup of G. If ψ is a Pfister form over G, then $D_G(\varphi)D_G(\psi) \subseteq D_G(\varphi \otimes \psi)$.*

vii - *If $a \in D_G(\varphi)$, then $\langle\langle a_1, ..., a_n, b\rangle\rangle \equiv_G \langle\langle a_1, ..., a_n, ab\rangle\rangle$.*

viii - $a \in D_G(\varphi) \Rightarrow \langle 1, a\rangle \otimes \varphi \equiv_G 2 \otimes \varphi$ *and* $\langle 1, -a\rangle \otimes \varphi$ *is hyperbolic.*

ix - $a \in D_G(\varphi)$ *and* $b \in D_G(1, a) \Rightarrow b \in D_G(2 \otimes \varphi)$.

x - $\langle 1, a\rangle \otimes \varphi \equiv_G 2 \otimes \varphi \Rightarrow a \in D_G(\varphi)$.

xi - $\langle 1, -a\rangle \otimes \varphi$ *hyperbolic* $\Rightarrow a \in D_G(\varphi)$.

xii - *The following are equivalent:*

a - *G is a reduced special group.*

b - $1 \neq -1$ *and for every Pfister form φ over G of degree ≥ 1 and $a \in G$:*

$$a, -a \in D_G(\varphi) \Rightarrow \varphi \text{ hyperbolic.}$$

c - $1 \neq -1$ *and for every Pfister form* φ *over* G *and* $a \in G$

$$a \in D_G(\langle 1, -a\rangle \otimes \varphi) \Rightarrow a \in D_G(\varphi).$$

Proof.

i - If $b \in D_G(1, a_1)$, then $\langle b, x\rangle \equiv \langle 1, a_1\rangle$, so $x = a_1 b$ (by SG3). By SG5, $\langle a_2, a_1a_2\rangle \equiv \langle a_2, a_1a_2b_2\rangle$. Now, using preservation of isometry by sum we get

$$\begin{aligned}\langle\langle a_1, a_2\rangle\rangle = \langle 1, a_1, a_2, a_1a_2\rangle = \langle 1, a_1\rangle \oplus \langle a_2, a_1a_2\rangle \equiv \\ \langle 1, a_1\rangle \oplus \langle a_2, a_1a_2b\rangle = \langle 1, a_1, a_2, a_2b\rangle = \langle\langle a_1, a_2b\rangle\rangle.\end{aligned}$$

ii - From $b \in D_G(a_1, a_2)$ we get $\langle b, a_1a_2b\rangle \equiv \langle a_1, a_2\rangle$. Now, using preservation of isometry by sum we get

$$\begin{aligned}\langle\langle a_1, a_2\rangle\rangle = \langle 1, a_1, a_2, a_1a_2\rangle = \langle 1, a_1a_2\rangle \oplus \langle a_1, a_1a_2\rangle \equiv \\ \langle 1, a_1a_2\rangle \oplus \langle b, a_1a_2b\rangle = \langle 1, b, a_1a_2, a_1a_2b\rangle = \langle\langle b, a_1a_2\rangle\rangle.\end{aligned}$$

iii - We proceed by induction on n. If $n = 1$ there is nothing to do. Suppose that holds for $n-1$ and let $\varphi = \langle\langle a_1b, ..., a_nb\rangle\rangle$.

$$\begin{aligned}\varphi = \langle\langle a_1b, ..., a_nb\rangle\rangle &= \langle 1, a_nb\rangle \otimes \langle\langle a_1b, ..., a_{n-1}b\rangle\rangle \\ &\overset{\text{IS}}{=} \langle 1, a_nb\rangle \otimes \langle 1, a_1b\rangle \otimes \langle\langle a_1a_2, ..., a_1a_{n-1}\rangle\rangle \\ &= \langle 1, a_nb, a_1b, a_1a_n\rangle \otimes \langle\langle a_1a_2, ..., a_1a_{n-1}\rangle\rangle \\ &= \langle 1, a_1b, a_1a_n, a_nb\rangle \otimes \langle\langle a_1a_2, ..., a_1a_{n-1}\rangle\rangle \\ &= \langle 1, a_1b\rangle \otimes \langle 1, a_1a_n\rangle \otimes \langle\langle a_1a_2, ..., a_1a_{n-1}\rangle\rangle \\ &= \langle 1, a_1b\rangle \otimes \langle\langle a_1a_2, ..., a_1a_n\rangle\rangle.\end{aligned}$$

iv - Proceed by induction on the degree n of φ. If $n = 1$, there is nothing to prove. Assume that $\varphi = \langle 1, a\rangle \otimes \psi$, where ψ is a Pfister form of degree n. Since $\varphi' = \psi' \otimes a\psi$, the hypothesis $b \in D_G(\varphi')$ and 4.2.4(c) yield $x \in D_G(\psi')$ and $y \in D_G(\psi)$, such that

$$b \in D_G(x, ay), \text{ that is, } \langle b, baxy\rangle \equiv \langle x, ay\rangle. \tag{I}$$

By the induction hypothesis, there are $z_2, ..., z_n \in G$, such that,

$$\psi \equiv \langle\langle x, z_2, ..., z_n\rangle\rangle. \tag{II}$$

Then, (II),(I) and $y\psi \equiv \psi$, yield, with $\alpha \equiv \langle\langle z_2, ..., z_n\rangle\rangle$,

$$\begin{aligned}\langle 1, b\rangle \otimes \langle 1, axy\rangle \otimes \alpha &= \langle 1, b, axy, abxy\rangle \otimes \alpha \\ &= (\langle 1, axy\rangle \oplus \langle b, abxy\rangle) \otimes \alpha \\ &= (\langle 1, axy\rangle \oplus \langle x, ay\rangle) \otimes \alpha \\ &\equiv (\langle 1, x\rangle \oplus ay\langle 1, x\rangle) \otimes \alpha \\ &= (\langle 1, x\rangle \otimes \alpha) \oplus ay(\langle 1, x\rangle \otimes \alpha) \\ &= \psi \oplus ay\psi = \psi \oplus a\psi = \varphi,\end{aligned}$$

completing the induction step.

v - Since $\varphi \cong \langle 1, -1\rangle \oplus \psi$, we have $-1 \in D_G(\varphi')$ by Witt's cancellation. By item (iv) $\varphi \cong \langle\langle -1, b_2, ..., b_n\rangle\rangle$, which is hyperbolic.

vi - Denote $G_\varphi = \{x \in G : x\varphi \equiv_G \varphi\}$. Since φ represents 1, we have that $G_\varphi \subseteq D_G(\varphi)$. To prove that $g \in D_G(\varphi) \Rightarrow \langle g\rangle\varphi \cong \varphi$, we appeal to some argument on the Witt ring. The Pfister form $\varphi\langle\langle -g\rangle\rangle \cong \varphi \perp \langle -g\rangle\varphi$ (of one higher fold) contains a subform $\langle g, -g\rangle \cong \langle 1, -1\rangle$, so by item (v) $\varphi\langle\langle -g\rangle\rangle$ is hyperbolic. Hence $\varphi\langle\langle -g\rangle\rangle = 0 \in W(G)$ and since $\dim(\langle g\rangle\varphi) = \dim(\varphi)$, it follows that $\langle g\rangle\varphi = \varphi \in W(G)$, then $\langle g\rangle\varphi \cong \varphi$.

vii - Proceed by induction on the degree n of φ. If $n = 1$, this is just item (i). Now, suppose the assertion true for $n-1$, and let $a \in D_G(\varphi)$ (remember: $\varphi = \langle\langle a_1, ..., a_n\rangle\rangle$). Then

$$\begin{aligned}\langle\langle a_1, ..., a_n, b\rangle\rangle &= \langle\langle a_1\rangle\rangle \otimes \langle\langle a_2, ..., a_n, b\rangle\rangle \\ &\overset{\text{IS}}{\equiv} \langle\langle a_1\rangle\rangle \otimes \langle\langle a_2, ..., a_n, ab\rangle\rangle = \langle\langle a_1, a_2, ..., a_n, ab\rangle\rangle.\end{aligned}$$

viii - Using the previous item, we have

$$\begin{aligned}2 \otimes \langle\langle a_1, ..., a_n\rangle\rangle &= \langle 1, 1\rangle \otimes \langle\langle a_1, ..., a_n\rangle\rangle = \langle\langle a_1, ..., a_n, 1\rangle\rangle \\ &\cong \langle\langle a_1, ..., a_n, a\rangle\rangle = \langle 1, a\rangle \otimes \langle\langle a_1, ..., a_n\rangle\rangle.\end{aligned}$$

Using SG4 on this isometry we obtain $\langle 1, -a\rangle \otimes \varphi$ hyperbolicity.

ix - Since φ is a Pfister form, $\langle 1, a\rangle \otimes \varphi = \langle 1, a\rangle \oplus \psi$. Now, is just use the previous item and 4.2.4(c).

x - Just an application of Witt's Cancellation to the fact that $2 \otimes \varphi = \langle 1, 1, 1\rangle \oplus \psi$.

xi - Use the fact that $\langle 1, -a\rangle \otimes \varphi$ hyperbolic implies $\langle -a\rangle \oplus \varphi$ hyperbolic and 4.2.4(d).

xii - (a)⇒(b): by item (viii), both $\langle 1, -a\rangle \otimes \varphi$ and $\langle 1, a\rangle \otimes \varphi$ are hyperbolic, so, by adding these forms we obtain $\langle 1, 1\rangle \oplus \varphi \oplus \varphi$ hyperbolic, and in particular, $\varphi \oplus \varphi$ is hyperbolic (and isotropic). Since G is reduced, by lemma 4.2.5 φ is isotropic, and by item (v), φ is hyperbolic.

(b)⇒(a): from $\langle a, a\rangle \equiv \langle 1, 1\rangle$ we obtain $\langle a, -1\rangle \equiv \langle 1, -a\rangle$ by SG4. Then $a, -a \in D_G(\langle\langle -a\rangle\rangle)$, and by item (b), $\langle\langle -a\rangle\rangle$ is hyperbolic. Thus $\langle 1, -a\rangle \equiv \langle 1, -1\rangle$, so $a = 1$, by SG3.

(b)⇒(c): In this case, $a, -a \in D_G(\langle 1, -a\rangle \otimes \varphi)$. By (b), $\langle 1, -a\rangle \otimes \varphi$ is hyperbolic and by (xi), $a \in D_G(\varphi)$.

(c)⇒(a): We proof by induction. If $b, -b \in \langle\langle x\rangle\rangle = \langle 1, x\rangle$, we have

$$\langle b, bx\rangle \equiv \langle 1, x\rangle \equiv \langle -b, -bx\rangle \Rightarrow \langle b, bx\rangle \equiv \langle -b, -bx\rangle \overset{SG5}{\Rightarrow} \langle 1, x\rangle \equiv \langle -1, -x\rangle.$$

Then $-x \in D(\langle 1, x\rangle \otimes \langle 1\langle)$, so by (c), $-x \in D(\langle 1\rangle)$ and $-x = 1$.

Now, suppose that holds for $n-1$ and let $\varphi = \langle\langle a_1, ..., a_n\rangle\rangle$. Let $\psi = \langle\langle a_1, ..., a_{n-1}\rangle\rangle$. If $b, -b \in D(\varphi)$, then by item (vi), $b\varphi \equiv \varphi \equiv -b\varphi$. Hence $\psi \otimes \langle 1, a_n\rangle \equiv -\psi \otimes \langle 1, -a\rangle$, so $-a_n \in D(\langle 1, a_n\rangle \otimes \psi)$. By induction step, $-a_n \in D(\psi)$ and by item (viii), $\varphi = \langle 1, -(-a_n)\rangle \otimes \psi$ is hyperbolic, finalizing the proof.

□

Definition 4.2.26. *Let G be a special group and let $\Delta \subseteq G$ be a subgroup. We say that Δ is saturated if for all $a \in G$,*

$$a \in \Delta \Rightarrow D_G(1, a) \subseteq \Delta. \tag{sat}$$

Note that if, in addition, $-1 \in \Delta$, then $\Delta = G$. Thus we will reserve the noun saturated for those subgroups satisfying [sat] such that $-1 \notin \Delta$, while G will be called the improper saturated subgroup of itself.

Lemma 4.2.27. *Let G be a special group and Δ a subgroup of G.*

a - The intersection of any family of saturated subgroups is saturated. The union of an upward directed family of saturated subgroup is saturated.

b - The following are equivalent:

i - Δ is saturated.

ii - For any Pfister forms φ, ψ over Δ and any $b, c \in \Delta$

$$D_G(\varphi), D_G(\psi) \subseteq \Delta \Rightarrow D_G(b\varphi \oplus c\psi) \subseteq \Delta.$$

iii - For any Pfister form φ over Δ, $D_G(\varphi) \subseteq \Delta$.

Proof.

a - Is an immediate consequence of the definition of saturatedness.

b - (i)⇒(ii): If $a \in D_g(b\varphi \oplus c\psi)$, there are $x \in D_G(\varphi)$ and $y \in D_G(\psi)$ such that $a \in D_G(bx, cy)$, which implies $abx \in D_G(1, bcxy)$. Since $D_G(\varphi)$ and $D_G(\psi)$ are contained in Δ, we have $x, y \in \Delta$; hence $bcxy \in \Delta$ and, by (i), $abx \in \Delta$. Since $bx \in \Delta$, we get $a \in \Delta$.

(ii)⇒(iii): By induction on the $\deg(\varphi) = n$. The case $n = 0$ is immediate. For the induction step, φ can be written

$$\varphi = \langle 1, a\rangle \otimes \psi \equiv_G \psi \oplus a\psi,$$

with $a \in \Delta$ and ψ a Pfister form over Δ of degree $n-1$. Hence, $D_G(\psi) \subseteq \Delta$ and the conclusion follows from (ii) for the values $b = 1$ and $c = a$.

(iii)⇒(i): Just use $\varphi = \langle 1, a\rangle = \langle\langle a\rangle\rangle$.

□

In the sequel it will be shown that saturated subgroups exist in profusion:

Lemma 4.2.28. *Let G be a special group and let Δ be a subgroup of G.*

a - The family $\mathcal{P}_\Delta$ of all Pfister forms over Δ contains the form $2 = \langle 1, 1\rangle$ and is closed under tensor products.

b - The following are equivalent:

i - Δ is a proper saturated subgroup of G.

ii - There is a family S of anisotropic Pfister forms over G containing 2, closed under tensor products and such that $\Delta = \bigcup\{D_G(\varphi) : \varphi \in S\}$.

Proof.

a - It is just the fact that $1 \in \Delta$ and the definition of Pfister forms.

b - (i)⇒(ii): If Δ is saturated, consider $\mathcal{S} = \mathcal{P}_\Delta$. Lemma 4.2.27(c) implies that

$$\Delta = \bigcup \{D_G(\varphi) : \varphi \in \mathcal{S}\}.$$

If some $\varphi \in \mathcal{S}$ is isotropic, then $-1 \in D_G(\varphi) \subseteq \Delta$, and so $\Delta = G$.

(ii)⇒(i): Suppose that $\mathcal{S}$ is as in (ii), and $\Delta = \bigcup \{D_G(\varphi) : \varphi \in S\}$. Let $a \in \Delta$ and $b \in D_G(1, a)$. Thus, $a \in D_G(\varphi)$ for some $\varphi \in \mathcal{S}$ and by 4.2.25(ix), we have $b \in D_G(2 \otimes \varphi)$. Since this form is in $\mathcal{S}$, we conclude that $b \in \Delta$. If $-1 \in D_G(\varphi)$ for some $\varphi \in \mathcal{S}$, then by 4.2.25(vi), $-\varphi \equiv_G \varphi$. But this means that $\varphi \oplus \varphi \equiv_G 2 \otimes \varphi$ is an isotropic form in $\mathcal{S}$.

□

Lemma 4.2.28 yields at once

Proposition 4.2.29. *Let G be a special group and let Δ be a subgroup of G. Then*

$$\overline{\Delta} = \bigcup \{D_G(\varphi) : \varphi \in \mathcal{P}_\Delta\} \qquad \text{(saturation)}$$

is the smallest saturated subgroup of G containing Δ. In particular, if Δ is saturated and φ is a Pfister form over Δ, then $D_G(\varphi) \subseteq \Delta$.

Proof. Items (a) and (b) of Lemma 4.2.28 show that $\overline{\Delta}$ is saturated (possibly improper). Since $\langle 1, a\rangle$ is in $\mathcal{P}_\Delta$, forall $a \in \Delta$, we have $\Delta \subseteq \overline{\Delta}$. If Γ is a saturated subgroup containing Δ and $\varphi \in \mathcal{P}_\Delta$, then φ is Pfister over Γ and item (iii) in 4.2.27(b) shows that $D_G(\varphi) \subseteq \Gamma$. Hence, $\overline{\Delta} \subseteq \Gamma$. □

Definition 4.2.30. *We call $\overline{\Delta}$ the saturation of Δ. If $\Delta = \{1\}$, we write $\overline{\{1\}} = Sat(G)$.*

Remark 4.2.31.

i - *$\overline{\Delta}$ may be improper even if -1 is not in Δ.*

ii - *$Sat(G)$ is the smallest saturated subgroup of G and*

$$Sat(G) = \bigcup \{D_G(\prod_{i=1}^{n} \langle 1, 1\rangle) : n \in \omega\} \bigcup \{D_G(2^k\langle 1\rangle) : k \in \omega\}.$$

iii - *$Sat(G) = \{1\}$ if and only if G is reduced.*

In case G is a **reduced** special group, there are further examples of saturated subgroups.

Lemma 4.2.32. *Let G be a special group.*

a - *$X_G \neq 0$ if and only if $Sat(G) \neq G$ if and only if $-1 \notin Sat(G)$.*

b - *If $\sigma \in X_G$, then $Sat(G) \subseteq Ker(\sigma)$. Thus σ factors through π to give a character $\hat{\sigma} \in X_{G/Sat(G)}$ satisfying $\hat{\sigma} \circ \pi = \sigma$, where $\pi : G \to G/Sat(G)$ is the canonical quotient map.*

c - *The map $X_{G/Sat(G)} \mapsto X_G$ given by $\tau \mapsto \tau \circ \pi$, is a homeomorphism.*

Proof.

a - By SG2 we have $D_G(1,-1) = G$. So $(\mathrm{Sat}(G) \neq G) \Leftrightarrow (-1 \notin \mathrm{Sat}(G))$ follow this. Now, suppose $X_G \neq \emptyset$ and let $\sigma \in X_G$. If $-1 \in \mathrm{Sat}(G)$, say $-1 \in D_G(\langle\langle 1, ..., 1\rangle\rangle)$ we have

$$\sigma(-1) \in D_{\mathbb{Z}_2}(\langle\langle \sigma(1), ..., \sigma(1)\rangle\rangle) \Rightarrow -1 \in D_{\mathbb{Z}_2}(\langle\langle 1, ..., 1\rangle\rangle),$$

contradiction. Finally, suppose $-1 \notin \mathrm{Sat}(G)$. Define $\sigma : G \to \mathbb{Z}_2$ by the rule

$$\sigma(g) = \begin{cases} 1 \text{ if } g \in \mathrm{Sat}(G); \\ -1 \text{ otherwise.} \end{cases}$$

We have that σ is a SG-morphism, finalizing the proof.

b - $\mathrm{Sat}(G) \subseteq \mathrm{Ker}(\sigma)$ follow by the very definition of $\mathrm{Sat}(G)$, X_G and SG-morphisms. The rest is just an application of the homomorphism theorem for groups.

c - Another application of homomorphism theorem.

□

Definition 4.2.33. *Any special group verifying the equivalent conditions in 4.2.32(a) will be called formally real.*

It is immediate that a field F is formally real iff the group $G(F)$ is formally real.

Lemma 4.2.34. *Let G be a reduced special group. Then:*

a - For any Pfister form φ on G, $D_G(\varphi)$ is a saturated subgroup of G. In fact, if $\varphi = \langle\langle a_1, ..., a_n\rangle\rangle$ then

$$D_G(\varphi) = \overline{D_G(1, a_1)D_G(1, a_2)...D_G(1, a_n)}.$$

b - For any form ψ on G, the set $\{a \in G : a\psi \equiv_G \psi\}$ is a saturated subgroup of G.

Proof.

a - Proposition 4.2.25(ix) shows that $a \in D_G(\varphi)$ and $b \in D_G(1, a)$ imply $b \in D_G(2 \otimes \varphi)$. Now use 4.2.5(b) to conclude that $b \in D_G(\varphi)$.

If Γ is a saturation subgroup of G containing $D_G(1, a_i)$, $1 \leq i \leq n$, then it follows from 4.2.29 that Γ contains $D_G(\varphi)$, since φ is a Pfister form over Γ. Hence, $D_G(\varphi)$ is in fact the saturation of the product of the $D_G(1, a_i)$.

b - If $a, b \in G$, then $a(b\psi) \equiv a\psi \equiv \psi$, so G is a subgroup. Assume that $a \in D_G(1, b)$, where $a\psi \equiv_G \psi$. Then, $\langle a, ab\rangle \equiv \langle 1, b\rangle$; tensoring both sides of this isometry with ψ yields $a\psi \oplus ab\psi \equiv_G \psi \oplus b\psi$, and hence $a\psi \oplus a\psi \equiv \psi \oplus \psi$. Now 4.2.5(d) gives $a\psi \equiv \psi$, as required.

□

Now we will prove two important properties of maximal saturated subgroups. The next lemma will be used in both proofs.

If S is a subset of a group G, let $[S]$ denote the subgroup generated by S in G.

Lemma 4.2.35. *Let G be a special group, Δ a saturated subgroup of G and $x \in G$. Then,*

$$\overline{[\Delta \cup \{x\}]} = G \text{ iff } -x \in \Delta.$$

Proof. If $-x \in \Delta$, then the subgroup generated by Δ and x will have -1, and so its saturation is G.

Now assume that the saturation Γ of $[\Delta \cup \{x\}] = \Delta \cup x\Delta$ is equal to G. Thus, $-x \in \Gamma$, and by the definition of saturation (proposition 4.2.29) there is a Pfister form φ over $\Delta \cup \{x\}$ such that $-x \in D_G(\varphi)$. We may write φ in the form

$$\varphi = \langle\langle a_1, ..., a_n, b_1x, ..., b_mx\rangle\rangle, \tag{*}$$

with $a_1, ..., a_n, b_1, ..., b_m \in \Delta$. By proposition 4.2.25(iii)

$$\langle\langle b_1x, ..., b_mx\rangle\rangle \equiv \langle\langle b_1b_2, ..., b_1b_m\rangle\rangle \otimes \langle 1, b_1x\rangle.$$

Substituting this isometry in (*) we get

$$\varphi \equiv_G \psi \otimes \langle 1, b_1x\rangle \equiv_G \psi \oplus b_1x\psi, \tag{**}$$

where $\psi = \langle\langle a_1, ..., a_n, b_1b_2, ..., b_1b_m\rangle\rangle$, a Pfister form over Δ. Since $-x \in D_G(\varphi)$, (**) implies the existence of $y, z \in D_G(\psi)$ such that $-x \in D_G(y, b_1xz)$, i.e,

$$\langle -x, -b_1yz\rangle \equiv_G \langle y, b_1xz\rangle.$$

It follows that

$$\langle -y, -b_1yz\rangle \equiv_G \langle x, b_1xz\rangle,$$

and hence $-xy \in D_G(1, b_1z)$. Since Δ is saturated, Lemma 4.2.27(b) yields $y, z \in \Delta$ and so $b_1z \in \Delta$. By saturatedness again, we get $-xy \in \Delta$ and hence $-x = (-xy)y \in \Delta$. □

Proposition 4.2.36. *Let Δ be a saturated subgroup of a special group G. Then, Δ is a maximal saturated subgroup iff for all $x \in G$, $x \in \Delta$ or (exclusive) $-x \in \Delta$.*

Proof. If $x \notin \Delta$ and Δ is maximal, the saturation of the subgroup generated by Δ and x must be G. By lemma 4.2.35, we conclude $-x \in \Delta$.

Conversely, suppose Δ is saturated and such that either x or $-x$ is in Δ, for all $x \in G$. Then any proper saturated extension Γ of Δ will contain z and $-z$, for some $z \in G$, which from $\Gamma = G$, by proposition 4.2.29. Thus, Δ is a maximal saturated subgroup of G. □

Theorem 4.2.37 (Separation Theorem)**.** *Let G be a special group, Δ a saturated subgroup of G and a an element of G such that $a \notin \Delta$. Then there is a maximal saturated subgroup Γ of G such that $\Delta \subseteq \Gamma$ and $a \notin \Gamma$.*

Proof. Let $\Sigma = \overline{[\Delta \cup \{-a\}]}$; Lemma 4.2.35 implies that Σ is a proper subgroup of G, otherwise a would be in Δ. In particular, $a \notin \Sigma$. Now, consider

$$\mathcal{V} = \{\Lambda : \Lambda \text{ is a proper saturated subgroup of } G,\ \Sigma \subseteq \Lambda \text{ and } a \notin \Lambda\},$$

ordered by inclusion. $\Sigma \in \mathcal{V}$, and since an upward directed family of saturated subgroups is again saturated (Lemma 4.2.27(a)), Zorn's Lemma furnishes a maximal element Γ in $\mathcal{V}$. To see that Γ is indeed a maximal saturated subgroup of G, let Θ be a saturated subgroup of G properly containing Γ. Then Θ is not in $\mathcal{V}$ and so $a \in \Theta$. Since Θ contains Σ, we have both a and $-a$ in Θ, which implies that $\Theta = G$. □

Corollary 4.2.38. *A special group G is formally real if and only if admits a maximal saturated subgroup.*

4.2.5 Quotients

Definition 4.2.39. *Let Δ be a subgroup of a special group $(G, \equiv_G, -1)$. We define a quaternary relation on the quotient group G/Δ as follows:*

$$\langle a/\Delta, b/\Delta\rangle \equiv^*_G \langle c/\Delta, b/\Delta\rangle \text{ iff } \begin{cases} \exists\, a', b', c', d' \in G \text{ such that} \\ aa', bb', cc', dd' \in \Delta \text{ and} \\ \langle a', b'\rangle \equiv_G \langle c', d'\rangle. \end{cases}$$

Remark that no conditions are imposed on Δ.

Proposition 4.2.40. *With notation as in definition 4.2.39, we have*

a - The relation $\equiv^*_{G/\Delta}$ is well defined.

b - $(G/\Delta, \equiv^*_{G/\Delta}, -1/\Delta)$ verifies the axioms [SG1]-[SG5] of special groups. The relation $\equiv^*_{G/\Delta}$ (on $G/\Delta \times G/\Delta$) is reflexive and symmetric, but not transitive in general. The canonical quotient map $\pi : G \to G/\Delta$ satisfies, $\forall\, a, b, c, d \in G$

$$\langle a, b\rangle \equiv_G \langle c, d\rangle \Rightarrow \langle \pi(a), \pi(b)\rangle \equiv^*_{G/\Delta} \langle \pi(c), \pi(d)\rangle. \qquad \text{(quo)}$$

c - $\equiv^*_{G/\Delta}$ is the smallest binary relation $\equiv$ on $G/\Delta \times G/\Delta$ satisfying contidion (quo) for all $a, b, c, d \in G$.

Definition 4.2.41. *Let G be a special group. A collection $\mathcal{S}$ of Pfister forms is said to be (upward) directed if for every $\varphi, \psi \in \mathcal{S}$, There is $\theta \in \mathcal{S}$ such that $D_G(\varphi), D_G(\psi) \subseteq D_G(\theta)$.*

*A subgroup Δ of G is a **Pfister subgroup** iff there is a directed family $\mathcal{S}$ of Pfister forms over G such that $\Delta = \bigcup\{D_G(\varphi) : \varphi \in \mathcal{S}\}$.*

Lemma 4.2.28(b) proves that any saturated subgroup is Pfister, since a family of Pfister forms closed under tensor products is directed (proposition 4.2.25(vi)). Note that the subgroups $D_G(\varphi)$, φ a Pfister form, are Pfister ($\mathcal{S} = \{\varphi\}$ is directed).

The class of Pfister and saturated subgroups are not identical, except in the case of reduced special groups – and only in that case – as shown by the following:

Proposition 4.2.42. *Let G be a special group such that $1 \neq -1$. Then G is reduced iff every Pfister subgroup of G is saturated.*

Proof. Suppose G is reduced and Δ is a Pfister subgroup, say $\Delta = \bigcup\{D_G(\varphi) : \varphi \in \mathcal{S}\}$, $\mathcal{S}$ a directed family of Pfister forms. By corollary 4.2.34, $D_G(\varphi)$ is saturated, for each $\varphi \in \mathcal{S}$. Thus, Δ is the directed union of saturated subgroups, and so itself saturated. The converse follows from item (iii) of the remarks after definition 4.2.30: since $\langle 1\rangle$ is a Pfister form such that $\{1\} = D_G(\langle 1\rangle)$, $\{1\}$ is saturated. But this is equivalent to G being reduced. □

Proposition 4.2.43. *Let G be a special group and Δ a Pfister subgroup of G, $\Delta = \bigcup\{D_G(\varphi) : \varphi \in \mathcal{S}\}$, $\mathcal{S}$ a directed family of Pfister forms. For $a, b, c, d \in G$, the following are equivalent:*

a - $\langle a/\Delta, b/\Delta\rangle \equiv^*_{G/\Delta} \langle c/\Delta, d/\Delta\rangle$.

b - There is a $\varphi \in \mathcal{S}$ such that $\langle a, b\rangle \oplus \varphi \equiv_G \langle c, d\rangle \oplus \varphi$.

Before proving this result we will deal with the particular case where $\mathcal{S}$ consists of a single form.

Lemma 4.2.44. *Let G be a special group and φ a Pfisfer form over G.*

a - For $a, b, c, d \in G$, the following are equivalent:

i - $\langle a, b\rangle \otimes \varphi \equiv_G \langle c, d\rangle \otimes \varphi$.

ii - There are $a', b', c', d' \in G$ such that $aa', bb', cc', dd' \in D_G(\varphi)$ and $\langle a', b'\rangle \equiv_G \langle c', d'\rangle$.

b - Conditions (i) or (ii) imply $abcd \in D_G(\varphi)$.

Proof.

a - (i)⇒(ii): By assumption, $a\varphi \oplus b\varphi \equiv_G c\varphi \oplus d\varphi$; in particular, $a \in D_G(c\varphi \oplus d\varphi)$. By proposition 4.2.4, there are $x, y \in D_G(\varphi)$ such that $a \in D_G(cx, dy)$, i.e

$$\langle a, acdxy\rangle \equiv_G \langle cx, dy\rangle. \qquad (*)$$

Setting $a' = a$, $b' = acdxy$, $c' = cx$ and $d' = dy$ we have $\langle a', b'\rangle \equiv_G \langle c', d'\rangle$. Further, $aa' = 1$, $cc' = x$ and $dd' = y$ are in $D_G(\varphi)$. Tensoring (*) with φ gives

$$a\varphi \oplus b'\varphi \equiv_G cx\varphi \oplus dy\varphi \equiv_G c\varphi \oplus d\varphi \equiv_G a\varphi \oplus b\varphi.$$

Cancelling $a\varphi$ on both sides (4.2.4) yields $b\varphi \equiv_G b'\varphi$, that is, $bb' \in D_G(\varphi)$.

(ii)⇒(i): Assume $\langle a', b'\rangle \equiv_G \langle c', d'\rangle$ with $aa', bb', cc', dd' \in D_G(\varphi)$. Then

(a) $a'\varphi \oplus b'\varphi = langlea', b'\rangle \otimes \varphi \equiv_G \langle c', d'\rangle \otimes \varphi = c'\varphi \oplus d'\varphi$.

(b) $a'\varphi \equiv a\varphi$, $b'\varphi \equiv b\varphi$, $c'\varphi \equiv c\varphi$, $d'\varphi \equiv d\varphi$.

Substituting the isometries in (2) for the corresponding terms in (1), we get

$$a\varphi \oplus b\varphi \equiv c\varphi \oplus d\varphi$$

i.e, $\langle a, b\rangle \otimes \varphi \equiv_G \langle c, d\rangle \otimes \varphi$ as required.

b - Using (ii) we obtain $a'b'c'd' = 1$. Since $aa', bb', cc', dd' \in D_G(\varphi)$, which is a subgroup, we conclude that $abcda'b'c'd' = abcd \in D_G(\varphi)$.

□

Proof of proposition 4.2.43. (a)⇒(b): by assumption (a) there are elements $a', b', c', d' \in G$ such that $aa', bb', cc', dd' \in \Delta$ and $\langle a', b'\rangle \equiv_G \langle c', d'\rangle$. Since Δ is Pfister, there are forms $\varphi_1, ..., \varphi_4$ in $\mathcal{S}$ such that $aa' \in D_G(\varphi_1)$, $bb' \in D_G(\varphi_2)$, $cc' \in D_G(\varphi_3)$ and $dd' \in D_G(\varphi_4)$. Using the directedness of $\mathcal{S}$, pick a form $\varphi \in \mathcal{S}$ so that $S_G(\varphi_i) \subseteq D_G(\varphi)$, $i = 1, 2, 3, 4$. Now (2) follows from (ii)⇒(i) of lemma 4.2.44(a) applied to φ.

(b)⇒(a): is immediate from (i)⇒(ii) in lemma 4.2.44(a). □

Lemma 4.2.45. *Let G be a special group and let φ_1, φ_2 be anisotropic Pfisfer forms over G, such that $D_G(\varphi_1) \subseteq D_G(\varphi_2)$. Then, for all forms ψ, θ over G,*

$$\psi \otimes \varphi_1 \equiv_G \theta \otimes \varphi_1 \Rightarrow \psi \otimes \varphi_2 \equiv_G \theta \otimes \varphi_2.$$

Proof. By induction on $n = \dim(\psi) = \dim(\theta)$. For $n = 1$, the conclusion is immediate, while for $n = 2$ it is a consequence of lemma 4.2.35(a). Assume the result is true for $n \geq 2$, and that $\psi = \langle a \rangle \oplus \lambda$, where $\dim(\lambda) = n$. Write $\theta = \langle b_1, ..., b_n, b_{n+1} \rangle$; thus

$$(\langle a \rangle \oplus \lambda) \otimes \varphi_1 \equiv \theta \otimes \varphi_1 = \langle b_1\varphi_1, ..., b_n\varphi_1, b_{n+1}\varphi_1 \rangle,$$

and so, by proposition 4.2.4(c), there are $x_j \in D_G(\varphi_1)$, $1 \leq j \leq n+1$, such that

$$a \in D_G(b_1x_1, ..., b_{n+1}x_{n+1}),$$

or equivalently, there are $c_2, ..., c_{n+1} \in G$, such that

$$\langle a, c_2, ..., c_{n+1} \rangle \equiv \langle b_1x_1, ..., b_{n+1}x_{n+1} \rangle. \tag{I}$$

Multiplying (I) by φ_1 yields

$$\begin{aligned} a\varphi_1 \oplus \langle c_2\varphi_1, ..., c_{n+1}\varphi_1 \rangle &\equiv b_1x_1\varphi_1 \oplus ... \oplus b_{n+1}x_{n+1}\varphi_1 \\ &\equiv b_1\varphi_1 \oplus ... \oplus b_{n+1}\varphi_1 \equiv a\varphi_1 \oplus (\lambda \otimes \varphi_1). \end{aligned} \tag{II}$$

Cancelling $a\varphi_1$ on both sides of (II) gives

$$\langle c_2, ..., c_{n+1} \rangle \otimes \varphi_1 \equiv c_2\varphi_1 \oplus ... \oplus c_{n+1}\varphi_1 \equiv \lambda \otimes \varphi_1. \tag{III}$$

From the induction hypothesis, we get

$$\langle c_2, ..., c_{n+1} \rangle \otimes \varphi_2 \equiv c_2\varphi_2 \oplus ... \oplus c_{n+1}\varphi_2 \equiv \lambda \otimes \varphi_2. \tag{IV}$$

Tensoring (I) with φ_2, yields, recalling that $D_G(\varphi_1) \subseteq D_G(\varphi_2)$,

$$\begin{aligned} \varphi_2 \oplus (c_2\varphi_2 \oplus ... \oplus c_{n+1}\varphi_2) &\equiv b_1x_1\varphi_2 \oplus ... \oplus b_{n+1}x_{n+1}\varphi_2 \\ &\equiv b_1\varphi_2 \oplus ... \oplus b_{n+1}\varphi_2 \equiv \theta \otimes \varphi_2. \end{aligned}$$

The substitution of (IV) in this last isometry shows that $\psi \otimes \varphi_2 \equiv \theta \otimes \varphi_2$, completing the induction step and the proof. □

Proposition 4.2.43 with lemmas 4.2.44 and 4.2.45, yield

Proposition 4.2.46. *Let G be a special group and Δ a Pfister subgroup of G, determined by the directed family $\mathcal{S}$ of Pfister forms over G. Then $(G/\Delta, \equiv^*_{G/\Delta}, -1/\Delta)$ is a special group, and the quotient map $\pi : G \to G/\Delta$ is a morphism of special groups. Further, $1 \neq -1$ in G/Δ iff $-1 \notin \Delta$. Moreover, in this situation we have*

a - If φ, ψ are n-forms in G, then $\pi \star \varphi \equiv^*_{G/\Delta} \pi \star \psi$ iff there is a Pfister form $\mathcal{P}$ in $\mathcal{S}$ such that $\varphi \otimes \mathcal{P} \equiv_G \psi \otimes \mathcal{P}$.

b - If $f : G \to H$ is a morphism of special groups satisfying $\Delta \subseteq Ker(f)$, then there is a unique SG-morphism $\hat{f} : G/\Delta \to H$ such that $f = \hat{f} \circ \pi$.

Proof.

a - Transitivity of the relation $\equiv^*_{G/\Delta}$ follows from lemma 4.2.45, using proposition 4.2.43. Likewise, axiom [SG6] is an immediate consequence of (a), which is proven by induction on n, using 4.2.45 and 4.2.43.

b - It is straightforward to verify that, setting $\hat{f}(\pi(a)) = f(a)$ one gets a well defined morphism of special groups.

□

The theory of quotients presented above yields the following result which in fact, is a version of Pfister's local-global principle:

Theorem 4.2.47 (Pfister local-global principle)**.** *For $a_1, ..., a_n, b_1, ..., b_n$ in a reduced special group G, the following are equivalent:*

a - $\langle a_1, ..., a_n\rangle \equiv_G \langle b_1, ..., b_n\rangle$.

b - $\langle a_1/\Delta, ..., a_n\Delta\rangle \equiv_{G/\Delta} \langle b_1/\Delta, ..., b_n/\Delta\rangle$ *for all maximal saturated subgroups Δ of G.*

Before proving this result, we show that it implies a more general version, holding in all special groups, reduced or not.

Proposition 4.2.48. *Let G be a special group such that $1 \neq -1$ and $a_1, ..., a_n, b_1, ..., b_n \in G$. The following are equivalent:*

a - *For some integer $k \geq 0$, $2^k \cdot \langle a_1, ..., a_n\rangle \equiv_G 2^k \cdot \langle b_1, ..., b_n\rangle$.*

b - $\langle a_1/\Delta, ..., a_n\Delta\rangle \equiv_{G/\Delta} \langle b_1/\Delta, ..., b_n/\Delta\rangle$ *for all maximal saturated subgroups Δ of G.*

Proof. (a)⇒(b): is consequence of Proposition 4.2.5 and that the quotient map $G \to G/\Delta$ is a SG-morphism.

(b)⇒(a): We apply Theorem 4.2.47 to $G/\mathrm{Sat}(G)$. Assume

$$2^k\langle a_1, ..., a_n\rangle \not\equiv 2^k\langle b_1, ..., b_n\rangle$$

for every $k \geq 0$. Proposition 4.2.46 applied to the family $\{2^n : n \geq 1\}$ of Pfister forms yields:

$$\langle a_1/\mathrm{Sat}(G), ..., a_n/\mathrm{Sat}(G)\rangle \not\equiv \langle b_1/\mathrm{Sat}(G), ..., b_n/\mathrm{Sat}(G)\rangle. \qquad (*)$$

By the preceding theorem, $G/\mathrm{Sat}(G)$ contains a maximal saturated subgroup, Γ, such that (*) holds modulo Γ, i.e, in $(G/\mathrm{Sat}(G))/\Gamma$. Let $\Delta = \pi^{-1}[\Gamma]$, where π is the canonical map from G to $G/\mathrm{Sat}(G)$. Using proposition 4.2.40(c), $\ker(\pi) \subseteq \Delta$, and the surjectivity of π, we check that Δ is a maximal saturated subgroup of G. Since $\Gamma = \Delta/\mathrm{Sat}(G)$ and G/Δ is isomorphic to $(G/\mathrm{Sat}(G))/\Gamma$ (as special groups), we obtain

$$\langle a_1/\Delta, ..., a_n/\Delta\rangle \not\equiv_{G/\Delta} \langle b_1/\Delta, ..., b_n/\Delta\rangle,$$

contrary to (2). □

Proof of Theorem 4.2.47. Lemma 4.2.13(c) gives (a)⇒(b). To prove the converse, assume G is reduced and $\langle a_1, ..., a_n\rangle \not\equiv_G \langle b_1, ..., b_n\rangle$. Then by proposition 4.2.5

$$2^k\langle a_1, ..., a_n\rangle \not\equiv_G 2^k\langle b_1, ..., b_n\rangle$$

for all $k \geq 0$. Hence, every Pfister form φ in the family $\{2^n : n \geq 0\}$ has the property

$$\langle a_1, ..., a_n\rangle \otimes \varphi \not\equiv_G \langle b_1, ..., b_n\rangle \otimes \varphi; \qquad (*)$$

further, it is closed under tensor products. By Zorn's Lemma, there is a maximal family $\mathcal{L}$ of Pfister forms over G containing $\langle 1,1\rangle$, closed under tensor products, and such that every $\varphi \in \mathcal{L}$ verifies (*). Note that every Pfister form φ verifying (*) is anisotropic; otherwise, φ would be hyperbolic (proposition 4.2.25(v)), and we know that for $l \geq 1$

$$\langle a_1, ..., a_n\rangle \otimes l\langle 1,-1\rangle \not\equiv_G \langle b_1, ..., b_n\rangle \otimes l\langle 1,-1\rangle, \qquad (**)$$

as the coefficients on each side occur in pairs c, $-c$.

Let $\Delta = \bigcup\{D_G(\varphi) : \varphi \in \mathcal{L}\}$. By lemma 4.2.28(b), Δ is a proper saturated subgroup of G. We show that Δ is maximal saturated. By 4.2.36 it is suffices to show that, for $x \in G$, either $x \in \Delta$ or $-x \in \Delta$.

For $y \in G$, let $\mathcal{L}_y = \mathcal{L} \cup \{\langle 1, y\rangle \otimes \varphi : \varphi \in \mathcal{L}\}$. $\mathcal{L}_y$ contains $\mathcal{L}$ and is closed under tensor products (because $\langle 1, y\rangle \otimes \langle 1, y\rangle \equiv_G \langle 1,1\rangle \otimes \langle 1, y\rangle$). If $y \notin \Delta$, by the maximality of $\mathcal{L}$, the isometry

$$\langle a_1, ..., a_n\rangle \otimes \langle 1, y\rangle \otimes \varphi \equiv_G \langle b_1, ..., b_n\rangle \otimes \langle 1, y\rangle \otimes \varphi \qquad (***)$$

holds for some form $\varphi \in \mathcal{L}$. Note that if we have $y, z \notin \Delta$ and φ_1, φ_2 are the forms in $\mathcal{L}$ satisfying (***) in relation to y and z, respectively, then $\varphi = \varphi_1 \otimes \varphi_2$ is in $\mathcal{L}$ and satisfies (***) with respect to y and z, simultaneously. Thus, we may assume that (***) holds as stated for x and $-x$.

Assume $x, -x \in \Delta$. Applying (***) to x and $-x$, and adding up the instance of (***) thus obtained, yields:

$$\langle a_1, ..., a_n\rangle \otimes \varphi \otimes (2 \oplus \langle 1,-1\rangle) \equiv_G \langle b_1, ..., b_n\rangle \otimes \varphi \otimes (2 \oplus \langle 1,-1\rangle),$$

recalling that $\langle 1, x, 1, -x\rangle \equiv_G \langle 1,1\rangle \oplus \langle 1,-1\rangle$. Cancelling out the terms

$$\langle a_1, ..., a_n\rangle \otimes \varphi \otimes \langle 1,-1\rangle \equiv_G \langle b_1, ..., b_n\rangle \otimes \varphi \otimes \langle 1,-1\rangle,$$

in agreement with (**), we get

$$\langle a_1, ..., a_n\rangle \otimes 2\varphi \equiv_G \langle b_1, ..., b_n\rangle \otimes 2\varphi,$$

in contradiction to (*), since $2\varphi \in \mathcal{L}$. □

4.2.6 Duality

Here, we want to construct a duality between the categories of $\mathcal{RSG}$ and $\mathcal{AOS}$, i.e, we want to prove that the categories of $\mathcal{RSG}$ and $\mathcal{AOS}^{op}$ are equivalent. Here, we will work with the third version of abstract ordering spaces, i.e, the structure $(X, G, -1)$ is an AOS if it verifies the following conditions:

O1 - X is closed in $\chi(G)$ (equivalently, in $\{\pm 1\}^G$).

O2 - $\sigma(-1) = -1$ for all $\sigma \in X$.

O3 - $\bigcap_{\sigma\in X} \mathrm{Ker}(\sigma) = \{1\}$.

O4 - If φ, ψ are forms over G and $x \in G$, then $x \in D_X(\varphi \oplus \psi)$ implies that there are $y \in D_X(\varphi)$ and $z \in D_X(\psi)$ such that $x \in D_X(y, z)$.

In her thesis, Lira [dL96] proves the following interesting result:

Proposition 4.2.49. *Let G be a group of exponent 2 with a distinguished element -1, and $X \subseteq \chi(G)$. If the structure $(X, G, -1)$ satisfies the axioms [O1], [O2] and [O3], the following are equivalent:*

a - $(X, G, -1)$ *satisfies [O4].*

b - Strong and weak isometry modulo X are identical on forms of all dimensions.

c - Strong isometry modulo X is transitive on forms of dimension 3, and $(X, G, -1)$ verifies the following maximality condition:

O5 - *For every $\sigma \in \chi(G)$, such that $\sigma(-1) = -1$, if for all $a \in G$ $[a \in Ker(\sigma) \Rightarrow D_X(1, a) \subseteq Ker(\sigma)]$, then $\sigma \in X$.*

We further use this characterization. Also, our notion of morphism here is:

Definition 4.2.50. *Let $(X, G, -1)$ and $(Y, H, -1)$ be AOS's. A map $\gamma : X \to Y$ is a **morphism** of AOS's iff there is a continuous group homomorphism $\Gamma : \chi(G) \to \chi(H)$, such that $\gamma = \Gamma|_X$.*

Definition 4.2.51. *Let G be a special group. The space of orderings of G is the set X_G of all SG-morphisms of G into $\mathbb{Z}_2$, endowed with the topology induced by the product $\{\pm 1\}^G$.*

The space of orderings has the following properties:

Proposition 4.2.52. *Let G be a rsg. Then*

a - X_G *is closed in $\{\pm 1\}^G$ (and in $\chi(G)$).*

b - X_G *is a Boolean space.*

c - $\bigcap_{\sigma \in X_G} Ker(\sigma) = 1$.

Proof. For itens (a) and (b), just reproduce the proof in 1.6.1. For (c), follows from the Separation Theorem 4.2.37: since G is reduced, $\{1\}$ is saturated; given $a \neq 1$, there is a maximal saturated subgroup Δ of G such that $a \notin \Delta$. But we have $\Delta = \ker(\sigma)$, for some $\sigma \in X_G$. □

For a form $\varphi = \langle a_1, ..., a_n \rangle$ ver G and a map $\sigma : G \to \{\pm 1\}$, we set $\text{sgn}_\sigma(\varphi) = \sum_{i=1}^n \sigma(a_1)$ (addition in $\mathbb{Z}$). $\text{sgn}_\sigma(\varphi)$ is called the *signature* of φ at σ. With notation as in 4.2.32, if φ is a form over a formally real special group G, then for all $\sigma \in X_G$, $\text{sgn}_\sigma(\varphi) = \text{sgn}_{\hat{\sigma}}(\pi \star \varphi)$.

Our next result, a reformulation of theorem 4.2.47, is another abstract version of Pfister local-global principle. It will be of crucial importance in the sequel.

Proposition 4.2.53 (Pfister's Local-Global Principle)**.** *For $a_1, ..., a_n, b_1, ..., b_n$ in a reduced special group G, the following are equivalent:*

a - $\langle a_1, ..., a_n \rangle \equiv_G \langle b_1, ..., b_n \rangle$.

b - For every $\sigma \in X_G$, $sgn_\sigma(\langle a_1, ..., a_n \rangle) = sgn_\sigma(\langle b_1, ..., b_n \rangle)$.

Proof. Immediate from Theorem 4.2.47. □

Definition 4.2.54. *Let G be a group of exponent 2 with a distinguished element -1. Let $X \subseteq \chi(G)$.*

a - The notion of weak isometry modulo X, denoted $\equiv_X$, is defined as follows: for forms $\varphi = \langle a_1, ..., a_n \rangle$ and $\psi = \langle b_1, ..., b_n \rangle$ over G

$$\varphi \equiv_X \psi \text{ iff for all } \sigma \in X, (sgn_\sigma(\varphi) = sgn_\sigma(\psi)).$$

b - If φ is a form of dimension n over G, define

$$D_X(\varphi) = \{b \in G : \exists\, b_2, ..., b_n \in G \text{ such that } \varphi \equiv_X \langle b, b_2, ..., b_n\rangle\},$$

the set of elements weakly represented by φ modulo X.

c - We denote by $\equiv_X^*$ the extension to forms of arbitrary dimension of the weak isometry relation on binary forms. The relation $\equiv_X^*$ is referred to as strong isometry modulo X.

Now, we state some properties of weak isometry:

Lemma 4.2.55. *Let G be a group of exponent 2 and $X \subseteq \chi(G)$. Then*

a - Weak isometry modulo X is transitive on forms of any dimension.

b - Strong isometry implies weak isometry (but not conversely!)

c - Let $\varphi, \theta_1, \theta_2$ be forms over G, then

$$\varphi \oplus \theta_1 \equiv_X \varphi \oplus \theta_2 \Leftrightarrow \theta_1 \equiv_X \theta_2.$$

The results proved above at once yield

Proposition 4.2.56. *If $(G, \equiv_G, -1)$ is a rsg, then $(X_G, G, -1)$ is an AOS.*

Proof. O1 and O3 come from Lemma 4.2.52(a) and (c); O2 is contained in the definition of X_G; O4 is an immediate consequence of Proposition 4.2.53 and 4.2.4(c). □

Conversely, any abstract order space generates a reduced special group, as follows:

Proposition 4.2.57. *If $(X, G, -1)$ be an AOS, then $(G, \equiv_X, -1)$ is a reduced special group.*

Proof. Checking that $(G, \equiv_X, -1)$ satisfies SG0-SG5 and the reduction axiom [red] is straightforward calculations. As for SG6, since weak isometry modulo X is transitive, it would be sufficient to show that, under our assumptions, strong and weak isometry modulo X are identical on forms of dimension 3. Indeed, this follows from O4, as we now prove: assume

$$\langle a_1, a_2, a_3\rangle \equiv_X \langle b_1, b_2, b_3\rangle; \tag{4.28}$$

then, $b_1 \in D_X(a_1, a_2, a_3)$. By O4, there is $x \in D_X(a_2, a_3)$ such that $b_1 \in D_X(a_1, x)$, i.e, there are $y, z \in G$ so that

$$\langle a_1, x\rangle \equiv_X \langle b_1, y\rangle; \tag{4.29}$$
$$\langle a_2, a_3\rangle \equiv_X \langle x, z\rangle. \tag{4.30}$$

It only remains to show that

$$\langle b_2, b_3\rangle \equiv_X \langle y, z\rangle. \tag{4.31}$$

The isometry 4.30 and 4.2.55(c) give $\langle a_1, a_2, a_3\rangle \equiv_X \langle a_1, x, z\rangle$. Similarly, 4.29 and 4.2.55(c) yield $\langle a_1, x, z\rangle \equiv_X \langle b_1, y, z\rangle$.

Since $\equiv_X$ is transitive, 4.28 and the last two isometries prove $\langle b_1, b_2, b_3\rangle \equiv_X \langle b_1, y, z\rangle$, which, using 4.2.55(c) again, implies 4.31. □

Summarizing, we have two correspondences between reduced special groups and abstract order spaces, as follows:

$$\Phi : \mathcal{RSG} \to \mathcal{AOS}, \qquad (G, \equiv_G, -1) \mapsto (X_G, G, -1)$$
$$\Psi : \mathcal{AOS} \to \mathcal{RSG}, \qquad (X, G, -1) \mapsto (G, \equiv_X, -1).$$

We show next that these correspondences are reciprocal to each other.

Proposition 4.2.58. *We have $\Phi \circ \Psi = Id_{\mathcal{AOS}}$ and $\Psi \circ \Phi = Id_{\mathcal{RSG}}$.*

Proof. First, we will prove that $\Psi \circ \Phi = Id_{\mathcal{RSG}}$. Since

$$\Psi \circ \Phi(G, \equiv_G, -1) = (G, \equiv_{X_G}, -1),$$

it suffices to show that the relations $\equiv_G$ and $\equiv_{X_G}$ are identical on binary forms. This is asserted by proposition 4.2.53.

Now, we will prove that $\Phi \circ \Psi = Id_{\mathcal{AOS}}$. Let us denote $\Psi(X, G, -1) = (G, \equiv_X, -1)$ by $G[X]$. Thus, $\Phi(G[X]) = (X_{G[X]}, G, -1)$, and we have to prove that $X = X_{G[X]}$.

By definition of the relation $\equiv_X$ each $\sigma \in X$ is a SG-morphism from $G[X]$ into $\mathbb{Z}_2$, so $X \subseteq X_{G[X]}$ follows. Conversely, since the special relation of $G[X]$ is $\equiv_X$, every $\sigma \in X_{G[X]}$ verifies the assumption of the maximality condition O5 in proposition 4.2.49 above; hence $\sigma \in X$. □

The final step is to extend the correspondences Φ, Ψ to functors. For this, we need to show that every morphism of AOS's is the restriction of a unique continuous group homomorphism of $\chi(G)$ into $\chi(H)$. This is an immediate consequence of

Proposition 4.2.59. *Let G be a group of exponent 2 and X a subset of $\chi(G)$ satisfying the separation axiom [O3]. Then, the subgroup of $\chi(G)$ generated by X, $[X]$, is dense in $\chi(G)$.*

For the proof of this result we need the following

Lemma 4.2.60. *Let K be a finite group of exponent 2, and let $\sigma_i \in \chi(K)$, $1 \leq i \leq n$. Then, $\{\sigma_1, ..., \sigma_n\}$ generates $\chi(K)$ iff $\bigcap_{i=1}^n Ker(\sigma_i) = \{1\}$.*

Proof. ($\Rightarrow$) If the conclusion fails, consider $a \in \bigcap_{i=1}^n \mathrm{Ker}(\sigma_i)$, $a \neq 1$, and any character σ such that $\sigma(a) = -1$ (such a σ exists because $\{a\}$ is an $\mathbb{F}_2$-linearly independent subset of K); then $\sigma \notin [\sigma_1, ..., \sigma_n]$.

($\Leftarrow$) We may assume that the character constantly equal to 1, $\mathbb{1}$, is not in $\{\sigma_1, ..., \sigma_n\}$. By induction on n we select an irredundant subset of $\{\sigma_1, ..., \sigma_n\}$, say $\sigma_1, ..., \sigma_m$, i.e, a subset with the following properties:

$$\bigcap_{i=1}^{m} \mathrm{Ker}(\sigma_i) = \{1\} \tag{4.32}$$

$$\text{For } 2 \leq j \leq m, \bigcap_{i=1}^{j-1} \mathrm{Ker}(\sigma_i) \not\subseteq \ker(\sigma_j). \tag{4.33}$$

By induction on m we choose elements $b_1, ..., b_m \in K$ such that

$$b_1 \notin \ker(\sigma_1) \tag{4.34}$$

$$\text{For } 2 \leq j \leq m, b_j \in \bigcap_{i=1}^{j-1} \mathrm{Ker}(\sigma_i),\ b_j \notin \ker(\sigma_j). \tag{4.35}$$

Claim. $\{b_1, ..., b_m\}$ is a $\mathbb{F}_2$-basis of K.

We prove by induction on m. If $m = 1$, by 4.32, $\ker(\sigma_1) = \{1\}$, that is, σ_1 is an isomorphism between K and $\{\pm 1\}$. By 4.34, $b_1 = -1$, a basis for K. Now suppose the claim true for $m-1$, $m \geq 2$. Consider the (proper) subgroup $K_1 = \ker(\sigma_1)$. For $i \geq 2$, let $\sigma' = \sigma_i|_{K_1}$; then $\sigma'_2, ..., \sigma'_m$ are in $\chi(K_1)$, $b_2, ..., b_m$ are in K_1 and

$$\bigcap_{i=2}^{m} \mathrm{Ker}(\sigma'_i) = \bigcap_{i=1}^{n} \mathrm{Ker}(\sigma_i) = \{1\};$$

$$\text{If } 3 \leq j \leq m, \text{ then } \bigcap_{i=2}^{j-1} \mathrm{Ker}(\sigma'_i) = \bigcap_{i=1}^{j-1} \mathrm{Ker}(\sigma_i) \not\subseteq \ker(\sigma_j);$$

whence $\bigcap_{i=2}^{j-1} \mathrm{Ker}(\sigma'_i) \not\subseteq \ker(\sigma_1) \cap \ker(\sigma_j) = \ker(\sigma'_j)$. By induction hypothesis, $\{b_2, ..., b_m\}$ is a basis for K_1. Since $b_1 \notin K_1$, $\{b_1, ..., b_m\}$ is a basis of K, proving the Claim.

The claim implies that $\{\sigma_1, ..., \sigma_m\}$ is an $\mathbb{F}_2$-basis of $\chi(K)$. Observe first that $\{\sigma_1, ..., \sigma_m\}$ is $\mathbb{F}_2$-linearly independent: if $1 \leq j \leq m$, we have $\sigma_j(b_j) = -1$, while $\sigma_i(b_j) = 1$ for $1 \leq i \leq j$; hence $\sigma_j \notin [\sigma_1, ..., \sigma_{j-1}]$. Now, the $\mathbb{F}_2$-dimension of K is equal to the $\mathbb{F}_2$-dimension of $\chi(K)$ (since $\chi(K)$ is the dual of K). So $\{\sigma_1, ..., \sigma_m\}$ is a basis for $\chi(K)$. □

Proof of theorem 4.2.59. Let $U \neq \emptyset$ be a clopen in $\chi(G)$; we show that $[X] \cap U \neq \emptyset$. The set U is of the form

$$U = \bigcap_{i=1}^{n} \{\sigma \in X : \sigma(a_i) = \delta(i)\},$$

for some $\{a_1, ..., a_n\} \subseteq G$, and $\delta : \{1, ..., n\} \to \{\pm 1\}$. Let $K = [a_1, ..., a_n]$; K is finite, and so is $\chi(K)$. Also, the finite set $X|_K = \{\sigma|_K : \sigma \in X\}$ separates points in K, i.e, $\bigcap_{\gamma \in X|_K} \ker(\gamma) = \{1\}$. Hence, tehre is a finite set $\{\sigma_1, ..., \sigma_n\} \subseteq X$ such that $\bigcap_{i=1}^{n} \mathrm{Ker}(\sigma_i|_K) = \{1\}$. Lemma 4.2.60 shows that $S = \{\sigma_i|_K : i \leq n\}$ generates $\chi(K)$. Thus, if $\lambda \in U$, we have that $\lambda|_K$ is a linear combination of S, say $\lambda|_K = \prod_{j=1}^{r} \sigma_{i_j}|_K$. Consequently, we have $\prod_{j=1}^{r} \sigma_{i_j} \in [X] \cap U$, as required. □

Now, we are in position to construct the functors Φ and Ψ. Let G, H be reduced special groups and $f : G \to H$ be a SG-morphism. The map $\Phi(f) : (X_H, H, -1) \to (X_G, G, -1)$ is obtained by composition

$$\Phi(f)(\sigma) = \sigma \circ f \text{ for } \sigma \in X_H. \tag{4.36}$$

$\sigma \circ f$ is a SG-morphism, so it is in X_G. Also $\Phi(f)$ is the restriction of the map $\chi(H) \to \chi(G)$ given by 4.36, which is a continuous group homomorphism. Hence $\Phi(f)$ is a morphism of AOS's.

Extending Ψ to morphisms is a more delicate task which requires a simple case of Pontrjagin's duality Theorem, namely

Theorem 4.2.61. *Let G be a group of exponent 2 and $\chi_c(\chi(G))$ be the group of **continuous** group character of $\chi(G)$ into $\{\pm 1\}$. Let $ev : G \to \chi_c(\chi(G))$ denote the **evaluation** map: for $g \in G$,*

$$ev(g) : \chi(G) \to \{\pm 1\}, \sigma \mapsto \sigma(g).$$

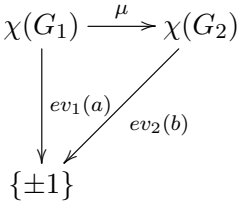
Then, ev is a group isomorphism between G and $\chi_c(\chi(G))$.

Let $\mu : (X_1, G_1, -1) \to (X_2, G_2, -1)$ be a morphism of AOS's. By proposition 4.2.59, μ is the restriction of a unique continuous homomorphism of $\chi(G_1)$ into $\chi(G_2)$, which we also denote by μ. By composition, μ induces a group homomorphism $\overline{\mu} : \chi_c(\chi(G_2)) \to \chi_c(\chi(G_1))$:

$$\overline{\mu}(\gamma) = \gamma \circ \mu \text{ for } \gamma \in \chi_c(\chi(G)).$$

If $b \in G_2$, then $ev_2(b) \in \chi_c(\chi(G_2))$, and hence $\overline{\mu}(ev_2(b)) \in \chi_c(\chi(G_1))$. Since ev_1 is an isomorphism between G_1 and $\chi_c(\chi(G_1))$, there is a unique $a \in G_1$ such that

$$ev_1(a) = ev_2(b) \circ \mu = \overline{\mu}(ev_2(b)). \tag{4.37}$$



This is equivalent to:

$$\text{For all } \sigma \in \chi(G_1),\ \sigma(a) = \mu(\sigma)(b). \tag{dual}$$

We now define,

$$\Psi(\mu)(b) = a.$$

Thus, setting $\mu^* = \Psi(\mu)$, we have $\mu^* : G_2 \to G_1$, while from [dual] comes

$$\text{For every } \sigma \in \chi(G_1) \text{ and } b \in G_2,\ \sigma(\mu^*(b)) = \mu(\sigma)(b). \tag{4.38}$$

Moreover, 4.37 and the fact that $ev_1(a)$ is an isomorphism yield

$$\mu^* = ev_1^{-1} \circ \overline{\mu} \circ ev_2. \tag{4.39}$$

Now we prove,

Theorem 4.2.62 (Duality Theorem)**.** *The correspondences Φ, Ψ are contravariant functors. Further, the compositions $\Phi \circ \Psi$ and $\Psi \circ \Phi$ are the identity functors, which shows that the pair (Φ, Ψ) establishes an equivalence between the categories $\mathcal{RSG}$ and $\mathcal{AOS}^{op}$.*

Proof. In view of Propositions 4.2.56, 4.2.57 and 4.2.58, only the assertions concerning morphisms require proof.

Straightforward checking shows that Φ and Ψ are contravariant functors (use identity 4.39 to check that Ψ reverses composition). The assertion of the statement are items (1), (2) and (3) below.

1. The map $\mu^* = \Psi(\mu)$ is a SG-morphism of $(G_2, \equiv_{X_2}, -1)$ into $(G_1, \equiv_{X_1}, -1)$.

   (a) μ^* is a group homomorphism. THis follows at once from 4.39, since $ev_2, \overline{\mu}$ and ev_1^{-1} are group homomorphisms.

   (b) $\mu^*(-1) = -1$. For this, let $a = \mu^*(-1)$; by 4.38,with $b = -1$ yields, for all $\sigma \in X_1$,

   $$\sigma(a) = \mu(\sigma)(-1) = -1,$$

since $\mu(\sigma) \in X_2$ (axiom O2). But then, axiom O3 guarantees that $a = -1$, since for all $\sigma \in X_1$, $\sigma(-a) = 1$.

(c) For $a, b, c, d \in G_2$,

$$\langle a, b\rangle \equiv_{X_2} \langle c, d\rangle \Rightarrow \langle \mu^*(a), \mu^*(b)\rangle \equiv_{X_1} \langle \mu^*(c), \mu^*(d)\rangle.$$

For this, let $\sigma \in X_1$. Since $\mu(\sigma) \in X_2$, we have

$$\mu(\sigma)(a) + \mu(\sigma)(b) = \mu(\sigma)(c) + \mu(\sigma)(d).$$

From 4.38 we get:

$$\sigma(\mu^*)(a) + \sigma(\mu^*)(b) = \sigma(\mu^*)(c) + \sigma(\mu^*)(d).$$

Since this holds for arbitrary $\sigma \in X_1$, we have $\mu^*(a), \mu^*(b)\rangle \equiv_{X_1} \langle \mu^*(c), \mu^*(d)\rangle$.

2. $\Phi \circ \Psi(\mu) = \mu$ for any morphism $\mu : (X_1, G_1, -1) \to (X_2, G_2, -1)$ of AOS's. Writing $\mu' = \Phi(\mu^*)$, we have $\mu'(\sigma) = \sigma \circ \mu^*$, for $\sigma \in \chi(G_1)$ (see 4.36). The left hand side of 4.38 gives $\sigma(\mu^*(a)) = \sigma \circ \mu^*(a) = \mu'(\sigma)(a)$; hence

$$\mu'(\sigma)(a) = \mu(\sigma)(a)$$

for arbitrary $a \in G_2$, $\sigma \in \chi(G_1)$. Fixing σ, this shows that $\mu'(\sigma) = \mu(\sigma)$, and hence $\mu' = \mu$.

3. For every SG morphism $f : (G_2, \equiv_{G_2}, -1) \to (G_1, \equiv_{G_1}, -1)$, $\Psi \circ \Phi(f) = f$. Let $\Phi(f) = f'$ and $f^* = \Psi(f')$. From 4.36 we have $f'(\sigma) = \sigma \circ f$, for $\sigma \in \chi(G_1)$. Computing the right side of 4.38 for $\mu^* = f^*$ and $\mu = f'$, gives

$$\sigma(f^*(a)) = f'(\sigma)(a) = \sigma(f(a))$$

for arbitrary $a \in G_2$, $\sigma \in \chi(G_1)$. Fixing a, this shows that $f^*(a) = f(a)$ and so $f = f^*$.

□

4.2.7 Boolean Algebras and Special Groups

One of the reasons why special group theory is so unique is its connection to Boolean algebras. This is the road that allows the applications of model theory to problems of quadratic forms. Here, let's just take a look at this story (a full proof of Marshall and Lam Conjectures stands for an upcoming work). Our main goal here is to define a group's boolean hull and sketch one of its applications in the next section, with the Invariants. In this purpose, we just list definitions and results, following closely chapters 4 and 5 of [DM00].

Definition 4.2.63. *A **Boolean algebra** B is a tuple $B = (B, \vee, \wedge, \neg, \bot, \top)$ where $(B, \vee, \wedge, \bot, \top)$ is a commutative ring with unit and $1 \neq 0$, satisfying the following properties for all $a, b \in B$:*

Absorption - $a \wedge (a \vee b) = a$ *e* $a \vee (a \wedge b) = a$;

Complementation - $a \vee \neg a = \top$ *e* $a \wedge \neg a = \bot$.

Lemma 4.2.64. *Let B be a Boolean algebra. Then for all $x, y \in B$:*

a - $x \wedge y = 0$ *and* $x \vee y = 1$ *imply* $x = y$.

b - $\neg(\neg x) = x$.

c - *(De Morgan's Laws)* $\neg(x \vee y) = \neg x \wedge \neg y$ *and* $\neg(x \wedge y) = \neg x \vee \neg y$.

d - *(Idempotence)* $x \vee x = x$ *and* $x \wedge x = x$.

e - $x \vee y = y$ *if and only if* $x \wedge y = x$.

Lemma 4.2.65. *For every Boolean algebra* B*, the relation* $\leq$ *defined by*

$$x \leq y \text{ if and only if } x \vee y = y$$

(iff $x \wedge y = y$ *by 4.2.64(e)) is a partial order in* B.

Definition 4.2.66. *Let* B, B' *be Boolean algebras and* $f : B \to B'$ *be a map between them.* f *is a* ***morphism of Boolean algebras, or BA-morphism*** *if*

1. $f(\bot) = \bot$, $f(\top) = \top$;
2. $f(\neg x) = \neg f(x)$;
3. $f(x \vee y) = f(x) \vee f(y)$ *and* $f(x \wedge y) = f(x) \wedge f(y)$.

An ***isomorphism*** *between* B *and* B' *is just a bijective BA-morphism* $f : B \to B'$. *The category of (non-trivial) Boolean algebras, i.e,* $\bot \neq \top$*, and Boolean algebra homomorphisms shall be denoted by* $\mathcal{BA}$.

If B is a BA, define the operation of **symmetric difference** on B by

$$a \triangle b = (a \wedge \neg b) \vee (\neg a \wedge b), \qquad (a, b \in B).$$

We have that $(B, \triangle, \bot)$ is a group of exponent 2. **A subgroup of** B **is a subset of** B **containing** $\top$ **and closed under** $\triangle$.

So, in this context, given a Boolean algebra B, we define:

Product the symmetric difference $a\Delta b = (a \wedge -b) \vee (a \wedge b)$;

Distinguished elements $1 = \bot$ and $-1 = \top$;

Isometry $\langle a, b\rangle \equiv_B \langle a, b\rangle$ if and only if $a \wedge b = c \wedge d$ e $a\Delta b = c\Delta d$.

Since for all $a, b \in B$ $a \triangle b = a \vee b \Leftrightarrow a \wedge b = \bot$ and

$$(a \triangle b) \vee (a \wedge b) = (a \triangle b) \triangle a \wedge b = a \vee b,$$

we verify that $\langle a, b\rangle \equiv_B \langle a, b\rangle$ if and only if $a \wedge b = c \wedge d$ e $a \vee b = c \vee d$.

Definition 4.2.67. *A Boolean algebra* B *endowed with the structure defined above, will be denoted by* $Sg(B) = (B, \equiv_B, -1)$.

So, naturally, we desire a result like this:

Proposition 4.2.68. *If* B *is a BA,* $Sg(B) = (B, \equiv_B, -1)$ *is a reduced special group.*

The next natural question, is if $Sg(B)$ with the structure of pre-special group defined above is in fact, a special group. We obtain this with the following theorem:

Theorem 4.2.69. *Let G be a subgroup of a BA, and $p, q, u, v \in G$. The following are equivalent:*

i - $\langle p, q, p \triangle q\rangle \cong_G \langle u, v, u \triangle v\rangle$;

ii - *There is $\gamma \in G$ such that*

$$p \vee \gamma = u \vee \gamma = p \vee q = u \vee v.$$

Corollary 4.2.70. *Let B be a Boolean Algebra and p, q, u, v be elements in B. Then:*

a - $\langle p, q, p \triangle q\rangle \equiv_B \langle u, v, u \triangle v\rangle$ *if and only if* $p \vee q = u \vee v$.

b - $Sg(B) = (B, \equiv_B, -1)$ *is a reduced special group.*

c - $p \in D_B(1, q)$ *if and only if* $p \leq q$ *(in B).*

Now, is the time to deal with morphisms:

Proposition 4.2.71. *Let A, B be a Boolean Algebras and $f : |A| \to |B|$ a map between their underlying sets. The following are equivalent:*

i - *f is a SG-morphism from $Sg(A)$ to $Sg(B)$.*

ii - *f is a morphism of BA's.*

Corollary 4.2.72. *The correspondence which assigns to each BA, B its special group structure $Sg(B)$, and to every BA-morphism $f : A \to B$ the same mapping $f : Sg(A) \to Sg(B)$ is a functor $Sg : \mathcal{BA} \to \mathcal{RSG}$.*

Proposition 4.2.73. *Let B be a BA and $\Delta \subseteq B$. Then,*

a - *Δ is a saturated subgroup of $Sg(B)$ if and only if Δ is an ideal in B.*

b - *If Δ is a saturated subgroup of $Sg(B)$, then $Sg(B)/\Delta$ is naturally isomorphic (as a BA and as a special group) to $Sg(B/\Delta)$.*

c - *Any reduced SG-homomorphic image of B is (the special group of) a BA.*

With notation as in section 4.2.6, let B_G be the Boolean algebra of clopens in X_G. Define a map ε_G by

$$\varepsilon_G : G \to B_G, \text{ where } \varepsilon_G(a) = [a = -1],\ a \in G.$$

Proposition 4.2.74. *Let $(G, \equiv_G, -1)$ be a RSG. Then*

a - *ε_G is an injective group homomorphism from $(G, \cdot, 1, -1)$ into $(B_G, \triangle, \emptyset, X_G)$, where $\triangle$ denotes the symmetric difference in B_G.*

b - *If u is an element in B_G, then there is a family $\{F_i : 1 \leq i \leq n\}$ of finite subsets of G such that*

$$u = \bigcup_{i \leq n} \bigcap_{a \in F_i} \varepsilon_G(a).$$

Proposition 4.2.75. *Let G be a RSG, $\varphi = \langle 1, a_1\rangle \otimes ... \otimes \langle 1, a_n\rangle$ be a Pfister form on G, and $a \in G$. Let $\Delta = D_G(\varphi)$. Then*

a - $\{\sigma \in X_G : sgn_\sigma(\varphi) = 2^n\} = \{\sigma \in X_G : \Delta \subseteq ker(\sigma)\} = \cap_{i=1}^n [a_i = 1]$.

b - $a \in D_G(\varphi)$ if and only if $\varepsilon_G(a) \subseteq \bigcup_{i\leq n} \varepsilon_G(a)$.

Corollary 4.2.76. *The map ε_G is an injective SG-morphism from G into $Sg(B_G)$. In fact, for all $a, b \in G$,*

$$b \in D_G(1, a) \text{ if and only if } \varepsilon_G(b) \subseteq \varepsilon_G(a).$$

Corollary 4.2.77. *Let $(G, \equiv, -1)$ be a RSG, and T be a subgroup of G. $\overline{T}$ denotees the saturation of T (4.2.30). Then,*

a - $\overline{T} = \{y \in G : \exists$ finite subset $F \subseteq T$ such that $\varepsilon_G(y) \subseteq \bigcup_{x\in F} \varepsilon_G(x).\}$

b - $\overline{T}$ is a proper subgroup of G if and only if $\varepsilon_G(T) = \{\varepsilon_G(x) : x \in T\}$ generates a proper ideal in B_G.

Definition 4.2.78.

a - If G is a RSG, $\Sigma(G)$ denotes the set, partially ordered by inclusion, of proper saturated subgroups of G. If B is a Boolean algebra, $\mathcal{I}(B)$ denotes the set, partially ordered by inclusion, of proper ideals in B.

b - Given a saturated subgroup Δ of a RSG G, let

$$\mathcal{I}(\Delta) = \{u \in B_G : \exists \text{ a finite subset } F \subseteq \Delta \text{ such that } u \leq \bigcup_{g\in F} \varepsilon_G(g)\},$$

denote the ideal generated by Δ in B_G. If $\Delta \subseteq \Gamma$ then $\mathcal{I}(\Delta) \subseteq \mathcal{I}(\Gamma)$.

c - If I is an ideal in B_G, let

$$\Sigma(I) = \{g \in G : \varepsilon_G(g) \in I\}.$$

It follows from Corollary 4.2.77 that $\Sigma(I)$ is a saturated subgroup of G. In fact, if we identify G with its image in B_G, $\Sigma(I)$ is simply $I \cap G$. If $I \subseteq J$ then $\Sigma(I) \subseteq \Sigma(J)$.

Corollary 4.2.77(b) implies that, in fact, we have increasing maps

$$\Sigma : \mathcal{I}(B_G) \to \Sigma(G) \text{ and } \mathcal{I} : \Sigma(G) \to \mathcal{I}(B_G).$$

The main properties of these maps are given by

Proposition 4.2.79. *Let G be a reduced special group and B_G be its associated BA. With notations as above, we have:*

a - $\Sigma \circ \mathcal{I} = id_{\Sigma(G)}$.

b - Σ and $\mathcal{I}$ are inverse bijective correspondences between the maximal saturated subgroup of G and the maximal ideals in B_G.

We now establish the existence of a functor from $\mathcal{SG}$ to $\mathcal{BA}$, in fact right adjoint to the functor $Sg : \mathcal{BA} \to \mathcal{SG}$ defined in Corollary 4.2.72.

Definition 4.2.80. *Let G and H be reduced special groups and let $f : G \to H$ be a SG-morphism. Let $f^* : X_H \to X_G$ be the continuous map dual to f given by the Duality Theorem 4.2.62. We define $B(f)$ to be the Stone dual of f^*, that is the BA-morphism $B(f) : B_G \to B_H$ given by*

$$B(f)(u) = (f^*)^{-1}[u] \in B_G.$$

Theorem 4.2.81. *Let G and H be reduced special groups. With notation as above:*

1. *The correspondence B defined by*

$$G \mapsto B_G \qquad (G \xrightarrow{f} H) \mapsto (B_G \xrightarrow{B(f)} B_H,$$

is a functor from the category of reduced special groups (with SG-morphisms) to the category of Boolean Algebras (with BA-morphisms).

2. *For all SG-morphisms $G \xrightarrow{f} H$, we have*

$$\varepsilon_H \circ f = B(f) \circ \varepsilon_G, \tag{BH}$$

that is, the following diagram is commutative:

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle \varepsilon_G}\downarrow & & \downarrow{\scriptstyle \varepsilon_H} \\ B_G & \xrightarrow[B(f)]{} & B_H \end{array} \tag{BH}$$

3. *(Uniqueness) Given a SG-morphism $G \xrightarrow{f} H$ and a BA-morphism $F : B_G \to B_H$ such that the diagram*

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle \varepsilon_G}\downarrow & & \downarrow{\scriptstyle \varepsilon_H} \\ B_G & \xrightarrow[F]{} & B_H \end{array} \tag{**}$$

commutes, then $F = B(f)$.

4. *The pair (B_G, ε_G) is a **hull** for G in the category of BA's: given a BA, B, any SG-morphism $G \xrightarrow{f} Sg(B)$ factors through ε_G, i.e, the following diagram of special groups is commutative*

$$\begin{array}{ccc} G & \xrightarrow{\varepsilon_G} & Sg(B_G) \\ {\scriptstyle f}\downarrow & \swarrow{\scriptstyle B(f)} & \\ Sg(B) & & \end{array}$$

modulo the identification of B with the BA of clopens in $S(B)$, via the canonical map.

5. *The functor in (1) is right adjoint to the (forgetful) functor Sg from $\mathcal{BA}$ to $\mathcal{RSG}$.*

*In view of item (4), the Boolean algebra B_G will in the sequel be referred to as the **Boolean Hull** of the RSG G.*

Definition 4.2.82. *Let G, H be special groups. A group homomorphism $f : G \to H$ such that $f(-1) = -1$ is a **complete embedding** if for all forms φ and ψ over G*

$$\varphi \equiv_G \psi \text{ if and only if } f \star \varphi \equiv_H f \star \psi.$$

Theorem 4.2.83 (Corollary 5.4 [DM00])**.** *Let G be a RSG and let $\varepsilon_G : G \to B_G$ be the canonical embedding of G into B_G.*

a - ε_G is a complete embedding.

b - Every $\sigma \in X_G$ extends uniquely to B_G.

4.2.8 Invariants and the Hauptsatz

In this subsection, we will present some usage for the "toys" in the last subsection. Here, we following closely chapter 7 of [DM00]. Indeed, the main philosophy is

"The isometry of quadratic forms over arbitrary dimension n over a reduced special group G is equivalent to the validity, in the Boolean hull B_G of G, of a finite number of (actually n) Boolean identities among their coefficients."

This is exactly the content of Theorem 4.2.85. A seemingly simple and innocent statement is the heart of substantial results, like this one:

Theorem 4.2.84 (The Arason-Pfister Hauptsatz)**.** *Let G be a reduced special group. Fix an integer $n \geq 2$. Assume that ψ is a form over G of dimension $m < 2^n$, Witt equivalent to a linear combination of Pfister forms of degree n over G. Then, ψ is hyperbolic over G.*

Now, start our job with the invariants:

Theorem 4.2.85. *Let G be a reduced special group, and let $a_1, ..., a_n, b_1, ..., b_n$ be elements of G. For each $1 \leq k \leq n$, let $S^{n,k}$ be the set of all **strictly** increasing sequences of length k of elements of $\{1, ..., n\}$, denoted $p = (p_1, ..., p_k)$. Then, the following are equivalent:*

1. *$\langle a_1, ..., a_n \rangle \equiv_G \langle b_1, ..., b_n \rangle$.*
2. *For all $1 \leq k \leq n$, the following identities hold in the Boolean Hull B_G of G:*

$$\bigvee_{p \in S^{n,k}} \bigwedge_{i=1}^{k} a_{p_i} = \bigvee_{p \in S^{n,k}} \bigwedge_{i=1}^{k} b_{p_i}. \tag{HT_k}$$

3. *For all $1 \leq k \leq n$, the following identities hold in the Boolean Hull B_G of G:*

$$\triangle_{p \in S^{n,k}} \bigwedge_{i=1}^{k} a_{p_i} = \triangle_{p \in S^{n,k}} \bigwedge_{i=1}^{k} b_{p_i}. \tag{SW_k}$$

Definition 4.2.86. *Let G be a reduced special group. We define the **Horn-Tarski** and the **Stiefel-Whitney invariants** of a form $\varphi = \langle a_1, ..., a_n \rangle$ over G to be the following elements **of the Boolean Hull** B_G of G:*

$$\mathcal{HT}_k = \bigvee_{p \in S^{n,k}} \bigwedge_{i=1}^{k} a_{p_i} = \bigvee_{p \in S^{n,k}} \bigwedge_{i=1}^{k} b_{p_i}. \qquad \text{(Horn-Tarski invariants)}$$

$$\mathcal{SW}_k = \triangle_{p\in S^{n,k}} \bigwedge_{i=1}^{k} a_{p_i} = \triangle_{p\in S^{n,k}} \bigwedge_{i=1}^{k} b_{p_i}. \qquad \text{(Stiefel-Whitney invariants)}$$

for every integer $1 \leq k \leq n$.

Now, is the time to state some basic properties of the Horn-Tarski and Stiefel-Whitney invariants.

Proposition 4.2.87. *Let G be a reduced special group, B_G the Boolean hull of G, and $\varphi = \langle a_1, ..., a_n\rangle$ be a form of dimension n over G. Then,*

HT1 - $\mathcal{SW}_1(\varphi) = d(\varphi)$, *the discriminant of* φ.

HT2 - $\mathcal{HT}_n(\varphi) = \mathcal{SW}_n(\varphi) = a_1 \wedge ... \wedge a_n$.

HT3 - *The Horn-Tarski invariants are decreasing:*

$$\mathcal{HT}_1(\varphi) \geq \mathcal{HT}_2(\varphi) \geq ... \geq \mathcal{HT}_n(\varphi).$$

HT4 - *Assume that the sequence of coefficients in φ is decreasing, $a_1 \geq ... \geq a_n$ (in the partial order $x \leq y$ if and only if $x \in D_G(1, y)$, $x, y \in G$). Then, for $1 \leq k \leq n$*

$$\mathcal{HT}_k(\varphi) = a_k.$$

HT5 - $\varphi \equiv_{B_G} \langle \mathcal{HT}_1(\varphi), \mathcal{HT}_2(\varphi), ..., \mathcal{HT}_n(\varphi)\rangle$.

The next result gives explict formulas for both types of invariants in terms of each other, in a way that depends only on k and the dimension of the form, **but not on its coefficients**!

Theorem 4.2.88. *With notation as in Proposition 4.2.87, we have:*

HT6 - *For $1 \leq k \leq n$,*

$$\mathcal{SW}_k(\varphi) = \mathcal{SW}_k(\langle \mathcal{HT}_1(\varphi), \mathcal{HT}_2(\varphi), ..., \mathcal{HT}_n(\varphi)\rangle) = \triangle_{p\in S^{n,k}} \mathcal{HT}_{p_k}(\varphi).$$

HT7 - $\triangle_{i=1}^{n} \mathcal{HT}_i(\varphi) = d(\varphi) \in G$.

HT8 - *For $2 \leq k \leq n$,*

$$\mathcal{SW}_k(\varphi) = \triangle_{l=k}^{n} [\mathcal{HT}_l(\varphi)]^{c_{l,k}},$$

where $c_{l,k}$ is the parity of the binomial coefficient $\binom{l-1}{k-1}$, i.e, $c_{l,k} = 0$ (resp. 1) if it is even (resp. odd).

HT9 -

a - $\mathcal{SW}_2(\varphi) = \triangle_{j=1}^{[n/2]} \mathcal{HT}_{2j}(\varphi)$.

b - $\mathcal{SW}_{n-1}(\varphi) = \begin{cases} \mathcal{HT}_{n-1}(\varphi) \text{ if } n \text{ is odd} \\ \mathcal{HT}_{n-1}(\varphi) \triangle \mathcal{HT}_n(\varphi) \text{ if } n \text{ is even.} \end{cases}$

HT10 - *For $1 \leq k \leq n$,*

$$\mathcal{HT}_k(\varphi) = \triangle_{p=k}^{n} [\mathcal{SW}_p(\varphi)]^{s(k,p)},$$

where $s(,k,k+j)$ is defined by induction on $j \geq 0$ as follows:

$$s(k,k) = 1 \text{ and } s(k,k+j) = \sum_{i=0}^{j-1} c_{k+j,k+i} \cdot s(k,k+i).$$

Definition 4.2.89.

a - For a form φ over G, we set

$$\mathcal{HT}_0(\varphi) = \mathcal{SW}_0(\varphi) = \top = (= -1).$$

b - Let n, m and k be positive integers such that $k \leq n+m$. We define

$$A^{n,m,k} = \{(s,r) : 0 \leq s \leq \min\{k,n\},\ 0 \leq r \leq \min\{k,m\},\ \text{and } s+r=k\}.$$

Proposition 4.2.90 (Addition formulas)**.** *Let φ, ψ be forms over a reduced special group G, of dimension n, m respectively. With notation as in definition 4.2.89(b), we have, for $1 \leq k \leq n+m$:*

HT11 - $\mathcal{HT}_k(\varphi \oplus \psi) = \bigvee_{(s,r)\in A^{n,m+k}} (\mathcal{HT}_s(\varphi) \wedge \mathcal{HT}_r(\psi))$.

HT12 - $\mathcal{SW}_k(\varphi \oplus \psi) = \triangle_{(s,r)\in A^{n,m+k}} (\mathcal{SW}_s(\varphi) \wedge \mathcal{SW}_r(\psi))$.

Corollary 4.2.91. *Let φ be a form of dimension n over a reduced special group G and $y \in G$. Then for $1 \leq k \leq n$, we have:*

$$\begin{aligned} \mathcal{HT}_k(\varphi \oplus \langle y\rangle) &= \mathcal{HT}_k(\varphi) \vee (\mathcal{HT}_{k-1}(\varphi) \wedge y) \qquad (\mathrm{HT}_{13}) \\ \mathcal{SW}_k(\varphi \oplus \langle y\rangle) &= \mathcal{SW}_k(\varphi) \triangle (\mathcal{SW}_{k-1}(\varphi) \wedge y) \\ \mathcal{HT}_{n+1}(\varphi \oplus \langle y\rangle) &= \mathcal{SW}_{n+1}(\varphi \oplus \langle y\rangle) = \mathcal{HT}_n(\varphi) \wedge y. \end{aligned}$$

Another natural question is wheter the Horn-Tarski and Stiefel-Whitney invariants of a tensor product can be expressed as Boolean functions of those of the factors in a reasonably simple and meaningful way. Proposition 4.2.92 below gives one such expansion for the Stiefel-Whitney invariants. However, we have not been able to find an expression of this kind for the Horn-Tarski invariants; the difficult lies in the absence of a tractable distributive law of join over symmetric difference.

Proposition 4.2.92. *Let G be a reduced special group, $\varphi = \langle a_1, ..., a_n\rangle$, $\psi = \langle x_1, ..., x_m\rangle$ be forms over G of dimensions n, m, respectively. For $\varepsilon \in \{\pm 1\}$ and $x \in G$, set*

$$\varepsilon x = \begin{cases} x \text{ if } \varepsilon = 1 \\ -x \text{if } \varepsilon = -1. \end{cases}$$

For integers k, n, m such that $k \leq mn$, define

$$F_{k,n}^m = \{(s_1, ..., s_m) : 0 \leq s_j \leq n \text{ and } \sum_{j=1}^{n} s_j = k\}.$$

Then, the following identities hold in B_G, for $1 \leq k \leq nm$:

$$\mathcal{SW}_k(\varphi \otimes \psi) = \triangle_{\varepsilon \in 2^m} \left(\triangle_{s \in F^m_{k,n}} \bigwedge_{j=1}^{m} \mathcal{SW}_{s_j}(-\varepsilon_j \varphi) \right) \wedge \varepsilon_1 x_1 \wedge ... \wedge \varepsilon_m x_m \tag{HT14}$$
$$= \triangle_{\eta \in 2^n} \left(\triangle_{t \in F^n_{k,m}} \bigwedge_{i=1}^{n} \mathcal{SW}_{t_i}(-\eta_i \psi) \right) \wedge \eta_1 a_1 \wedge ... \wedge \eta_n a_n.$$

The case $m = 1$ of Proposition 4.2.92 is interesting in its own right:

Proposition 4.2.93. *Let G be a RSG. Let φ be a form of dimension n over G and $x \in G$. Then, for $1 \leq k \leq n$:*

$$\mathcal{SW}_k(x\varphi) = (\mathcal{SW}_k(\varphi) \wedge -x) \triangle (\mathcal{SW}_k(-\varphi) \wedge x). \tag{HT15}$$

$$\mathcal{HT}_k(x\varphi) = (\mathcal{HT}_k(\varphi) \wedge -x) \triangle (\mathcal{HT}_k(-\varphi) \wedge x). \tag{HT16}$$

Now, we are deal with computations of the Horn-Tarski and Stiefel-Whitney invariants of Pfister forms and their multiples:

Theorem 4.2.94. *Let G be a reduced special group. Let $a \in G$, and $\varphi = \langle 1, a_1 \rangle \otimes ... \otimes \langle 1, a_n \rangle$ be a Pfister form over G of degree $n \geq 1$. Then:*

$$\mathcal{HT}_k(a\varphi) = \begin{cases} a \vee \bigvee_{i=1}^{n} a_i = \mathcal{HT}_1(a\varphi) \text{ for } 1 \leq k \leq 2^{n-1} \\ a \wedge - \bigvee_{i=1}^{n} a_i = \mathcal{HT}_{2^n}(a\varphi) \text{ for } 2^{n-1} + 1 \leq k \leq 2^n. \end{cases}$$

In particular,

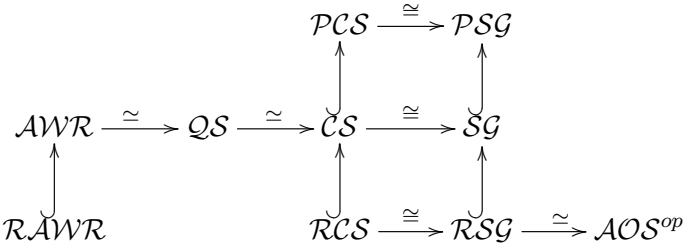
$$\mathcal{HT}_k(\varphi) = \begin{cases} \bigvee_{i=1}^{n} a_i = \mathcal{HT}_1(\varphi) \text{ for } 1 \leq k \leq 2^{n-1} \\ \bot = \mathcal{HT}_{2^n}(\varphi) \text{ for } 2^{n-1} + 1 \leq k \leq 2^n. \end{cases}$$

Theorem 4.2.95. *Let G be a reduced special group. Let $\varphi_1, ..., \varphi_r$ ($r \geq 1$) be Pfister forms over G of the same degree $n \geq 1$. Let $a_1, ..., a_r$ be elements of G. Given an integer m, $1 \leq m \leq r2^n$, let k be the unique integer such that $(k-1)2^{n-1} + 1 \leq m \leq k2^{n-1}$. Then*

$$\mathcal{HT}_k \left(\bigoplus_{i=1}^{r} a_i \varphi_i \right) = \mathcal{HT}_k(\langle \mathcal{HT}_1(a_1\varphi_1), ..., \mathcal{HT}_1(a_r\varphi_r), ..., \mathcal{HT}_{2^n}(a_1\varphi_1), ..., \mathcal{HT}_{2^n}(a_r\varphi_r) \rangle).$$

4.3 The Second Functorial Picture

Here is our second functorial picture



Since we already know the Duality Theorem 4.2.62, our task is establish the functors between special groups and quaternionic structures and special groups and Cordes schemes. Again, we do not have founded these explicit relations in literature.

Theorem 4.3.1. *Let $(G,-1,V)$ be a pre-quadratic scheme. Define a relation $\equiv_S \subseteq G\times G\times G\times G$ by $\langle a,b\rangle \equiv_S \langle c,d\rangle$ if and only if $ab=cd$ and $ac\in V(cd)$. Then $(G,-1,\equiv_S)$ is a pre-special group. Moreover, $(G,-1,\equiv_S)$ is a special group iff $(G,-1,V)$ is a Cordes scheme and $(G,-1,\equiv_S)$ is reduced iff $(G,-1,V)$ is reduced.*

Proof. We will check each axiom of pre-special group:

SG0 - $\langle a,b\rangle \equiv_S \langle a,b\rangle$ since $a^2=1\in V(ab)$. If $\langle a,b\rangle \equiv_S \langle c,d\rangle$, then $ab=cd$ and $ac\in V(cd)=V(ab)$. Hence $\langle a,b\rangle \equiv_S \langle c,d\rangle$. Now, suppose $\langle a,b\rangle \equiv_S \langle c,d\rangle$ and $\langle c,d\rangle \equiv_S \langle e,f\rangle$.

SG1 - $\langle a,b\rangle \equiv_S \langle b,a\rangle$ since $ab\in V(ab)$.

SG2 - $\langle a,-a\rangle \equiv_S \langle 1,-1\rangle$ since $a\cdot(-a)=-1\in V(-1)$.

SG3 - Is just the definition of $\equiv_S$.

SG4 - $\langle a,b\rangle \equiv_S \langle c,d\rangle$ implies $ab=cd$ and $ac\in V(cd)=V(ab)$. $ab=cd\Rightarrow ab(-bc)=cd(-bc)\Rightarrow -ac=-bd$ and by C2 we have

$$ac\in V(ab)\Rightarrow -ab\in V(-cd).$$

Then $\langle a,-c\rangle \equiv_S \langle -b,d\rangle$.

SG5 - $\langle a,b\rangle \equiv_S \langle c,d\rangle$ implies $ab=cd$ and $ac\in V(cd)=V(ab)$, i.e, $(ag)(bg)=(cg)(dg)$ and $(ag)(cg)\in V((cg)(dg))$. Hence $\langle ag,bg\rangle \equiv_S \langle cg,dg\rangle$.

This proves the first part of theorem. Since SG6 is the prescription of theorem 3.3.9 and $\langle a,a\rangle \equiv_S \langle 1,1\rangle \Leftrightarrow a\in V(1)$, we have the second part. □

Corollary 4.3.2. *The correspondence $(G,-1,V)\mapsto(G,-1,\equiv_S)$ induces functors $S:\mathcal{PCS}\to\mathcal{PSG}$, $S:\mathcal{CS}\to\mathcal{SG}$ and $S:\mathcal{RCS}\to\mathcal{RSG}$.*

Proof. let $f:(G,V_G,-1)\to(H,V_H,-1)$ be a C-morphism. Since f is in particular a group homomorphism, we have

$$\begin{aligned}\langle a,b\rangle \equiv_S \langle c,d\rangle &\Rightarrow ab=cd \text{ and } ac\in V_G(cd)\\ &\overset{f(V_G(cd))\subseteq V_H(f(cd))}{\Rightarrow} f(a)f(b)=f(c)f(d) \text{ and } f(a)f(d)\in V(f(c)f(d))\\ &\Rightarrow \langle f(a),f(b)\rangle \equiv_S \langle f(c),f(d)\rangle.\end{aligned}$$

Then f is a SG-morphism. Defining $S(G,V,-1)=(G,\equiv_S,-1)$ and $S(f)=f$, we have the desired functors. □

Theorem 4.3.3. *Let $(G,-1,\equiv)$ be a pre-special group. For each $g \in G$, set $V_G(g)$ as the subgroup $D_G\langle 1,g\rangle$. Then $(G,-1,V_G)$ is a pre scheme. Moreover, $(G,-1,V_G)$ is a Cordes scheme iff $(G,-1,\equiv)$ is a special group and $(G,-1,V_G)$ is reduced iff $(G,-1,\equiv)$ is reduced.*

Proof. Note that $a \in V_G(1,a) = D(1,a)$. Now, suppose $g \in V_G(a)$. Then $g \in D_G(1,a)$, and there exist $x \in G$ such that $\langle g,x\rangle \equiv \langle 1,a\rangle$. By SG3, $gx = a$ and $x = ga$. So $\langle g,ga\rangle \equiv \langle 1,a\rangle$, and by SG4 $\langle 1,-g\rangle \equiv \langle -a,ga\rangle$, and $-a \in D_G(1,-g) = V_G(-g)$. Then $(G,V_G,-1)$ is a pre scheme. This proves the first part of theorem. Since SG6 is the prescription of theorem 3.3.9 and $\langle a,a\rangle \equiv_S \langle 1,1\rangle \Leftrightarrow a \in V_G(1)$, we have the second part. □

Corollary 4.3.4. *The correspondence $(G,-1,\equiv) \mapsto (G,V_G,-1)$ induces functors $C : \mathcal{PSG} \to \mathcal{PCS}$, $C : \mathcal{SG} \to \mathcal{CS}$ and $C : \mathcal{RSG} \to \mathcal{RCS}$.*

Proof. Let $f : (G,\equiv_G,-1) \to (H,\equiv_H,-1)$ be a SG-morphism.

$$\begin{aligned} g \in V_G(a) &\Rightarrow g \in D_G(1,a) \Rightarrow \langle g,ag\rangle \equiv_G \langle 1,a\rangle \Rightarrow \langle f(g),f(ag)\rangle \equiv_H \langle f(1),f(a)\rangle \\ &\Rightarrow f(g) \in D_H(1,f(a)) \Rightarrow f(g) \in V_H(f(a)). \end{aligned}$$

Then f is a C-morphism. Defining $C(G,-1,\equiv) = (G,V_G,-1)$ and $C(f) = f$ we have the desired functors. □

Theorem 4.3.5. *The functors S and C are quasi-inverse equivalences. In particular, $\mathcal{PCS} \cong \mathcal{PSG}$, $\mathcal{CS} \cong \mathcal{SG}$ and $\mathcal{RCS} \cong \mathcal{RSG}$.*

Theorem 4.3.6. *Let (G,Q,q) be a quaternionic structure. Define a relation $\equiv_Q \subseteq G\times G\times G\times G$ by $\langle a,b\rangle \equiv_Q \langle c,d\rangle$ if and only if $ab = cd$ and $q(a,b) = q(c,d)$ (this relation is just the binary isometry in quaternionic structures). Then $(G,-1,\equiv_Q)$ is a special group. Moreover, this correspondence is functorial.*

Proof. The results in section 3.1.2 yields the axioms SG0-SG6 for $(G,-1,\equiv_Q)$. Then we only need to treat about morphisms. Let $f : (G,Q_G,q_G) \to (H,Q_H,q_H)$ be a QS-morphism and $a \in G$. Of course, we already have $f(-1) = -1$ (and hence, $f(-a) = -f(a)$). Now, for $a,b \in G$ we have:

$$\begin{aligned} \langle a,b\rangle \equiv_Q \langle c,d\rangle &\Rightarrow ab = cd \text{ and } q(a,b) = q(c,d) \\ &\Rightarrow f(a)f(b) = f(c)f(d) \text{ and } q(f(a),f(b)) = q(f(c),f(d)) \\ &\Rightarrow \langle f(a),f(b)\rangle \equiv_Q \langle f(c),f(d)\rangle \end{aligned}$$

then f is a SG-morphism. Defining $S(G,Q,q) = (G,\equiv_Q,-1)$ and $S(f) = f$ we have the desired functor $S : \mathcal{QS} \to \mathcal{SG}$. □

For the converse of theorem 4.3.6 we will make (again!) the same construction made for the theorem 3.1.1. Let $(G,\equiv,-1)$ be a special group. We define Q_G to be the set of all isometry classes of quadratic forms of the type $\langle 1,-a,-b,ab\rangle$, with $a,b \in G$ and consider Q_G to be a "pointed set" with point 0 equal to the isometry class of $\langle 1,-1,1,-1\rangle$. In the sequel, we define $q_G : G\times G \to Q_G$ to be the map sending (a,b) to the isometry class of $\langle 1,-a,-b,ab\rangle$.

Theorem 4.3.7. *Let $(G,-1,\equiv)$ be a special group. Then (G,Q_G,q_G) is a quaternionic structure. Moreover, this correspondence provides a functor $Q : \mathcal{SG} \to \mathcal{QS}$.*

Proof. Using the forms theory for special groups, the verification of Q1-Q4 is the same made in theorem 3.4.3. Now, let $f : (G,\equiv_G,-1) \to (H,\equiv_H,-1)$ be a SG-morphism. Since f is in particular

a group homomorphism, we have

$$q_G(a,b) = 0 \Rightarrow \langle 1, -a, -b, ab\rangle = 0 \Rightarrow \langle 1, -f(a), -f(b), f(a)f(b)\rangle = 0 \Rightarrow q_H(f(a), f(b)) = 0.$$

Then f is a QS-morphism. Defining $Q(G, \equiv_G, -1) = (G, Q_G, q_G)$ and $Q(f) = f$, we have the desired functor $Q : \mathcal{QS} \to \mathcal{SG}$. □

Corollary 4.3.8. *The functors Q and S are quasi-inverse equivalences and the categories $\mathcal{QS}$ and $\mathcal{SG}$ are equivalent.*

Chapter 5

A third generation of abstract theories

We see how abstract ordering spaces and special groups generalizes almost entire classical and reduced theory of quadratic forms over fields. But in the sense of generalization, we could ask

Is there some reasonable theory of quadratic forms over general coefficients in rings?

There is an excellent book, [Knu91], that deal with quadratic forms in an style near to that was presented in chapter 1, in the most general possible setting. And of course, some abstract theories appears trying to deal with this question. In 90's Marshall generalizes the AOS to rings, and called his new theory by "Abstract Real Spectrum". As we will see, the ring-theoretic case is much more difficult that the field one, the isometry is not well behaved and an algebraic counterpart of the ARS's appears just in years 2000, with the real semigroups (RS) of Dickmann and Petrovich.

The RS appears in an atempt to creat a duality $\mathcal{RS} \simeq \mathcal{ARS}^{op}$ likewise $\mathcal{SG} \simeq \mathcal{AOS}^{op}$. They are successful in explore the analogies with the $\mathcal{SG}$ case (e.g, the Duality $\mathcal{RS} \simeq \mathcal{ARS}^{op}$), but this is not pay off in deep theorems yet, since the theory still is in development.

5.1 Abstract Real Spectra

The ring-theoretic case is entire new for us, so we need to describe the basic facts about orderings and quadratic forms over rings. The axioms for ARS will be verified as we make in chapter 4. We cover chapters 5 and 6 of [Mar96].

5.1.1 Orderings on rings

All rings we consider here are commutative with 1. Let A be a ring and $\mathfrak{p}$ a prime ideal of A. We denote by $k(\mathfrak{p})$ the field $\mathrm{Frac}(A/\mathfrak{p})$, the field of quotients of $A/\mathfrak{p}$. $k(\mathfrak{p})$ is referred to as the **residue field** of A at $\mathfrak{p}$. Here, all prime ideals are considered to be **proper**, i.e, $\mathfrak{p} \neq A$.

An *ordering* on A is a subset $P \subseteq A$ such that $P + P \subseteq P$, $PP \subseteq P$, $P \cup -P = A$ and $P \cap -P$ is a prime ideal of A. The prime ideal is called the *support* of P.

Note that as in the field case, for an ordering P, $\sum A^2 \subseteq P$ and $-1 \notin P$, since $1 = 1^2 \in P$ and if $-1 \in P$, then $1 \in P \cap -P$, contradicting the fact that $P \cap -P$ is proper.

Proposition 5.1.1. *The set of orderings on A is in natural one-to-one correspondence with the set of pairs $(\mathfrak{p}, \overline{P})$ where $\mathfrak{p} \subseteq A$ is a prime ideal and $\overline{P}$ is an ordering on $k(\mathfrak{p})$.*

Proof. It suffices to show for each prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$, that the set of orderings in A with support $\mathfrak{p}$ is in natural one-to-one correspondence with the set of orderings in $k(\mathfrak{p})$. The natural homomorphism $A \to k(\mathfrak{p})$ is the composite of the natural homomorphism $q : A \to A/\mathfrak{p}$ with the inclusion $A/\mathfrak{p} \subseteq k(\mathfrak{p})$. Because of this, the proof breaks into two parts:

1. Orderings in A with support $\mathfrak{p}$ are in natural one-to-one correspondence with orderings in $A/\mathfrak{p}$ with support $\{0\}$ (via $q^{-1}(0)$).

2. If D is an integral domain with field of quotients k, then orderings in D with support $\{0\}$ are in natural one-to-one correspondence with orderings in k. If P is an ordering in k, then $Q = P \cap D$ is an ordering in D with support $\{0\}$. We must show that if Q is any ordering on D with support $\{0\}$, then there exists a unique ordering P on k with $P \cap D = Q$. Suppose $a, b \in D$, $b \neq 0$. Since $a/ab = ab/b^2$ and P contain squares, follow that $a/b \in P$ iff $ab \in Q$. Thus P is unique. To complete the proof it remains to check that

$$P = \{a/b : a, b \in D,\, b \neq 0,\, ab \in Q\}$$

is an ordering on k. It follows by properties of fractions on k and by the fact that Q is an ordering.

□

Orderings play roughly the same role in real algebraic geometry that prime ideals play in classical algebraic geometry. The set of all orderings in A is called the **real spectrum** of A, denoted by $\mathrm{Sper}(A)$.

We have a natural mapping $\mathrm{Sper}(A) \to \mathrm{Spec}(A)$ given by $P \mapsto P \cap -P$. This is neither surjective nor injective in general (for a given prime ideal $\mathfrak{p}$ in A, there may be no orderings on $k(\mathfrak{p})$ or there may be many).

A prime ideal is said to be **real** if there exist an ordering on A with support $\mathfrak{p}$, i.e, if $k(\mathfrak{p})$ is formally real, i.e, if $-1 \notin \sum k(\mathfrak{p})^2$. If $a_0^2 + ... + a_n^2 \in \mathfrak{p}$ and $a_0 \notin \mathfrak{p}$, then

$$-1 + \mathfrak{p} = \sum_{j=1}^{n} \left(\frac{a_j + \mathfrak{p}}{a_0 + \mathfrak{p}} \right)^2$$

and conversely. Thus, since we can always choose a common denominator for elements in $k(\mathfrak{p})$, we see that the condition for $\mathfrak{p}$ to be real is that $a_0^2 + ... + a_n^2 \in \mathfrak{p} \Rightarrow a_0 \in \mathfrak{p}$.

A *preordering* in A is a subset T of A satisfying $T + T \subseteq T$, $TT \subseteq T$ and $A^2 \subseteq T$. A preordering T of A is said to be *proper* if $-1 \notin T$. Every ordering is a proper preordering. $\sum A^2$ us a preordering, and is the unique smallest preordering of A.

If 2 is a unit in A, then we have the identity $a = (\frac{a+1}{2})^2 - (\frac{a-1}{2})^2$ holding on A so, in this case, a preordering $T \subseteq A$ is proper iff $T \neq A$. If 2 is not a unit in A, the situation is more complicated.

Lemma 5.1.2. *A proper preordering $P \subseteq A$ is an ordering iff it satisfies the following condition: $a \notin P, b \notin P \Rightarrow -ab \notin P$.*

Proof. ($\Rightarrow$) Suppose P is an ordering with support $\mathfrak{p}$ and suppose $a \notin P$, $b \notin P$. Then $-a, -b \in P$ so $ab = (-a)(-b) \in P$. If $-ab \in P$, then $ab \in \mathfrak{p}$ so one of a, b is in $\mathfrak{p}$, say $a \in \mathfrak{p}$. This contradicts $a \notin P$.

($\Leftarrow$) If $a \notin P$ and $-a \notin P$ then $-(a)(-a) = a^2 \notin P$, a contradiction. This proves $P \cup -P = A$. Let $\mathfrak{p} = P \cap -P$. Then $-\mathfrak{p} = \mathfrak{p}$, $\mathfrak{p} + \mathfrak{p} = \mathfrak{p}$, and $P\mathfrak{p} = \mathfrak{p}$. Since $A = P \cup -P$, this shows $A\mathfrak{p} = \mathfrak{p}$,

i.e, $\mathfrak{p}$ is an ideal. If $a \notin \mathfrak{p}$, $b \notin \mathfrak{p}$, but $ab \in \mathfrak{p}$ then, replacing a, b by $\pm a, \pm b$ if necessary, we get $a \notin P, b \notin P$, but $ab \in -P$, a contradiction. This proves $\mathfrak{p}$ is a prime ideal. □

Theorem 5.1.3. *If T is a proper preordering in A then there exists an ordering P of A with $T \subseteq P$. In particular, A has an ordering iff A has a proper preordering iff $-1 \notin \sum A^2$.*

Proof. Let P be a proper preordering containig T and maximal with respect to inclusion. Such a P exists by Zorn's lemma. Suppose $a \notin P$, $b \notin P$, but $ab \in -P$. Then $P + aP$ is a preordering containing P properly so $-1 \in P + aP$. Thus $-1 = s_1 + t_1 a$, $s_1, t_1 \in P$. Similarly, $-1 = s_2 + t_2 b$, $s_2, t_2 \in P$. Thus $abt_1t_2 = (-t_1a)(-t_2b) = (1 + s_1)(1 + s_2) = 1 + s$, $s = s_1 + s_2 + s_1s_2 \in P$, so $-1 = s - abt_1t_2 \in P$, a contradiction. □

Suppose $\alpha : A \to B$ is a ring homomorphism. If P is a some ordering of B, then $\alpha^{-1}(P)$ is an ordering on A. We refer to $\alpha^{-1}(P)$ as the **induced ordering** on A. The support of $\alpha^{-1}(P)$ is $\alpha^{-1}(\mathfrak{p})$ where $\mathfrak{p}$ is the support of P.

Example 5.1.4.

1. *Suppose $\mathfrak{a}$ is an ideal of A and $\alpha : A \to A/\mathfrak{a}$ is the natural homomorphism. Then $P \mapsto \alpha^{-1}(P)$ is a one-to-one correspondence between orderings in $A/\mathfrak{a}$ and orderings in A containing $\mathfrak{a}$ in their support.*

2. *Consider the natural homomorphism $\alpha : A \to S^{-1}(A)$, where $S \subseteq A$ is a multiplicative set. We don't exclude the zero ring, it could be $0 \in S$. Also, α is not generally injective: $\alpha(a) = 0 \Leftrightarrow as = 0$ for some $s \in S$. Then, $P \mapsto \alpha^{-1}(P)$ is a one-to-one correspondence between orderings in $S^{-1}(A)$ and orderings in A whose supports have empty intersection with S.*

3. *If $\mathfrak{p} \subseteq A$ is a prime ideal, the associated mapping $P \mapsto \alpha^{-1}(P)$ is a one-to-one correspondence between orderings of $k(\mathfrak{p})$ and orderings in A having support $\mathfrak{p}$. This has already been proved in 5.1.1.*

Now, we will make a couple of examples of orderings on rings:

Example 5.1.5. *Orderings on fields.*

Example 5.1.6. *If P, Q are orderings in A with $P \subseteq Q$ then $Q = P \cup (Q \cap -Q)$ (for, if $a \in Q \setminus P$, then $-a \in P$ so $-a \in Q$). Of course, in the field case, $Q \cap -Q = \{0\}$, so this implies $P = Q$. In the ring case, on the other hand, ordeings can exist which are not maximal with respect to inclusion. For example, take A to be the polynomial ring $\mathbb{R}[t]$, and let*

$$P_0 = \{a_0 + a_1t + ... + a_kt^k : k \geq 0,\, a_0 \geq 0\} \cup \{0\}$$
$$P_{0^+} = \{a_jt^j + ... + a_kt^k : 0 \leq j \leq k,\, a_j > 0\} \cup \{0\}.$$

Then P_0, P_{0^+} are orderings in $\mathbb{R}[t]$ and $P_{0^+} \subsetneq P_0$. Observe that P_{0^+} has support $\{0\}$ where as P_0 has support (t), the principal ideal generated by t.

Example 5.1.7. *An ordering P can be maximal without the prime ideal $P \cap -P$ being maximal. For example, take A to be the polynomial ring $\mathbb{R}[t]$ again, and*

$$P_{\infty^+} = \{a_0 + a_1t + ... + a_kt^k : k \geq 0,\, a_k > 0\} \cup \{0\}.$$

Then P_{∞^+} is an ordering in A which is maximal but the support of P_{∞^+} is $\{0\}$ which is not maximal.

Example 5.1.8. *In 5.1.6 and 5.1.7 we constructed three orderings $P_0, P_{0^+}, P_{\infty^+}$ on $\mathbb{R}[t]$. Applying the automorphism $t \mapsto -t$ to P_{0^+}, P_{∞^+} yields two additional orderings P_{0^-}, P_{∞^-}. Applying the automorphism $t \mapsto t - a$ $(a \in \mathbb{R})$ to P_0, P_{0^+}, P_{0^-} yields orderings P_a, P_{a^+}, P_{a^-} with $P_{a^+}, P_{a^-} \subsetneq P_a$. The orderings P_{a^+}, P_{a^-} for $a \in \mathbb{R}$ together with $P_{\infty^+}, P_{\infty^-}$ have support $\{0\}$. The ordering P_a has as support $(t-a)$. We have*

$$Sper(\mathbb{R}[t]) = P_{\infty^+} \cup P_{\infty^-} \cup \{P_a, P_{a^+}, P_{a^-}\}_{a \in \mathbb{R}[t]}.$$

The support $\{0\}$ orderings on $\mathbb{R}[t]$ are just the orderings on the field $\mathbb{R}(t)$.

Example 5.1.9. *For the study of semi-algebraic sets in $\mathbb{R}^n$, one is interested in the real spectrum of the polynomial ring $\mathbb{R}[t_1, ..., t_n]$. As the reader may well imagine, this is pretty complicated in $n \geq 2$. On the other hand, as in the case $n = 1$, there is a small subset of $Sper(\mathbb{R}[t_1, ..., t_n])$ which is easily described. For each $a \in \mathbb{R}^n$, define*

$$P_a = \{f \in \mathbb{R}[t_1, ..., t_n] : f(a) \geq 0\}.$$

This is an ordering with support equal to the maximal ideal $(t_1 - a_1, ..., t_n - a_n)$ where $a_1, ..., a_n$ are the coordinates of a. The mapping $a \mapsto P_a$ from $\mathbb{R}^n$ into $Sper(\mathbb{R}[t_1, ..., t_n])$ is injective. If $a \in \mathbb{R}^n$, let

$$f = \sum_{j=1}^{n} (t_j - a_j)^2.$$

Then $f(a) = 0$, $f(b) > 0$ if $b \neq a$. Thus $-f \in P_a$, $-f \notin P_b$, if $b \neq a$.

Example 5.1.10. *Suppose $A = C(Y, \mathbb{R})$, the ring of all continuous functions from Y to $\mathbb{R}$, where Y is some compact Hausdorff space. For each $x \in Y$, we get the maximal ideal $\mathfrak{m}_x = \{a \in A : a(x) = 0\}$, and every maximal ideal of A is of this form. Otherwise we have a maximal ideal $\mathfrak{m} \neq \mathfrak{m}_x$ for all $x \in Y$ so, for each $x \in Y$, we get $a_x \in \mathfrak{m}$ with $a_x(x) \neq 0$. By compactness of Y, we have a finite set $a_1, ..., a_k \in \mathfrak{m}$ such that, for all $x \in Y$, $a_i(x) \neq 0$ for some i. Let $b = a_1^2 + ... + a_k^2$. Then $b \in \mathfrak{m}$ and $b(x) > 0$ for all $x \in Y$, so b is a unity of A, a contradiction.*

On the other hand, it is known that, except in very special cases, there are a lots of prime ideals of A which are not maximal. Observe that if $a, b \in A$, then $\sqrt{a^2 + b^2} \in A$. Using this we see that $\sum A^2 = A^2$. For any prime $\mathfrak{p} \subseteq A$, let

$$P = A^2 + \mathfrak{p} := \{a^2 + b : a \in A,\, b \in \mathfrak{p}\}.$$

Using $(A^2)(A^2) = A^2$ and $A^2 + A^2 = A^2$, we see that $PP = P$ and $P + P = P$. If $a \in A$, then $|a| \in A$ and $(|a| - a)(|a| + a) = a^2 - a^2 = 0 \in \mathfrak{p}$, so either $a \equiv |a| \mod \mathfrak{p}$, or $a \equiv -|a| \mod \mathfrak{p}$. Since $|a|$ is a square in A, this proves $P \cup -P = A$. Suppose $a^2 \equiv -b^2 \mod \mathfrak{p}$, and let

$$c = \begin{cases} \dfrac{a^2}{a^2 + b^2} \text{ if } a \neq 0 \\ 0 \text{ if } a = 0 \end{cases}$$

Then $c \in A$ so $a^3 = (a^2 + b^2)c \in \mathfrak{p}$, so $a \in \mathfrak{p}$. This proves $P \cap -P = \mathfrak{p}$. Thus P is an ordering with support $\mathfrak{p}$. In fact, it is the only ordering with support $\mathfrak{p}$: if Q is an ordering with support $\mathfrak{p}$, then $A^2 \subseteq Q$, $\mathfrak{p} \subseteq Q$ so $P = A^2 + \mathfrak{p} \subseteq Q$. If $a \in Q$, $a \notin P$, then $-a \in P \subseteq Q$, so $Q \cap -Q = \mathfrak{p} \subseteq P$, a contradiction.

Thus the natural mapping $Sper(A) \to Spec(A)$ is a bijection in this example.

Example 5.1.11. *The ring $\mathbb{Z}$ of integers is uniquely ordered. The unique ordering has support $\{0\}$ and corresponds to the unique ordering on $\mathbb{Q}$. The remaining residue fields are the finite fields $\mathbb{Z}_p$, p prime integer, and these have no orderings. Thus Sper($\mathbb{Z}$) is a singleton set.*

Example 5.1.12. *Suppose (X, G) is a space of orderings and W is the Witt ring of (X, G). Suppose $P \subseteq W$ is an ordering and $\mathfrak{p}$ is the support of P. If $a \in G$ then $a^2 = 1$ so*

$$\langle 1, -a\rangle \otimes \langle 1, a\rangle \cong \langle 1, a, -a, -1\rangle \sim 0 \in \mathfrak{p}.$$

Thus either $\langle 1, -a\rangle \in \mathfrak{p}$ or $\langle 1, a\rangle \in \mathfrak{p}$, i.e, $\langle a\rangle \equiv \pm 1$ mod $\mathfrak{p}$. Since the 1-dimensional forms generate W, this means $W/\mathfrak{p} \cong \mathbb{Z}$ or $\mathbb{Z}_p$ for some prime integer p. Since the finite field $\mathbb{Z}_p$ has no orderings, the second case is impossible, i.e, $W/\mathfrak{p}$ is the only possibility. By 4.1.21(ii), there is some unique $x \in X$ such that $\mathfrak{p} = \{\varphi \in W : \varphi(x) = 0\}$ and, since $\mathbb{Z}$ is uniquely ordered. $P = \{\varphi \in W : \varphi(x) \geq 0\}$. Thus the mapping

$$x \mapsto P_x := \{\varphi \in W : \varphi(x) \geq 0\}$$

defines a natural one-to-one correspondence between elements of X and orderings on W.

5.1.2 Constructible sets and semi-algebraic sets

The main motivation for studying the real spectrum comes from real algebraic geometry and model theory. We explain this now. Fix an ordered field (k, Q) and a real closed extension field R of (k, Q) (so $Q = R^2 \cap k$). We are interested in semi-algebraic sets in R^n defined over k (we define this terminology below).

Our first result is an consequence of Lang's homomorphism theorem:

Theorem 5.1.13. *Let $f_1, ..., f_k, g_1, ..., g_l \in k[t_1, ..., t_n]$ and suppose there exists an ordering $P \subseteq k[t_1, ..., t_n]$ with $Q \subseteq P$ such that $f_i \in P \setminus -P$, $i = 1, ..., k$ and $g_j \in P$, $j = 1, ..., l$. Then there exists $a \in R^n$ such that $f_i(a) > 0$, $i = 1, ..., k$ and $g_j(a) \geq 0$, $j = 1, ..., l$.*

We just state this theorem, because the proof involves Tarski's Transfer Principle, and this escapes of the escope of this work:

Theorem 5.1.14 (Lang's Homomorphism Theorem)**.** *Suppose (k, Q) is an ordered field with real closure R and suppose D is a finitely generated k-algebra which is an integral domain and that the ordering Q extends to an ordering in the quotient field of D in some way. Then*

i - There exists a k-algebra homomorphism $\varphi : D \to R$.

ii - More generally, if $a_1, ..., a_n \in D$ are positive in this extended ordering then there exists a k-algebra homomorphism $\varphi : D \to R$ such that $\varphi(a_1) > 0$, $i = 1, ..., n$.

Now, we proof our result:

Proof of Theorem 5.1.13. Let $\mathfrak{p} = P \cap -P$ and let $\overline{P}$ be the ordering on the residue field $k(\mathfrak{p})$ induced by P. By 5.1.14, we have a ring homomorphism

$$\gamma : k[t_1, ..., t_n]/\mathfrak{p} \to R$$

such that $\gamma(f_i + \mathfrak{p}) > 0$, $i = 1, ..., k$ and $\gamma(g_j + \mathfrak{p}) > 0$ for those j satisfying $g_j \in P \setminus -P$ (of course, $\gamma(g_j + \mathfrak{p} = 0$ if $g_j \in \mathfrak{p}$). Define $a = (a_1, ..., a_n)$ where $a_i = \gamma(t_i + \mathfrak{p})$. Then $\gamma(f + \mathfrak{p}) = f(a)$ for all $f \in k[t_1, ..., t_n]$. It follows that $f_i(a) > 0$, $i = 1, ..., k$ and $g_j(a) \geq 0$, $j = 1, ..., l$. □

Thus, we are interested in a certain part of the real spectrum of the polynomial ring $k[t_1, ..., t_n]$, namely, those orderings P on $k[t_1, ..., t_n]$ with $Q \subseteq P$. We denote this set by $\mathrm{Sper}_Q(k[t_1, ..., t_n])$. More generally, for any k-algebra A, we denote by $\mathrm{Sper}_Q(A)$ the set of all orderings P in A with $Q \subseteq P$. For $a \in R^n$, define

$$P_a := \{f \in k[t_1, ..., t_n] : f(a) \geq 0\}.$$

This is an ordering in $k[t_1, ..., t_n]$ and $Q \subseteq P_a$ so we have a mapping

$$\Phi : R^n \to \mathrm{Sper}_Q(k[t_1, ..., t_n])$$

given by $a \mapsto P_a$. The argument in example 5.1.9 shows that Φ is injective if $k = R$, but Φ is generally not injective. On the other hand, and this is an important point, 5.1.13 says that, for a certain natural topology on $\mathrm{Sper}_Q(k[t_1, ..., t_n])$, the image of R^n in $\mathrm{Sper}_Q(k[t_1, ..., t_n])$ is dense. When we describes this topology eventually, we need notation for various sorts of subsets of $\mathrm{Sper}_Q(A)$. We introduce this notation now. Namely, for $f \in A$, we define:

$$\begin{aligned} U(\overline{f}) &:= \{P \in \mathrm{Sper}_Q(A) : f \in P \setminus -P\} \\ Z(\overline{f}) &:= \mathrm{Sper}_Q(A) \setminus (U(\overline{f}) \cup U(-\overline{f})) = \{P \in \mathrm{Sper}_Q(A) : f \in P \cap -P\} \\ W(\overline{f}) &:= \mathrm{Sper}_Q(A) \setminus U(-\overline{f}) = U(\overline{f}) \cup Z(\overline{f}) = \{P \in \mathrm{Sper}_Q(A) : f \in P\} \end{aligned}$$

We explain the reason for the "bar" in the next section. Also, for $f_1, ..., f_k \in A$, we define:

$$\begin{aligned} U(\overline{f}_1, ..., \overline{f}_n) &:= \bigcap_{j=1}^{n} U(\overline{f}_j) \\ Z(\overline{f}_1, ..., \overline{f}_n) &:= \bigcap_{j=1}^{n} Z(\overline{f}_j) \\ W(\overline{f}_1, ..., \overline{f}_n) &:= \bigcap_{j=1}^{n} W(\overline{f}_j) \end{aligned}$$

A subset $C \subseteq \mathrm{Sper}_Q(A)$ is said to be **constructible** if it can be built up from the sets $U(\overline{f})$, $f \in A$ in a finite number of steps, by taking complements, finite intersections and finite unions. A subset of R^n is said to be **semi-algebraic** (defined over k) if it has the form $\Phi^{-1}(C)$ for some constructible $C \subseteq \mathrm{Sper}_Q(k[t_1, ..., t_n])$, i.e, if it can be built up from the sets $\Phi^{-1}(U(\overline{f}))$, $f \in k[t_1, ..., t_n]$ in a finite number of steps, by taking complements, finite intersections and finite unions.

Note that the sets $Z(\overline{f}), W(\overline{f})$ are constructible too. Beside this, for $f \in k[t_1, ..., t_n]$,

$$\begin{aligned} \Phi^{-1}(U(\overline{f})) &= \{a \in R^n : f(a) > 0\} \\ \Phi^{-1}(Z(\overline{f})) &= \{a \in R^n : f(a) = 0\} \\ \Phi^{-1}(W(\overline{f})) &= \{a \in R^n : f(a) < 0\} \end{aligned}$$

Any constructible set is expressible as a finite union of sets of the form

$$U(\overline{f}_1, ..., \overline{f}_k) \cap W(\overline{g}_1, ..., \overline{g}_l).$$

The proof just amounts to checking that sets of this form are closed under taking complements, finite intersections and finite unions. Consequently, any semi-algebraic set is expressible as a finite

union of sets of the form

$$\{a \in R^n : f_i(a) > 0,\ g_j(a) \geq 0,\ i = 1, ..., k,\ j = 1, ..., l\}$$

where $f_1, ..., f_k, g_1, ..., g_l \in k[t_1, ..., t_n]$.

Corollary 5.1.15. *The natural mapping $\Phi : R^n \to Sper_Q(k[t_1, ..., t_n])$ induces a one-to-one correspondence $C \mapsto \Phi^{-1}(C)$ between constructible sets in $Sper_Q(k[t_1, ..., t_n])$ and semi-algebraic sets in R^n.*

Proof. From 5.1.13 it follows that for any constructible set C, $C \neq \emptyset \Rightarrow \Phi^{-1}(C) \neq \emptyset$. Let C_1, C_2 be constructible, and let C be the constructible set defined by $C = (C_1 \setminus C_2) \cup (C_2 \setminus C_1)$. Then $C_1 = C_2 \Leftrightarrow C = \emptyset$, and similarly, $\Phi^{-1}(C_1) = \Phi^{-1}(C_2) \Leftrightarrow \Phi^{-1}(C)\emptyset$. Putting these together, we get $C_1 \neq C_2 \Rightarrow \Phi^{-1}(C_1) \neq \Phi^{-1}(C_2)$. □

We often use a "relative" version of 5.1.15. Let $\mathfrak{a} \subseteq k[t_1, ..., t_n]$ be an ideal and let $V(\mathfrak{a}) \subseteq R^n$ denote the zero set, i.e,

$$V(\mathfrak{a}) = \{a \in R^n : f(a) = 0 \text{ for all } f \in \mathfrak{a}\}.$$

By the Hilbert Basis Theorem, $\mathfrak{a}$ is finitely generated, so

$$V(\mathfrak{a}) = \{a \in R^n : f_i(a) = 0,\ i = 1, ..., m\}$$

where $f_1, ..., f_m$ are generators for $\mathfrak{a}$, i.e, $V(\mathfrak{a})$ is the semi-algebraic set in R^n corresponding to the constructible set $Z(\overline{f}_1, ..., \overline{f}_m)$ in $\mathrm{Sper}_Q(k[t_1, ..., t_n])$. On the other hand, the natural homomorphism

$$k[t_1, ..., t_n] \to k[t_1, ..., t_n]/\mathfrak{a}$$

identifies orderings in $\mathrm{Sper}_Q(k[t_1, ..., t_n]/\mathfrak{a})$ with orderings in $Z(\overline{f}_1, ..., \overline{f}_m)$. Thus we have the following immediate consequence of 5.1.15:

Corollary 5.1.16. *The natural mapping*

$$\Phi|_{V(\mathfrak{a})} : V(\mathfrak{a}) \to Sper_Q(k[t_1, ..., t_n]/\mathfrak{a})$$

induces a one-to-one correspondence between semi-algebraic sets in $V(\mathfrak{a})$ and constructible sets in $Sper_Q(k[t_1, ..., t_n]/\mathfrak{a})$.

There are some subtle points to the theory. R^n has a natural topology namely the product topology, where R is given the usual order topology. A subset $C \subseteq \mathrm{Sper}_Q(A)$ is said to be **open constructible (resp. closed constructible)** if C is expressible as a finite union of the sets of the form $U(\overline{f}_1, ..., f_k)$ (resp. of the form $U(\overline{f}_1, ..., f_k)$. The topological meaning of this terminology will be made clear later.

5.1.3 Nullstellensatz and Positivstellensatz

We work relative to a fixed preordering in a ring A. We are trying to generalize what we did in the field case for AOS, as in section 4.1. If $T \subseteq A$ is any preordering, X_T denotes the set of all orderings of A lying over T, i.e,

$$X_T = \{P \in \mathrm{Sper}(A) : P \supseteq T\}.$$

We consider the subset $\{-1,0,1\} \subseteq \mathbb{Z}$ viewed as a monoid, with multiplication as the operation. For any set X, $\{-1,0,1\}^X$ denotes the set of all functions $a : X \to \{-1,0,1\}$. Thus $\{-1,0,1\}^X$ is a monoid with operation given by $(ab)(x) = a(x)b(x)$. For $a, b\{-1,0,1\}^X$,

i - If $a(x) = 0 \Rightarrow b(x) = 0$ for all $x \in X$, then $b = a^2b$, and conversely.

ii - $a^3 = a$, $a^4 = a^2$, etc.

iii - If $a(x) \geq 0$ for all $x \in X$ then $a = a^2$, and conversely.

iv - If $a(x) \neq 0$ for all $x \in X$, then $a^2 = 1$, and conversely.

We denote the constant functions in $\{-1,0,1\}^X$ by $-1, 0, 1$. For any submonoid $G \subseteq \{-1,0,1\}^X$ containing $-1, 0, 1$, $\dot{G}$ denote the multiplicative group of the monoid G (also called the unit group), i.e,

$$\dot{G} := \{a \in G : \text{ there exists } b \in G \text{ such that } ab = 1\} = \{a \in G : a^2 = 1\}.$$

G^2 denotes the set of idempotents of G, i.e,

$$G^2 = \{a \in G : a^2 = a\} = \{a \in G : a(x) \geq 0 \text{ for all } x \in X\} = \{a^2 : a \in G\}.$$

Let T be a proper preordering in the ring A, i.e, $-1 \notin T$. We know by 5.1.3 that $X_T \neq \emptyset$. Each $a \in A$ defines a function $\overline{a} = \overline{a}_T : X_T \to \{-1,0,1\}$ given by

$$\overline{a}(P) = \begin{cases} 1 \text{ if } a \in P \setminus -P \\ 0 \text{ if } a \in P \cap -P \\ -1 \text{ if } a \in -P \setminus P \end{cases}$$

Let $G_T = \{\overline{a} : a \in A\}$. Since $\overline{ab} = \overline{a} \cdot \overline{b}$, G_T is a submonoid of $\{-1,0,1\}^{X_T}$ that contains the constant functions $-1, 0, 1$.

Theorem 5.1.17. *Suppose T is a proper preordering on a field k. Then $G_T = G_T^* \cup \{0\}$ and G_T^* is naturally isomorphic to $\dot{k}/\dot{T}$. Here, $\dot{k} = k \setminus \{0\}$, $\dot{T} := T \setminus \{0\}$.*

Proof. Since orderings in k have support $\{0\}$, $G_T = \dot{G}_T \cup \{0\}$. By 4.1.10, the mapping $a\dot{T} \mapsto \overline{a}$ defines an isomorphism from $\dot{k}/\dot{T}$ onto $\dot{G}_T$. □

Observe that what was denoted by G_T in 4.1 is now being denoted by $\dot{G}_T$.

If $\alpha : A \to B$ is a ring homomorphism and T, S are preorderings in A and B respectively with $\alpha(T) \subseteq S$, then we have an induced mapping $\alpha^* : X_S \to X_T$ given by $P \mapsto \alpha^{-1}(P)$ and an induced mapping $\alpha_* : G_T \to G_S$ is given by $\overline{a}_T \mapsto \overline{\alpha(a)}_S$. Observe that $\alpha_*(\overline{a}_T) = \overline{a}_T \circ \alpha^*$ where $\circ$ denotes composition.

Example 5.1.18.

*a- Commonly, we start with T as given and take $S = \sum \alpha(T)B^2$, the set of all finite sums $\sum \alpha(t_i)b_i^2$, $t_i \in T$, $b_i \in B$. This is called the **preordering in B induced by** T (note that if $T = \sum A^2$, then $S = \sum B^2$). Or, we start with $B = A$, $\alpha =$ the identity mapping, S, T preorderings of A with $T \subseteq S$, to get the inclusion $\alpha^* : X_S \subseteq X_T$ and the restriction $\alpha_* : G_T \to G_S$.*

b- If $\mathfrak{a} \subseteq A$ is an ideal and $T \subseteq A$ is a preordering, then $T + \mathfrak{a}$ is a preordering. The induced preordering on $A/\mathfrak{a}$ is

$$T/\mathfrak{a} := (T + \mathfrak{a})/\mathfrak{a} = \{t + \mathfrak{a} : t \in T\}.$$

The mapping $X_{T/\mathfrak{a}} \to X_T$ corresponding to $A \to A/\mathfrak{a}$ is injective (since $G_T \to G_{T/\mathfrak{a}}$ is surjective) and it identifies $X_{T/\mathfrak{a}}$ with the Zariski-closed set

$$X_{T+\mathfrak{a}} = \{P \in X_T : \overline{a}_T(P) = 0 \text{ for all } a \in \mathfrak{a}\}$$

in X_T.

c- *Suppose $S \subseteq A$ is any multiplicative set and $T \subseteq A$ is a preordering. The preordering on $S^{-1}(A)$ induced by T is*

$$S^{-2}(T) := \{t/s^2 : t \in T,\, s \in S\}.$$

An ordering P on A with support $\mathfrak{p}$ extends to an ordering on the localization $S^{-1}(A)$ iff $\mathfrak{p} \cap S = \emptyset$. The unique extension on P to $S^{-1}(A)$ is $S^{-2}P$. The mapping $X_{S^{-2}(T)} \to X_T$ corresponding to $A \to S^{-1}(A)$ indentifies $X_{S^{-2}(T)}$ with

$$\{P \in X_T : \overline{a}_T(P) \neq 0 \text{ for all } a \in S\}.$$

Note that $\overline{(a/s)}_{S^{-2}(T)} = \overline{(as)}_{S^{-2}(T)}$, so $G_T \to G_{S^{-2}(T)}$ is surjective.

Paraphrasing M. Marshall ([Mar96], pg 93):

> *"It is important to realize that, in replacing A by G_T, we are already in deep water."*

For $a, b \in A$, what does the statement $\overline{a}_T = \overline{b}_T$ really means? By 5.1.17, we know the answer in the field case. In general, using 5.1.3, we have the following:

Theorem 5.1.19. *Suppose T is a preordering in A. Then*

i - $\overline{a}_T = 0$ *iff* $-a^{2k} \in T$ *for some integer* $k \geq 0$.

ii - $\overline{a}_T = 1$ *iff* $(1+s)a = 1+t$ *for some* $s, t \in T$.

iii - $\overline{a}_T \geq 0$ *iff* $(a^{2k}+s)a = a^{2k}+t$ *for some* $s, t \in T$ *and some* $k \geq 0$.

These results are abstract versions of results in real algebraic geometry: the real Nullstellensatz of Dubois and Risler and the real Positivstellensatz of Stengle.

Proof of Theorem 5.1.19.

i - ($\Rightarrow$) Go to the localization

$$A[1/a] := \{b/a^k : b \in A,\, k \geq 0\},$$

the localization of A at the multiplicative set $\{a^k : k \geq 0\}$, and the induced preordering

$$T[1/a^2] := \{t/a^{2k} : t \in T,\, k \geq 0\}$$

in $A[1/a]$. If $\overline{a} = 0$ then $X_{T[1/a^2]} = \emptyset$ and $-1 \in T[1/a^2]$ so $-1 = t/s^2$ for some $s \in T$, $k \geq 0$. Clearing fractions by multiplying by $a^{2(k+l)}$, $l \geq 0$ sufficiently large, we obtain $-a^{2(k+l)} = sa^{2l} \in T$.

($\Leftarrow$) If $-a^{2k} \in T$ for some $k \geq 0$, then $-a^{2k} \in T \cap -T \subseteq P \cap -P$ for all $P \in X_T$ (since $A^2 \subseteq T$). Hence $\overline{-a^{2k}}_T = 0$, and this implies $\overline{a} = 0$ (because if $\overline{a}_T \neq 0$, then $\overline{a}_T^2 = 1$).

ii - ($\Rightarrow$) Go to the preordering $T-aT$ in A. Then $X_{T-aT}=\emptyset$ so $-1\in T-aT$. Also $1-a\in T-aT$ and $T-aT$ is closed under multiplication so $-(1-a)=t-sa$, i.e, $(1+s)a=1+t$ for some $s,t\in T$.

($\Leftarrow$) Follow by definition of $\overline{a}$.

iii - ($\Rightarrow$) Go to preordering $T[1/a^2]$ in the localization $A[1/a^2]$ and apply (ii) to get $(1+s')a=1+t'$ for some $s',t'\in T[1/a^2]$, say $s'=s/2^{2k}$, $t'=t/a^{2l}$, $s,t\in T$. Clearing fractions, this yields

$$(a^{2(k+l)}+sa^{2l})a=a^{2(k+l)}+ta^{2l}$$

for some integer $l\geq 0$.

($\Leftarrow$) Follow by definition of $\overline{a}$ (if necessary, use itens (i) and (ii)!).

□

Corollary 5.1.20. *$\overline{a}_T=\overline{b}_T$ iff $sab=(a^2+b^2)^k+l$ for some $s,t\in T$ and some $k\geq 0$.*

Proof. ($\Rightarrow$) Go to the localization $A[1/a^2+b^2]$ and the induced preordering $T[1/a^2+b^2]$ in $A[1/a^2+b^2]$. Since $\overline{a}_T=\overline{b}_T$ on X_T, it follows that $\overline{a}_T\overline{b}_T=1$ on $X_{T[1/a^2+b^2]}$ so, by 5.1.19(ii), $s'ab=1+t'$ for some $s',t'\in T[1/a^2+b^2]$. Clearing fractions by multiplying by $(a^2+b^2)^k$, k sufficiently large, yields what we want.

($\Leftarrow$) Follow by definition of $\overline{a}$. □

Suppose we are in the set up of section 5.1.2, $\mathfrak{a}\subseteq k[t_1,...,t_n]$ is an ideal, and $T:=\sum k[t_1,...,t_n]^2Q$. Then $\mathrm{Sper}_Q(k[t_1,...,t_n])=X_T$, and the constructible set in $\mathrm{Sper}_Q(k[t_1,...,t_n])$ corresponding to $V(\mathfrak{a})$ is

$$\mathrm{Sper}_Q\,(k[t_1,...,t_n]/\mathfrak{a})=\{P\in X_T:\overline{a}_T(P)=0\text{ for all }a\in\mathfrak{a}\}=X_{T+\mathfrak{a}}.$$

Thus, combining 5.1.16 and 5.1.19(i), we see that, for any $f\in k[t_1,...,t_n]$, $f=0$ on $V(\mathfrak{a})$ iff $-f^{2k}\in T+\mathfrak{a}$ for some $k\geq 0$. Parts (ii) and (iii) of 5.1.19 have similar concrete interpretations in this special case.

There are several equivalent ways of expressing the condition $\overline{a}_T=\overline{1}$. Multiplying both sides of $(1+s)a=1+t$ by $(1+s)$, we get $ab^2=1+t'$ for some $b\in A$ and some $t'\in T$. This implies $as'=1+t'$ for some $s',t'\in T$. Finally, if the latter holds, then $\overline{a}_T=\overline{1}$, so all these conditions are equivalent. Similarly, there are several equivalent ways of expressing the condition $\overline{a}_T\geq 0$.

If T is a preordering in a field k, the situation in 5.1.19 simplifies drastically: $\overline{a}_T=0$ just means $a=0$, $\overline{a}_T=1$ just means $a\in\dot{T}$, and $\overline{a}_T\geq 0$ just means $a\in T$. This is immediate from the proof of 5.1.17.

5.1.4 Value Sets of quadratic forms

We continue to assume that T is a proper preordering in a ring A. We introduce quadratic form terminology as in the field case. A **(quadratic) form of dimension** n with entries in G_T is just an n-tuple $\varphi=(\overline{a}_1,...,\overline{a}_n)$, $a_1,...,a_n\in A$. The **discriminant** of φ is $\prod_{j=1}^n\overline{a}_j\in G_T$. The **signature** of φ at $P\in X_T$ is

$$\varphi(P):=\sum_{j=1}^n\overline{a}_j(P)\in\mathbb{Z}.$$

We write $\varphi\cong\psi$ (read φ is **isometric** to ψ) to indicate that φ and ψ have the same dimension and the same signature at each $P\in X_T$.

From the reduced theory of quadratic forms developed in chapter 2 we know isometry and value sets are well-behaved in the field case. In the ring case, the isometry relation is not very well-behaved. On the other hand, we do have reasonably good results concerning value sets. We define the **value set** of $\varphi = \langle \overline{a}_1, ..., \overline{a}_n \rangle$ to be

$$D(\varphi) = D(\overline{a}_1, ..., \overline{a}_n) := \{\overline{b} : b \in Ta_1 + ... + Ta_n\}.$$

We say $\overline{b}$ is represented by φ if $\overline{b} \in D(\varphi)$. Note that we are including $\overline{0}$ in the value sets now. In AOS case, $\overline{0}$ was specifically excluded.

Proposition 5.1.21.

i - $D(\overline{a}) = \{\overline{t}\overline{a} : t \in A, \overline{t} \geq 0\} = \{\overline{b} : \overline{b}^2\overline{a} = \overline{b}\}$
$= \{\overline{b} : \textit{for each } P \in X_T \textit{ either } \overline{b}(P) = 0 \textit{ or } \overline{a}(P)\overline{b}(P) > 0\}.$

ii - $D(\overline{a}, \overline{b}) = \{\overline{c} : \langle \overline{a}\overline{c}^2, \overline{b}\overline{c}^2 \rangle \cong \langle \overline{c}, \overline{a}\overline{b}, \overline{c} \rangle\} =$
$\{\overline{c} : \textit{for each } P \in X_T, \textit{ either } \overline{c}(P) = 0 \textit{ or } \overline{a}(P)\overline{c}(P) > 0 \textit{ or } \overline{b}(P)\overline{c}(P) > 0\}.$

iii - *If* $n \geq 3$, $D(\overline{a}_1, ..., \overline{a}_n) = \bigcup_{\overline{c} \in D(\overline{a}_2, ..., \overline{a}_n)} D(\overline{a}_1, \overline{c})$.

iv - $D(\overline{a}_1, ..., \overline{a}_n)$ *depends only on* $\overline{a}_1, ..., \overline{a}_n$ *(not on the particular representatives* $a_1, ..., a_n$*).*

v - $\overline{b} \in D\langle \overline{a}_1, ..., \overline{a}_n \rangle$ *iff* $t_0 b = \sum_{i=1}^n t_i a_i$ *for some* $t_0, ..., t_n \in T$ *with* $\overline{t}_0\overline{b} = \overline{b}$.

Proof.

i - Follow by calculations with the definition of D.

ii - Comparing the signatures of $\langle \overline{a}\overline{c}^2, \overline{b}, \overline{c}^2 \rangle$ and $\langle \overline{c}, \overline{a}\overline{b}\overline{c} \rangle$ we obtain the equality between the second and third set. If $c = t_1 a + t_2 b$, $t_1, t_2 \in T$, then $c^2 = t_1 ac + t_2 bc$. From this, we obtain the inclusion of the first set in the third. To prove the inclusion of the third set in the first, pick $c \in A$ such that $\overline{c}$ belongs to the third set. Go to the preordering $T' = T[1/c^2]$ in the localization $A' = A[1/c]$. Let $a' = ac$, $b' = bc$. On $X_{T'-a'T'}$, $b' > 0$, so by 5.1.19(ii), $(1+s)b' = 1 + t$ for some $s, t \in T' - a'T'$. Thus

$$(1+s)^2 b' = (1+s)(1+t) = 1 + u$$

for some $u \in T' - a'T'$, say $u = t_0 - t_1 a'$, $t_0, t_1 \in T'$, so $1 + t_0 = t_1 a' + t_2 b'$ where $t_2 = (1+s)^2$. Multiplying by c^{2m+1}, m sufficiently large, we get

$$c_1 := (c^{2m} + s_0)c = s_1 a + s_2 b,\ s_0, s_1, s_2 \in T.$$

Since $\overline{c}_1 = \overline{c}$, this completes the proof.

iii - Let

$$\overline{x} \in \bigcup_{\overline{c} \in D(\overline{a}_2, ..., \overline{a}_n)} D(\overline{a}_1, \overline{c}).$$

Then $\overline{x} \in D(\overline{a}_1, \overline{c})$ for some $\overline{c} \in D(\overline{a}_2, ..., \overline{a}_n)$, and hence $x = t_1 a_1 + t_0 c$, $c = t_2 a_2 + ... + t_n a_n$, $t_j \in T$, $j = 0, ..., n$. So, $x = t_1 a_1 + t_0 t_2 a_2 + ... + t_0 t_n a_n$, and by definition of D, $\overline{x} \in D(\overline{a}_1, \overline{a}_2, ..., \overline{a}_n)$. Conversely, if $\overline{x} \in D(\overline{a}_1, \overline{a}_2, ..., \overline{a}_n)$, say $x = t_1 a_1 + ... + t_n a_n$, $t_j \in T$, $j = 1, ..., n$. Taking $c := t_2 a_2 + ... + t_n a_n$, we have $x = t_1 a_1 + 1c$, and $\overline{c} \in D(\overline{a}_2, ..., \overline{a}_n)$, so

$$\overline{x} \in \bigcup_{\overline{c} \in D(\overline{a}_2, ..., \overline{a}_n)} D(\overline{a}_1, \overline{c}).$$

iv - This is true when $n = 1$ or 2 using (i) and (ii). For $n \geq 3$, it follows by induction on n, using (iii).

v - ($\Leftarrow$) is just the definition of D. For ($\Rightarrow$), suppose $\overline{b} \in D(\overline{a}_1, ..., \overline{a}_n)$. Then by definition, there exists b' and $s_1, ..., s_n \in T$ such that $b' = \sum_{i=1}^n s_i a_i$ and $\overline{b} = \overline{b}'$. By 5.1.20,

$$sbb' = (b^2 + b'^2)^k + t \text{ for some } s, t \in T \text{ and some } k \geq 0.$$

Then

$$((b^2 + b'^2)^k + t)b = sb^2b' = \sum_{i=1}^n sb^2 s_i a_i$$

so $t_0 b = \sum_{i=1}^n t_i a_i$ where $t_0 = (b^2 + b'^2)^k + t$ and $t_i = sb^2 s_i$, $i = 1, ..., n$.

□

It is important to realize that value sets are not preserved by isometry. For example,

$$\langle \overline{1}, -\overline{1} \rangle \cong \langle \overline{0}, \overline{0} \rangle,\ D(\overline{1}, -\overline{1}) = G_T,\ D(\overline{0}, \overline{0}) = \{\overline{0}\}.$$

The reader will also note that 5.1.21 is more complicated than the corresponding result in the field case. In the ring case, the situation is further complicated by the fact that there are two sorts of value sets, both important. We denote the second sort of value set by $D^t(\overline{a}_1, ..., \overline{a}_n)$ and refer to it as the **transversal value set** of $\langle \overline{a}_1, ..., \overline{a}_n \rangle$. This is defined to be the set of all $\overline{b} \in G_T$ such that there exists $b', a'_1, ..., a'_n \in A$ such that $\overline{b} = \overline{b}'$, $\overline{a}_i = \overline{a}'_i$, $i = 1, ..., n$, and $b' = \sum_{j=1}^n a'_j$. We say $\overline{b}$ is **transversally represented by** $\langle \overline{a}_1, ..., \overline{a}_n \rangle$ if $\overline{b} \in D^t(\overline{a}_1, ..., \overline{a}_n)$.

The multiplication on G_T satisfies $\overline{a}\overline{b} = \overline{ab}$, i.e, it is just the operation on G_T induced by multiplication on A. On the other hand, the addition $\overline{a} + \overline{b} = \overline{a + b}$ is not well-defined. The outcome of adding in G_T is not a single element, but rather is the set of elements $D^t(\overline{a}, \overline{b})$. Thus, in studying transversal values sets, we are just studying what remains of the addition when we pass from A to G_T.

Since we know $D(\overline{a}_1, ..., \overline{a}_n)$, we have $D^t(\overline{a}_1, ..., \overline{a}_n) \subseteq D(\overline{a}_1, ..., \overline{a}_n)$.

Proposition 5.1.22. *The following are equivalent:*

a - $\overline{b} \in D\langle \overline{a}_1, ..., \overline{a}_n \rangle$.

b - $\overline{b} \in D^t\langle \overline{b}^2\overline{a}_1, ..., \overline{b}^2\overline{a}_n \rangle$.

c - $\overline{b} \in D(\overline{t}_1\overline{a}_1, ..., \overline{t}_n\overline{a}_n)$ *for some* $t_1, ..., t_n \in T$.

Proof. (a)⇒(b): We can suppose $b = \sum_{i=1}^n t_i a_i$ for some $t_1, ..., t_n \in T$. Go to the localization $A[1/2b]$. $1/2 = b/2b$ and $1/b = 2/2b$ belong to $A[1/2b]$. Using the identity $p = (p+1)^2/2 - (p-1)^2/2$, we get

$$\frac{a_1 + ... + a_n}{b} = r^2 - s^2 = (1 + r^2) - (1 + s^2)$$

for some $r, s \in A[1/2b]$. Thus

$$(1 + r^2)b = a_1 + ... + a_n + (1 + s^2)b = \sum_{i=1}^n (1 + (1 + s^2)t_i)a_i$$

in $A[1/2b]$. Multiplying each side by $4^k b^k$ sufficiently large, to clear fractions, this yields an equation

$$t'_0 b = t'_1 a_1 + ... + t'_n a_n$$

in A, with $t'_0, ..., t'_n \in T$, $\overline{t}'_i = \overline{b}^2$, $i = 0, ..., n$. Since $\overline{b}^3 = \overline{b}$, this means $\overline{b} \in D^t(\overline{b}^2\overline{a}_1, ..., \overline{b}^2\overline{a}_n)$.

(b)⇒(c): Take $\overline{t}_i = \overline{b}^2$.

(c)⇒(a): Follow from

$$D^t(\overline{t}_1\overline{a}_1, ..., \overline{t}_n\overline{a}_n) \subseteq D(\overline{t}\overline{a}_1, ..., \overline{t}_n\overline{a}_n) \subseteq D(\overline{a}_1, ..., \overline{a}_n).$$

□

Suppose T is a preordering in a field F and $a_1, ..., a_n \in \dot{F}$. If $b \in F$, $b \neq 0$, then $\overline{b}^2 = 1$ so by 5.1.22,

$$\overline{b} \in D(\overline{a}_1, ..., \overline{a}_n) \Leftrightarrow \overline{b} \in D^t(\overline{a}_1, ..., \overline{a}_n),$$

i.e, $D(\overline{a}_1, ..., \overline{a}_n), D^t(\overline{a}_1, ..., \overline{a}_n)$ have the same non-zero elements.

5.1.22 gives a description of value sets in terms of transversal value sets. The next result reverses the process, describing transversal value sets in terms of value sets.

Proposition 5.1.23. *The following are equivalent:*

a - $\overline{b} \in D^t(\overline{a}_1, ..., \overline{a}_n)$.

b - $\overline{b} \in D(\overline{a}_1, ..., \overline{a}_n)$ *and* $-\overline{a}_i \in D(\overline{a}_1, ..., \overline{a}_{i-1}, -\overline{b}, \overline{a}_{i+1}..., \overline{a}_n)$, $i = 1, ..., n$.

Proof. (a)⇒(b): We can assume $b = \sum_{i=1}^n a_i$. Then $\overline{b} \in D(\overline{a}_1, ..., \overline{a}_n)$ and

$$-a_i = a_1 + ... + a_{i-1} - b + a_{i+1} + ... + a_n,$$

so $-\overline{a}_i \in D(\overline{a}_1, ..., \overline{a}_{i-1}, -\overline{b}, \overline{a}_{i+1}, ..., \overline{a}_n)$, $i = 1, ..., n$.

(b)⇒(a): By 5.1.21(v), we get $n + 1$ equations $t_{0j}b = \sum_{i=1}^n t_{ij}a_i$, $j = 0, ..., n$ with $t_{ij} \in T$, $\overline{t_{00}}\overline{b} = \overline{b}$, and $\overline{t_{ii}}\overline{a}_i = \overline{a}_i$, $i = 1, ..., n$. Adding these yields an equation

$$b' = \sum_{i=1}^n a'_i \text{ where } b' = \sum_{j=0}^n t_{0j}b,\ a'_i = \sum_{j=0}^n t_{ij}a_i.$$

Then $\overline{b'} = \overline{b}$ and $\overline{a'} = \overline{a}_i$, $i = 1, ..., n$ so $\overline{b} \in D^t(\overline{a}_1, ..., \overline{a}_n)$. □

Proposition 5.1.24.

a - $D^t(\overline{a}) = \{\overline{a}\}$.

b - $D^t(\overline{a}, \overline{b}) = \{\overline{c} : \langle \overline{a}, \overline{b} \rangle \cong \langle \overline{c}, \overline{a}\overline{b}\overline{c} \}$.

c - *If* $n \geq 3$ *then* $D^t(\overline{a}_1, ..., \overline{a}_n) = \bigcup_{\overline{c} \in D^t(\overline{a}_2, ..., \overline{a}_n)} D^t(\overline{a}, \overline{c})$.

Proof.

a - Follow from definition.

b - Suppose $\overline{c} \in D^t(\overline{a}, \overline{b})$. We can suppose $c = a + b$. Then

$$\overline{a}(P) + \overline{b}(P) = \overline{c}(P) + \overline{a}(P)\overline{b}(P)\overline{c}(P) \text{ for each } P \in X_T.$$

For the other inclusion, suppose $\langle \overline{a}, \overline{b} \rangle \cong \langle \overline{c}, \overline{a}\overline{b}\overline{c} \rangle$. Using 5.1.21(b), we see that $\overline{c} \in D(\overline{a}, \overline{b})$ and also that $-\overline{a} \in D(-\overline{c}, \overline{b})$ and $-\overline{b} \in D(\overline{a}, \overline{c})$. Thus, by 5.1.23, $\overline{c} \in D^t(\overline{a}, \overline{b})$.

c - Suppose $\overline{b} \in D^t(\overline{a}_1, ..., \overline{a}_n)$. We may as well suppose $b = \sum_{i=1}^n a_i$. Then $\overline{b} \in D^t(\overline{a}, \overline{c})$ and $\overline{c} \in D^t(\overline{a}_2, ..., \overline{a}_n)$ where $c := \sum_{i=2}^n a_i$. Now suppose $\overline{b} \in D^t(\overline{a}_1, \overline{c})$, $\overline{c} \in D^t(\overline{a}_2, ..., \overline{a}_n)$. Then $\overline{b} \in D(\overline{a}_1, \overline{c})$, $-\overline{a}_1 \in D(\overline{b}, \overline{c})$, $\overline{c} \in D(\overline{a}_2, ..., \overline{a}_n)$ so $\overline{b} \in D(\overline{a}_1, ..., \overline{a}_n)$ and $-\overline{a}_1 \in D(-\overline{b}, \overline{a}_2, ..., \overline{a}_n)$. Also $-\overline{a}_2 \in D(-\overline{c}, \overline{a}_3, ..., \overline{a}_n)$ and $-\overline{c} \in D(\overline{a}_1, -\overline{b})$ so $-\overline{a}_2 \in D(\overline{a}_1, -\overline{b}, \overline{a}_3, ..., \overline{a}_n)$. Similarly, $-\overline{a}_i \in D(\overline{a}_1, ..., \overline{a}_{i-1}, \overline{b}, \overline{a}_{i+1}, ..., \overline{a}_n)$, $i = 3, ..., n$. By 5.1.23, this means $\overline{b} \in D^t(\overline{a}_1, ..., \overline{a}_n)$.

□

5.1.5 Axioms for abstract real spectra

Recall that for any set X, $\{-1, 0, 1\}^X$ denotes the set of all function $a : X \to \{-1, 0, 1\}$. This is a monoid with operation given by $(ab)(x) = a(x)b(x)$.

Definition 5.1.25 (Abstract Real Spectra)**.** *An abstract real spectrum or space of signs, abreviatted to ARS, is a pair (X, G) satisfying:*

AX1 - *X is a non-empty set, G is a submonoid of $\{-1, 0, 1\}^X$, G contais the constants functions $-1, 0, 1$, and G separates points in X.*

If $a, b \in G$, the value set $D(a, b)$ is defined to be the set of all $c \in G$ such that, for all $x \in X$, either $a(x)c(x) > 0$ or $b(x)c(x) > 0$ or $c(x) = 0$. The value set $D^t(a, b)$ is defined to be the set of all $c \in G$ such that, for all $x \in X$, either $a(x)c(x) > 0$ or $b(x)c(x) > 0$ or $c(x) = 0$ and $b(x) = -a(x)$. Note that $c \in D^t(a, b) \Rightarrow c \in D(a, b)$. Conversely, $c \in D(a, b) \Rightarrow c \in D^t(ac^2, bc^2)$.

AX2 - *If P is a submonoid of G satisfying $P \cup -P = G$, $-1 \notin P$, $a, b \in P \Rightarrow D(a, b) \subseteq P$ and $ab \in P \cap -P \Rightarrow a \in P \cap -P$ or $b \in P \cap -P$, then there exists $x \in X$ (necessarily unique) such that $P = \{a \in G : a(x) \leq 0\}$.*

AX3a (Weak Associativity) - *For all $a, b, c \in G$, if $p \in D(a, r)$ for some $q \in D(b, c)$ then $p \in D(r, c)$ for some $r \in D(a, b)$.*

AX3b - *For all $a, b \in G$, $D^t(a, b) \neq \emptyset$.*

We hasten to point out that AX3a and AX3b combined are equivalent to the simgle axiom AX3 below:

AX3 (Strong Associativity) - *For all $a, b, c \in G$, if $p \in D^t(a, r)$ for some $q \in D^t(b, c)$ then $p \in D^t(r, c)$ for some $r \in D^t(a, b)$.*

We begin immediately by checking the easy half of this:

Proposition 5.1.26. *AX3 $\Rightarrow$ AX3a and AX3b.*

Proof. Suppose $b \in D(a_1, c)$ for some $c \in D(a_2, a_3)$. Then $b \in D^t(b^2a_1, b^2c)$, and $c \in D^t(c_2a_2, c^2a_3)$ (so $b^2c \in D^t(b^2c^2a_2, b^2c^2a_3)$). By AX3, this implies $b \in D^t(d, b^2c^2a_3)$ for some $d \in D^t(b^2a_1, b^2c^2a_2)$. Since $D^t(b^2a_1, b^2c^2a_2) \subseteq D(b^2a_1, b^2c^2a_2) \subseteq D(a_1, a_2)$ and $D^t(d, b^2c^2a_3) \subseteq D(d, b^2c^2a_3) \subseteq D(d, a_3)$, this complete the proof of AX3a.

For AX3b just note that $1 \in D^t(a, 1)$ and $1 \in D^t(b, 1)$, so by AX3, $1 \in D^t(d, 1)$ for some $d \in D^t(a, b)$. □

AX3 is certainly very natural and elegant and is the desirable axiom to use from this point of view. We use AX3a and AX3b because they seem to be easier to check than AX3. The reader will already have some feeling for why this is so from the proofs in last section. It is also reflected in the fact that the proof of the convers of 5.1.26 is quite difficult.

We prove the converse of 5.1.26 later. For now we concentrate on more elementary results. We begin with our main example.

Theorem 5.1.27. *If T is a proper preordering on a ring A, then the pair (X_T, G_T) is an abstract real spectrum.*

Proof. AX1 is immediate from definitions involved. For AX2, suppose $\overline{P}$ is a submonoid of G_T satisfying the hypothesis of AX2. Let $P = \{a \in A : \overline{a} \in \overline{P}\}$. If $t \in T$, then $\overline{t} = \overline{t}^2 \in \overline{P}$. This proves $T \subseteq P$. $PP \subseteq P$ and, since $\overline{a+b} \in D^t(\overline{a}, \overline{b})$, $P + P \subseteq P$. Also, $P \cup P = A$ and $P \cap -P$ is a prime ideal, so P is an ordering. Since $\overline{P} = \{\overline{a} \in G_T : \overline{a}(P) \geq 0\}$, this complete the proof. AX3a is immediate from description of value sets given in last section and 5.1.21. Of couser, AX3b is immediate using the fact that $\overline{a+b} \in D^t(\overline{a}, \overline{b})$. □

Just as in the case of space of orderings, AX1 and AX2 are trivial in the sense that they can be forced in a natural way: suppose X is any non-empty set and G is any submonoid of $\{-1, 0, 1\}^X$ containing the constant functions. First identify points in X which are not separated by elements of G and then add in the extra points required by AX2. The binary value sets $D(a, b)$, $D^t(a, b)$ are not changed by this process.

Just as we allow the zero ring in ring theory, it is sometimes convenient to allow the trivial abstract real spectrum, obtained by taking $X = \emptyset$ and $G = \{0\}$ (so $-1 = 0 = 1$ in G). If T is a preordering in a ring A and T is not proper, then (X_T, G_T) is the trivial abstract real spectrum.

Let (X, G) be an abstract real spectrum. Elements of X are sometimes referred to as **orderings**. The **positive cone** of $x \in X$ is

$$P_x := \{a \in G : a(x) \geq 0\}.$$

For $x \in X$, the **support** of x is

$$\mathfrak{p}_x = P_x \cap -P_x = \{a \in G : a(x) = 0\}.$$

$\mathrm{Supp}(X)$ denotes the set $\{\mathfrak{p}_x : x \in X\}$. We have a natural mapping

$$X \to \mathrm{Supp}(X) \text{ given by } x \mapsto \mathfrak{p}_x.$$

Recall that G^* denotes the unit group of the monoid G, i.e,

$$G^* = \{a \in G : ab = 1 \text{ for some } b \in G\} = \{a \in G : a^2 = 1\},$$

and G^2 denotes the set of idempotents, i.e,

$$G^2 = \{a^2 : a \in G\} = \{a \in G : a(x) \geq 0 \text{ for all } x \in X\}.$$

It is important to understand the relationship between spaces of orderings and abstract real spectra:

Proposition 5.1.28. *For any abstract real spectrum (X, G), the following are equivalent:*

a - All $x \in X$ have the same support ($= \{0\}$).

b - $G = G^* \cup \{0\}$.

c - $G^2 = \{0, 1\}$.

Proof. (a)⇒(b): suppose $\mathfrak{p}_x = \mathfrak{p}_y$ for all $x \in X$. Then for any $a \in \mathfrak{p}_x$, $a(y) = 0$ for all $y \in X$ so $a = 0$. In other words, if $a \neq 0$, then $a(x) \neq 0$ for all $x \in X$, so $a \in G^*$.

(b)⇒(c): is immediate.

(c)⇒(a): if $a \neq 0$ then $a^2 = 1$ so $a \in G^*$ so $a(x) \neq 0$ for each $x \in X$. This means $\mathfrak{p}_x = \{0\}$ for each $x \in X$. □

It is not necessary to distinguish between a space of orderings and an abstract real spectrum with $G = G^* \cup \{0\}$. This is the content of the next result.

Proposition 5.1.29. *If (X, G) is an abstract real spectrum with $G = G^* \cup \{0\}$, then (X, G^*) is a space of orderings. Conversely, if (X, G^*) is a space of orderings then we obtain an abstract real spectrum (X, G) with $G = G^* \cup \{0\}$ by adjoining 0 to G^*.*

Proof. (⇒) We want to show that AX1, AX2 and AX3 for (X, G^*) as an AOS are consequence of AX1, AX2, AX3a and AX3b for (X, G) (as an ARS). AX1 is immediate. AX2: suppose x is a character on G^* satisfying the hypothesis of AX2 for (X, G^*). Then $P = \ker(x) \cup \{0\}$ satisfies the hypothesis of AX2 for (X, G). Thus, by AX2 for (X, G), we have $y \in X$ satisfying $P = P_y$ and y viewed as a character on G^* is equal to x. AX3: suppose $a_1, a_2, a_3 \in G^*$ and $b \in D(a_1, c)$ for some $c \in D(a_2, a_3)$, $b, c \neq 0$. By AX3a, $b \in D(d, a_3)$ for some $d \in D(a_1, a_2)$. if $d \neq 0$, we are done. If $d = 0$, then $b = a_3$ sp we can replace d by a_1 in this case.

(⇐) AX1 and AX2 for (X, G) (as an ARS) is consequence of AX1 and AX2 for (X, G^*) (as an AOS). AX3a: suppose $b \in D(a_1, c)$ for some $c \in D(a_2, a_3)$. We want to show that $b \in D(d, a_3)$ for some $d \in D(a_1, a_2)$. The existence of d is immediate if one of b, c, a_1, a_2, a_3 is 0. So suppose b, c, a_1, a_2, a_3 are non-zero. In this case, existence of d follows from AX3 for (X, G^*). AX3b: i f a, b are both zero, then $0 \in D^t(a, b)$. Otherwise, if $a \neq 0$ say, then $a \in D^t(a, b)$. □

Later, when working with the topology on X, we need notation for various sorts of subsets of X. We introduce this notation now. Namely, for $a \in G$

$$U(a) := \{x \in X : a(x) > 0\}.$$

Thus

$$\begin{aligned} U(-a) &= \{x \in X : a(x) < 0\} \\ U(a^2) &= \{x \in X : a(x) \neq 0\} = U(a) \cup U(-a). \end{aligned}$$

Now, define

$$\begin{aligned} Z(a) &:= X \setminus (U(a) \cup U(-a)) = X \setminus U(a^2) = \{x \in X : a(x) = 0\}. \\ W(a) &= X \setminus U(-a) = U(a) \cup Z(a) = \{x \in X : a(x) \geq 0\}. \end{aligned}$$

For $a_1, ..., a_k \in G$,

$$U(a_1, ..., a_k) := \bigcap_{i=1}^{k} U(a_i)$$
$$Z(a_1, ..., a_k) := \bigcap_{i=1}^{k} W(a_i)$$
$$W(a_1, ..., a_k) := \bigcap_{i=1}^{k} W(a_i)$$

More generally, for any subset $S \subseteq G$,

$$U(S) := \bigcap_{a \in S} U(a),$$
$$Z(S) := \bigcap_{a \in S} Z(a),$$
$$W(S) := \bigcap_{a \in S} W(a).$$

We make frequent use of the following:

Proposition 5.1.30.

i - For any $a, b \in G$, $D^t(a^2, b^2) = \{c^2\}$ for some unique $c^2 \in G^2$.

ii - For any $a, b \in G$, there exists $c \in G$ such that $Z(a, b) = Z(c)$.

iii - For any $a, b, d \in G$, $D(a^2 d, b^2 d) = \{c^2 d\}$ for some unique $c^2 d \in G$.

Proof.

i - Let $c \in D^t(a^2, b^2)$. Then for all $x \in X$, $c(x) \geq 0$ and $c(x) = 0$ iff $a(x) = b(x) = 0$. This proves that c is unique and also that $c = c^2 \in G^2$.

ii - Pick c such that $c \in D^t(a^2, b^2)$.

iii - Is the same argument of item (i).

□

We mention briefly the idea of a morphism of abstract real spectra. This generalizes the corresponding idea for space of orderings.

Definition 5.1.31. *A morphism of ARS's $(X, G) \to (Y, H)$ is a mapping $\tau : X \to Y$ such that for each $a \in H$, the composite mapping is $a \circ \tau : X \to \{-1, 0, 1\}$ is an element of G (so τ is surjective and induces a mapping $a \mapsto a \circ \tau$ from H to G). τ is said to be an isomorphism if the mappings $X \to Y$ and $H \to G$ are bijective.*

With this definition and proposition 5.1.29, we have a full and faithfull functor $\mathcal{AOS} \to \mathcal{ARS}$, that is injective on the objects.

5.1.6 Properties of value sets

Let (X, G) be an abstract real spectrum. Dimension and discriminant of forms, signature of forms, etc, are defined exactly as in the concrete case $(X, G) = (X_T, G_T)$. A **form of dimension** n with entries in G is just an n-tuple $\varphi = \langle a_1, ..., a_n\rangle$, $a_1, ..., a_n \in G$. The **discriminant** of φ is $\text{disc}(\varphi) = a_1...a_n \in G$. The **signature** of φ at $x \in X$ is

$$\varphi(x) := \sum_{i=1}^{n} a_i(x) \in \mathbb{Z}.$$

We write $\varphi \cong \psi$ (read φ is **isometric** to ψ) to indicate that φ and ψ have the same dimension and the same signature at each $x \in X$. Initially at least, we will be mainly interested in the isometry of binary (2-dimensional) forms. It is important to note that

$$D(a, b) = \{c \in G : \langle c^2a, c^2b\rangle \cong \langle c, abc\rangle\},$$
$$D^t(a, b) = \{c \in G : \langle a, b\rangle \cong \langle c, abc\rangle\}.$$

For the remaining dimensions, value sets and transversal value sets are defined as in 5.1.21 and 5.1.24 i.e,

$$D(a) := \{b \in G : \text{ for all } x \in X,\ b(x) = a(x) \text{ or } b(x) = 0\} = \{b^2a : b \in G\},$$

and

$$D(a_1, ..., a_n) := \bigcup_{x \in D(a_2,...,a_n)} D(a_1, c) \text{ if } n \geq 3.$$

Similarly, $D^t(a) = \{a\}$ and

$$D^t(a_1, ..., a_n) := \bigcup_{x \in D^t(a_2,...,a_n)} D^t(a_1, c) \text{ if } n \geq 3.$$

The form notation and terminology we use is standard: if $\varphi = \langle a_1, ..., a_n\rangle$, $\psi = \langle b_1, ..., b_m\rangle$ are forms with entries in G and $c \in G$ then

$$\varphi \oplus \psi := \langle a_1, ..., a_n, b_1, ..., b_n\rangle,$$
$$c\varphi := \langle ca_1, ..., ca_n\rangle$$
$$\varphi \otimes \psi := a_1\psi \oplus ... \oplus a_n\psi = \langle a_1b_1, ..., a_ib_j, ..., a_nb_m\rangle.$$

Also, if $k \geq 1$,

$$k \times \varphi := \varphi \oplus ... \oplus \varphi \, k\text{-times}.$$

A form of shape $\langle 1, a_1\rangle \otimes ... \otimes \langle 1, a_n\rangle$ is called a **n-fold Pfister form**, and denoted by $\langle\langle a_1, ..., a_n\rangle\rangle$.

As mentioned before, isometry is badly behaved in general. We have the example

$$\langle 1, -1\rangle \cong \langle 0, 0\rangle \; D(1, -1) = G,\ D(0, 0) = \{0\}.$$

On the positive side, by 5.1.32(i) below, value sets are preserved under permutation of entries at least. Thus, for what we do here there is no harm in identifying two forms φ, ψ if the entries of ψ are some permutation of the entries of φ. This allows us to write $\varphi \oplus \psi = \psi \oplus \varphi$ and $\varphi \otimes \psi = \psi \otimes \varphi$, for example.

Proposition 5.1.32.

i - $D(\varphi)$ *does not depend on the order of the entries of* φ.

ii - *If* $b \in D(\varphi)$ *then* $bc \in D(c\varphi)$ *for any* $c \in G$. *Conversely, if* $b \in D(c\varphi)$ *then* $b = bc^2 = (bc)c$ *and* $bc \in D(c^2\varphi) \subseteq D(\varphi)$.

iii - $c \in D(\varphi \oplus \psi)$ *iff* $c \in D(a, b)$ *for some* $a \in D(\varphi)$, $b \in D(\psi)$.

iv - $c \in D(\varphi_1 \oplus ... \oplus \varphi_k) \Leftrightarrow c \in D(a_1, ..., a_k)$ *for some* $a_i \in D(\varphi_i)$, $i = 1, ..., k$.

Proof.

i - Let $\varphi = \langle a_1, ..., a_n \rangle$. If $n = 1$ or 2 we are done. Suppose $n \geq 3$. It suffices to show the value set does not change if we permute two adjacent entries a_i, a_j. If $i, j \geq 2$, this follows by induction. This leaves the case $i = 1$, $j = 2$. Suppose $b \in D(a_2, a_1, a_3, ..., a_n)$. Thus $b \in D(a_2, c)$, $c \in D(a_1, d)$, $d \in D(a_3, ..., a_n)$. By AX3a, $b \in D(a_1, e)$ for some $e \in D(a_2, d)$. This proves $b \in D(a_1, a_2, ..., a_n)$.

ii - The first assertion is immediate for $n = 1$ or 2 and follows by induction for $n \geq 3$. If $b \in D(c\varphi)$ then $c = 0 \Rightarrow b = 0$ so $b = bc^2$. The second assertion is immediate from the first once this observation is made.

iii - Let $\varphi = \langle a_1, ..., a_k \rangle$, $\psi = \langle a_{k+1}, ..., a_n \rangle$.

($\Rightarrow$) If $k = 1$, $c \in D(a_1, b)$, $b \in D(a_2, ..., a_n)$ so we can take $a = a_1$. If $k \geq 2$ then $c \in D(a_1, d)$, $d \in D(\varphi' \oplus \psi)$, where $\varphi' = \langle a_2, ..., a_k \rangle$. By induction, we have $d \in D(e, f)$, $e \in D(\varphi')$, $f \in D(\psi)$. By AX3a we have $c \in D(g, f)$ for some $g \in D(a_1, e)$. Thus $g \in D(\varphi)$ so we can take $a = g$, $b = f$.

($\Leftarrow$) If $k = 1$ then $c \in D(a_1, b)$ (since $a \in D(a_1)$) so $c \in D(\varphi \oplus \psi)$. If $k \geq 2$ then $a \in D(a_1, d)$, $d \in D(\varphi')$ where $\varphi' = \langle a_2, ..., a_n \rangle$. By AX3a, $c \in D(a_1, c)$ where $e \in D(d, b)$. By induction on k, $e \in D(\varphi' \oplus \psi)$. This proves $c \in D(\varphi \oplus \psi)$.

iv - This follows from (iii) using induction on k.

□

We use the following key result:

Lemma 5.1.33.

i - *Suppose* $Z(a) \cap W(c) \subseteq Z(c)$. *Then there exists* $a_1 \in D^t(a, b)$ $a_1 = a$ *on* $W(c)$.

ii - *If* $b \in D(ea_1, ea_2, a_3)$ *then* $b \in D(ed, a_3)$ *for some* $d \in D^t(b^2a_1, b^2a_2)$.

Proof.

i - By hypothesis, $b^2 \in D(a^2b^2, -b^2c)$ so $b^2 \in D(-a^2b^2, a^2b^2, -b^2c)$. Since $D(-a^2b^2, a^2b^2) = D(-ab, ab)$, this implies $b^2 \in D(-ab, ab, -b^2c)$ so, there exists $e \in D(ab, -b^2c)$ such that $b^2 \in D(-ab, e)$. Pick any $a_1 \in D^t(a, be)$. We claim that $a_1 \in D^t(a, b)$ and $a_1 = a$ on $W(c)$. On the part of X where $b = 0$ it follows (from $a_1 \in D^t(a, be)$). On the part of X where $b \neq 0$, either $e \geq 0$ or $ab < 0$ (since $b^2 \in D^t(-ab, e)$). If $e \geq 0$ then $a_1 \in D^t(a, b)$ (since $a_1 \in D^t(a, be)$) and, if we also have $c \geq 0$, then $ab > 0$ (since $e \in D(ab, -b^2c)$) so $a_1 = a$. This leaves the part of X where $ab < 0$ and $e \geq 0$. So $a_1 \in D^t(a, b)$ on this part and, since $e \leq 0$ and $a_1 \in D^t(a, be)$, we must have $a_1 = a$ on this part. This proves the claim.

ii - Scaling by b and applying 5.1.32, $b^2 \in D(f_0, a_3b)$ for some $f_0 \in D(ea_1b, ea_2b)$. Let $f = ef_0$. Then $ef = e^2f_0 = f_0$, so $b^2 \in D(ef, a_3b)$ and $f \in D(a_1b, a_2b)$. Thus, on $W(-a_3b) \cap U(b^2)$, $ef > 0$ (so $f^2 > 0$) so $b^2 \in D(f^2, a_3b)$. Pick $g \in D^t(a_1b, a_2b)$. Then $Z(f) \cap W(-a_3b) \subseteq Z(b) \subseteq Z(g)$ so, by (i), there exists $f_1 \in D^t(f, g)$ such that $f_1 = f$ on $W(-a_3b)$. We claim that $f_1 \in D^t(a_1b, a_2b)$ and $b^2 \in D(ef_1, a_3b)$. Since $f \in D(a_1b, a_2b)$ and $g \in D^t(a_1b, a_2b)$ and $f_1 \in D^t(f, g)$, it follows that $f_1 \in D(a_1b, a_2b)$. If $f_1 = 0$ then $f = -g$. If $g = 0$, this forces $a_1b = -a_2b$. If $g \neq 0$ it also forces $a_1b = -a_2b$. This proves $f_1 \in D^t(a_1b, a_2b)$. From $a_3b > 0$ we get $b^2 \in D(ef_1, a_3b)$. If $a_3b \leq 0$, then $f_1 = f$ and $b^2 \in D(ef, a_3b)$. This proves the claim. By the claim, $f_1b \in D^t(a_1b^2, a_2b^2)$, $b \in D(ef_1b, a_3b^2)$. Now, just take $d = f_1b$ to complete the proof.

□

Theorem 5.1.34. *Suppose X is a non-empty set and G is a submonoid of $\{-1, 0, 1\}^X$ containing the constant functions. Then the following are equivalent:*

a - AX3 holds.

b - AX3a and AX3b holds.

c - $b \in D(a_1, c)$ for some $c \in D(a_2, a_3) \Rightarrow b \in D(d, a_3)$ for some $d \in D^t(b^2a_1, b^2a_2)$.

Proof. (a)⇒(b): is just 5.1.26.

(b)⇒(c): Follow from 5.1.33(ii), taking $e = 1$.

(c)⇒(a): AX3a follows from (c), so 5.1.32 holds. Also AX3b follows from c using the fact that $1ainD(a, b, 1)$. Now suppose $b \in D^t(a_1, c)$ for some $c \in D^t(a_2, a_3)$. Let $a_0 = -b$. Thus $-a_0 \in D^t(a_1, c)$, $c \in D^t(a_2, a_3)$. Also $-a_1 \in D^t(a_0, c)$, $c \in D^t(a_2, a_3)$. Similarly, $-a_2 \in D^t(a_3, -c)$, $-c \in D^t(a_0, a_1)$ and $-a_3 \in D^t(a_2, -c)$, $-c \in D^t(a_0, a_1)$. Thus, using (c) there exists $d_0, d_1, d_2, d_3 \in G$ such that

$$\begin{aligned}
&-a_0 \in D^t(a_3a_0^2, d_0),\ d_0 \in D^t(a_1a_0^2, a_2a_0^2),\\
&-a_1 \in D^t(a_2a_1^2, -d_1),\ -d_1 \in D^t(a_0a_1^2, a_3a_1^2),\\
&-a_2 \in D^t(a_1a_2^2, -d_2),\ -d_2 \in D^t(a_0a_2^2, a_3a_2^2),\\
&-a_3 \in D^t(a_0a_3^2, d_3),\ d_3 \in D^t(a_1a_3^2, a_2a_3^2).
\end{aligned}$$

In summary, d_0, d_1, d_2, d_3 satisfy

$$-a_0a_i^2 \in D^t(a_3a_i^2, d_i),\ d_i \in D^t(a_1a_i^2, a_2a_i^2),\ i = 0, 1, 2, 3. \qquad (*)$$

Pick any element $d \in D^t(d_0, d_1, d_2, d_3)$ (d exist by AX3b and induction). A straightforward check shows that $-a_0 \in D^t(a_3, d)$, $d \in D^t(a_1, a_2)$ as required. We check that $-d \in D^t(a_0, a_3)$ (the proof that $d \in D^t(a_1, a_2$ is similar). Since $d \in D(d_0, d_1, d_2, d_3)$ and $-d_i \in D(a_0, a_3)$ by (*), $-d \in D(a_0, a_3)$. It remains to show that, at each point in X, $a_0 \neq a_3 \Rightarrow d \neq 0$. So suppose $a_0 \neq a_3$. One of a_0, a_3 is not zero, say $a_3 \neq 0$ (so $a_0 = a_3$ or $a_0 = 0$). By (*), $d_i = -a_3d_i^2$, so each d_i has the same sign as $-a_3$, or $d_i = 0$. Also, $d_3 = -a_3a_3^2 = -a_3 \neq 0$. Since $d \in D^t(d_0, d_1, d_2, d_3)$ this forces d to have the same sign as $-a_3$ so $d \neq 0$. □

Proposition 5.1.35.

a - $D^t(\varphi)$ does not depend on the order of the entries of φ.

b - If $b \in D^t(\varphi)$ then $bc \in D^t(c\varphi)$ for any $c \in G$.

c - $c \in D^t(\varphi \oplus \psi) \Leftrightarrow c \in D^t(a,b)$ *for some* $a \in D^t(\varphi)$, $b \in D^t(\psi)$.

d - $c \in D^t(\varphi_1 \oplus ... \oplus \varphi_k) \Leftrightarrow c \in D^t(a_1,...,a_k)$ *for some* $a_i \in D^t(\varphi_i)$, $i = 1,...,k$.

Proof. This is basically the same as the proof of 5.1.32 except now we use AX3 instead of AX3a. □

Value sets are describable in terms of transversal value sets as follows:

Proposition 5.1.36. *The following are equivalent:*

a - $b \in D(a_1,...,a_n)$.

b - $b \in D^t(c_1^2a_1,...,c_n^2a_n)$ *for some* $c_1,...,c_n \in G$.

c - $b \in D^t(b^2a_1,...,b^2a_n)$.

Proof. This is immediate if $n = 1$ or $n = 2$ so we assume $n \geq 3$.

(a)⇒(b): this follows immediately by induction on n.

(b)⇒(c): by assumption $b \in D^t(c_1^2a_1, c)$ for some $c \in D^t(c_2^2a_2,...,c_n^2a_n)$. Thus $b \in D(a_1,c)$ so $b \in D^t(b^2a_1, b^2c)$. Since $b^2c \in D^t(b^2c_2^2a_2,...,b^2c_n^2a_n)$ this proves $b \in D^t(b^2a_1, c_2^2a_2,...,c_n^2a_n)$. Now permute the entries of $\langle b^2a_1, c_2^2a_2,...,c_n^2a_n\rangle$ so that $b^2c_2^2a_2$ is in the first position and repeat the argument, etc (using the fact that $b^2b^2 = b^2$).

(c)⇒(a): this follows immediately from

$$D^t(b^2a_1,...,b^2a_n) \subseteq D(b^2a_1,...,b^2a_n) \subseteq D(a_1,...,a_n).$$

□

Proposition 5.1.37. *For* $a_0,...,a_n \in G$, *the following are equivalent:*

a - $-a_0 \in D^t(a_1,...,a_n)$.

b - $-a_i \in D^t(a_1,...,a_{i-1},a_{i+1},...,a_n)$ *for all* $i \in \{0,...,n\}$.

c - $-a_i \in D(a_1,...,a_{i-1},a_{i+1},...,a_n)$ *for all* $i \in \{0,...,n\}$.

Proof. (a)⇒(b): In view of 5.1.35(i), it suffices to show $-a_0 \in D(a_1,...,a_n)$ implies $-a_1 \in D^t(a_0,a_2,...,a_n)$. Say $-a_0 \in D^t(a_1,c)$, $c \in D^t(a_2,...,a_n)$. Then $-a_1 \in D^t(a_0,c)$, $c \in D^t(a_2,...,a_n)$, so $-a_1 \in D^t(a_0,a_2,...,a_n)$.

(b)⇒(c): is immediate.

(c)⇒(a): since $-a_i \in D(a_0,...,a_{i-1},a_{i+1},...,a_n)$, $-a_i = -a_ia_i^2 \in D^t(a_0a_i^2,...,a_{i-1}a_i^2,a_{i+1}a_i^2,...,a_na_i^2)$ so, using the implication (a)⇒(b),

$$-a_0a_i^2 \in D^t(a_1a_i^2,...,a_na_i^2),\ i = 0,...,n.$$

Observe that $a_i \in D^t(a_i\langle a_0^2,...,a_n^2\rangle)$, in fact, by 5.1.30(iii) and induction, a_i is the only element in $D^t(a_i\langle a_0^2,...,a_n^2\rangle)$. In particular, $-a_0 \in D^t(-a_0\langle a_0^2,...,a_n^2\rangle)$ so, by 5.1.35(iv),

$$-a_0 \in D^t(a_1a_0^2,...,a_na_0^2) \oplus ... \oplus D^t(a_1a_n^2,...,a_na_n^2).$$

The entries of $a_1\langle a_0^2,...,a_n^2\rangle \oplus ... \oplus a_n\langle a_0^2,...,a_n^2\rangle$ are a permutation of the entries of $\langle a_1a_0^2,...,a_na_0^2\rangle \oplus ... \oplus \langle a_1a_n^2,...,a_na_n^2\rangle$ so, by 5.1.35(i),

$$-a_0 \in D^t(a_1\langle a_0^2,...,a_n^2\rangle \oplus ... \oplus a_n\langle a_0^2,...,a_n^2\rangle).$$

Thus, by 5.1.35(iv) again, $-a_0 \in D^t(a'_1, ..., a'_n)$ where $a'_i \in D^t(a_i\langle a_0^2, ..., a_n^2)$. Since a_i is the unique element of $D^t(a_i\langle a_0^2, ..., a_n^2\rangle)$, this means $-a_0 \in D^t(a_1, ..., a_n)$. □

Theorem 5.1.38.

i - $b \in D(c\varphi \oplus \psi) \Rightarrow b \in D(\langle cd\rangle \oplus \psi)$ *for some* $d \in D^t(b^2\varphi)$.

ii - *If* $b \in D(c_1\varphi_1 \oplus ... \oplus c_k\varphi_k)$ *then* $b \in D(c_1d_1, ..., c_kd_k)$ *for some* $d_i \in D^t(b^2\varphi_i)$, $i = 1, ..., k$.

Proof.

i - Let $\varphi = \langle a_1, ..., a_n\rangle$. If $n = 1$, taking $d = b^2a_1$ we obtain the desired. Suppose $n \geq 2$ and let $\varphi' = \langle a_3, ..., a_n\rangle$. Thus $b \in D(ca_1, ca_2, e)$, $e \in D(c\varphi' \oplus \psi)$. By 5.1.33(ii), $b \in D(cf, e)$, $f \in D^t(b^2a_1, b^2a_2)$. Thus $b \in D(c(\langle f\rangle \oplus \varphi') \oplus \psi)$. By induction on n, $b \in D(\langle cd\rangle \oplus \psi)$, $d \in D^t(\langle b^2f\rangle \oplus b^2\varphi')$. Since $b^2f = f$ and $f \in D^t(b^2a_1, b^2a_2)$, this means $d \in D^t(b^2\varphi)$.

ii - This follows by repeated use of (i).

□

5.2 Real semigroups

Here introduce a new class of algebraic structures dual to the category of abstract real spectra. This structure first appear in [DP04], and was baptised real semigroups (abbreviated RS).

We realize that both ARS's and real semigroups provides a reduced theory of quadratic forms over rings, but the non-reduced case is still unknown. In view of this, we avoid as much as possible the uses of the reduction axiom, and as contribution, we gave new elementary proofs of basic facts in real semigroups.

5.2.1 Ternary semigroups

As a preliminary step, we devote some attention to the ternary semigroups, a class of semigroups underlying the RS's in very much same sense that the groups of exponent 2 underlie the notion of special group.

Definition 5.2.1. *A ternary semigroup (abbreviated TS) is a struture* $(S, \cdot, 1, 0, -1)$ *with individual constants* $1, , 0, -1$ *and a binary operation "*$\cdot$*" such that:*

TS1 - $(S, \cdot, 1)$ *is a commutative semigroup with unity;*

TS2 - $x^3 = x$ *for all* $x \in S$*;*

TS3 - $-1 \neq 1$ *and* $(-1)(-1) = 1$*;*

TS4 - $x \cdot 0 = 0$ *for all* $x \in S$*;*

TS5 - *For all* $x \in S$, $x = -1 \cdot x \Rightarrow x = 0$.

We shall write $-x$ *for* $(-1) \cdot x$. *The semigroup verifying conditions [TS1] and [TS2] (no extra constants) will be called 3-semigroups.*

Example 5.2.2.

a - The three-element structure $\mathbf{3} = \{1, 0, -1\}$ *has an obvious ternary semigroup structure.*

b - *For any set X, the set $\mathbf{3}^X$ under pointwise operation and constant functions with values $1, 0, -1$, is a TS.*

c - *The class of ternary semigroups is closed under direct product and subestructures.*

d - *Any group of exponent 2 is a 3-semigroup; the pointed group of exponent 2 with a distinguished element $-1 \neq 1$ underlying a RSG also verifies [TS3]. Any such group G, becomes a ternary semigroup by adding a new absorbent element 0, i.e, extending the operation by $x \cdot 0 = 0$ for $x \in G \cup \{0\}$. Note that the set of invertible elements of a 3-semigroup is a group of exponent 2.*

e - *For any commutative ring A with 1, the set G_A of all functions $\overline{a} : Sper(A) \to \mathbf{3}$, for $a \in A$, where*

$$\overline{a}(\alpha) = \begin{cases} 1 \text{ if } a \in \alpha \setminus (-\alpha) \\ 0 \text{ if } a \in \alpha \cap (-\alpha) \\ -1 \text{ if } a \in (-\alpha) \setminus \alpha \end{cases}$$

with the operation induced by product in A is a TS.

By a *subsemigroup* we mean a subset closed under the operation $\cdot$ and containing 1. Thus, a subsemigroup of a TS may not contain 0 or -1 and hence may not be a substructure for the language used in 5.2.1. A *TS-morphism* is a function $f : (S, \cdot, 1, 0, -1) \to (T, \cdot, 1, 0, -1)$ such that $f(ab) = f(a)f(b)$ and $f(-1) = -1$. A *TS-character* is a TS-morphism into $\mathbf{3}$.

An *ideal* in a semigroup S is a subset $I \subseteq S$ such that $I \cdot S \subseteq I$. An ideal is *prime* if it is proper and $ab \in I \Rightarrow a \in I$ or $b \in I$, for all $a, b \in S$.

Of course, given a ternary semigroup T and a subset $X \subseteq T$, the *ideal generated by X* is

$$[X] = \bigcap \{I \text{ ideal} : I \supseteq X\} = \{1\} \cup \left\{ \prod_{i=1}^{n} r_i a_i : a_i \in X,\, r_i \in T\, n \in \mathbb{N} \right\}.$$

The basic properties of ideals holds here: intersection of ideals is an ideal, directed union of ideals is an ideal, etc.

Lemma 5.2.3. *Let I be an ideal in a TS, T, and let Δ be a subsemigroup of T such that $I \cap \Delta = \emptyset$. Let J be an ideal of G containing I and maximal with respect to being disjoint from Δ. Then J is prime. In particular, if $a \notin I$ (by setting $\Delta = \{1, a^2\}$) it follows that an ideal maximal for not containing a is prime.*

Proof. Suppose by absurd that J is not prime, i.e, that $ab \in J$ with $a \notin J$ and $b \notin J$. Let $J_1 = [J \cup \{a\}]$ and $J_2 = [J \cup \{b\}]$. Since $J \subsetneq J_1$ and $J \subsetneq J_2$, by maximality of J we must have $x \in \Delta \cap J_1$ and $y \in \Delta \cap J_2$. Note that $x = ax'$ and $y = by'$ (because $J \cap \Delta = \emptyset$). Then $xy \in \Delta$ and $xy = ab(x'y') \in [J \cup \{ab\}] = J$, contradiction. Therefore $a \in J$ or $b \in J$. □

Definition 5.2.4. *Let T be a TS and $S \subseteq T$. S will be called a prime subsemigroup of T if*

i - *S is a subsemigroup of T containing $Id(T)$ (the idempotents of T).*

ii - *$S \cap -S$ is a prime ideal.*

iii - *$S \cup -S = T$.*

The prime subsemigroups S of T are in one-one correspondence with the TS-characters of T; indeed, S defines a TS-character upon setting, for $x \in T$:

$$h_S(x) = \begin{cases} 1 \text{ if } x \in S \setminus (-S) \\ 0 \text{ if } x \in S \cap -S \\ -1 \text{ if } x \in (-S) \setminus S. \end{cases}$$

The following lemma gives the tool used in practice to construct TS-characters:

Lemma 5.2.5. *Let T be a TS and let I be a prime ideal of T. Let S be a subsemigroup of T such that:*

1. *$Id(T) \cup I \subseteq S$.*
2. *S is maximal such that $S \cap -S = I$.*

Then S is a prime subsemigroup, i.e, $S \cup -S = T$. The TS-character h_S defined by S (as above) verifies $I = h_S^{-1}[0]$ and $S = h_S^{-1}[\{0, 1\}]$.

Proof. Suppose that there exist $x \in T$ with $x, -x \notin S$. Let $S_1 = [S \cup \{x\}]$ and $S_2 = [S \cup \{-x\}]$. Since $S \subsetneq S_1$ and $S \subsetneq S_2$, by maximality of S we must have $a \in (S_1 \cap -S_1) \setminus I$ and $b \in (S_2 \cap -S_2) \setminus I$. From (2) we have $a, b \notin S \cap -S$. Note that we cannot either have $a, -a \in Sx$ or $b, -b \in S(-x)$. If for instance $a, -a \in Sx$, then $a = s_1 x$ and $-a = s_2 x$. Multiplying both these equalities by x, we get $ax = s_1 x^2$ and $-ax = s_2 x^2$, both which are in S, by (1). Since $x, a \notin I$, I cannot be prime.

Thus, one of a or $-a$ in S and the other in Sx, and similarly for $b, -b$. However, each of these situations contradicts the primality of I. For illustration, say $a \in S$, $-a \in Sx$, $b \in S(-x)$, $-b \in S$. Then $-ab \in S$, $-a = s_1 x$, $-b = s_2 x$ with $s_1, s_2 \in S$. Multiplying these equalities given $ab = (-a)(-b) = s_1 s_2 x^2 \in S$, by (1). Then $ab \in I$, but $a, b \notin I$, a contradiction. □

Theorem 5.2.6 (Weak separation theorem)**.** *Let T be a TS, I be an ideal of T, and $a \in T \setminus I$. Then:*

a - There is a TS-character h of T such that $h[I] = 0$ and $h(a) \neq 0$.

b - If, in addition, $-a \cdot Id(T) \cap Id(T) \subseteq I$, then there is a character h such that $h[I] = 0$ and $h(a) = 1$.

If I is prime, in both (a) and (b) the character h can be chosen such that $h^{-1}[0] = I$

The following will be used in the proof of theorem 5.2.6(b):

Lemma 5.2.7. *Let T be a TS, I an ideal of T, and $a \in I$. Assume that $-a \cdot Id(T) \cap Id(T) \subseteq I$. Then, for $x \in T$,*

$$x, -x \in Id(T) \cup a \cdot Id(T) \Rightarrow x \in I.$$

Proof. If $x, -x \in \mathrm{Id}(T)$, then $-x = (-x)^2 = x^2 = x$ and by TS5 $x = 0 \in I$. If $x, -x \in -a \cdot \mathrm{Id}(T)$, then $x = ay^2$, $-x = az^2$. Squaring both these equalities gives $x^2 = a^2 y^2 = (-x)^2 = a^2 z^2$. Scaling by a we get $ay^2 = az^2$, i.e, $x = -x$, and hence $x = 0$. If $x \in \mathrm{Id}(T)$, $-x \in a \cdot \mathrm{Id}(T)$, then $x = x^2$ and $-x = ay^2$, so $-ay^2 = x = x^2 \in -a \cdot \mathrm{Id}(T) \cap \mathrm{Id}(T) \subseteq I$ by hypothesis. The remaining case is similar. □

proof of theorem 5.2.6.

a - First of all, by lemma 5.2.3 we get a prime ideal $J \supseteq I$ maximal for not $a \notin J$. If I is itself prime, just pick $J = I$. Now, let

$$\mathcal{F} = \{S \subseteq G \text{ subsemigroup} : S \supseteq J \cup \mathrm{Id}(T) \text{ and } S \cap (-S) = J\}.$$

$\mathcal{F} \neq \emptyset$ since $J \cup \mathrm{Id}(T) \in \mathcal{F}$. Hence, by Zorn's Lemma there is a maximal element $R \in \mathcal{F}$. By lemma 5.2.5 there exist a character h_R determined by R. This character has the properties stated in (a), since $a \notin J = h^{-1}[0]$.

b - As in the previous case we may assume I prime. Now, we will factory a subsemigroup $S \supseteq \{a\} \cup I \cup \mathrm{Id}(T)$ maximal for $S \cap -S = I$. Using Zorn's Lemma it is suffice to show that there is a subsemigroup S' with these two properties. We claim $S' = \mathrm{Id}(T) \cup a \cdot \mathrm{Id}(T) \cup I$ meets these conditions. Of course, S' is a subsemigroup of T. To prove $S' \cap -S' = I$, assume $x, -x \in S'$. In the non-trivial case where $x, -x \in \mathrm{Id}(T) \cup a \cdot \mathrm{Id}(T)$, our assumption and lemma 5.2.7 entail that $x \in I$, as required. Since $a \in S \setminus I = S \setminus (-S)$, we have $h(a) = 1$, where h is the character determined by S.

□

Definition 5.2.8. *For $c \in T$, let $I_c = \{x \in T : c^2 x = x\}$.*

Theorem 5.2.9 (Separation theorem for ternary semigroups)**.** *Let T be a TS and let $a, b \in T$, $a \neq b$. Then, there is a TS-character h of T such that $h(a) \neq h(b)$. In other words, the set X_T of TS-characters separates points (in T). Equivalently, the evaluation map from T to $\mathbf{3}^{X_T}$ is an injective TS-homomorphism.*

Proof. We consider two cases:

1. $a^2 \neq b^2$.

   If $a \in I_b$ and $b \in I_a$, then $a^2 b = b$ and $b^2 a = a$, from which $a^2 b^2 = b^2 = a^2$, contrary to this case assumption. Assume, without loss of generality, that $a \notin I_b$. Let $I \supseteq I_b$ be an prime ideal maximal for not containing a (conform lemma 5.2.3). By theorem 5.2.6(a) we get a character h of T such that $I = h^{-1}[0]$; hence $h(b) = 0$ and $h(a) \neq 0$.

2. $a^2 = b^2$.

   Let $J = \{x \in T : ax = bx\}$. Of course, J is an ideal. If $a \in J$, then $a^2 b = ba$, and hence $b^2 = ba$. Scaling by b we get $b = b^3 = b^2 a = a^2 a = a$, contrary to the assumption $a \neq b$. Hence $a \notin J$. Let $I \supseteq J$ be an ideal maximal for $a \notin I$. Then $b \notin I$; otherwise, $a^2 = b^2 \in I$, which implies $a = a^2 a \in I$. Since I is prime, we get $b \notin I$, from which $-ab \notin I$. By showing that $ab \cdot \mathrm{Id}(T) \cap \mathrm{Id}(T) \subseteq I$, theorem 5.2.6(b) applied to $-ab$ yields a character h so that $h(-ab) = 1$, which proves $h(a) \neq h(b)$.

   Elements in $\mathrm{Id}(T) \cap \mathrm{Id}(T)$ are of the form aby^2 with $aby^2 = (aby^2)^2 = a^2 b^2 y^2$. Scaling by b and using $a^2 = b^2$ gives

   $$ab^2 y^2 = a^3 y^2 = ay^2,$$
   $$a^2 b^3 y^2 = a^2 by^2 = b^3 y^2 = by^2,$$

   i.e, $ay^2 = by^2$. Then $y^2 \in J \subseteq I$, from which $aby^2 \in I$, as required.

□

Consider X_T, the set of TS-characters of T, as a subset of $\mathbf{3}^T$. The set X_T becomes a closed subset of $\mathbf{3}^T$, when the latter is endowed with the product topology. Hence, with the induced topology, it is a Boolean space having the sets of the form

$$\bigcap_{i=1}^{n}[t_i = 1] \cap \bigcap_{j=1}^{m}[t'_j \in \{0,1\}],\ t_i, t'_j \in T$$

as a basis of clopen sets, where $[t = i] = \{f \in X_T : f(t) = i\}$, $t \in \{-1, 0, 1\}$. This is the *constructible (or patch)* topology on X_T. Thus, with the sets

$$H(t_1, ..., t_n) = \bigcap_{i=1}^{n}[t_1 = 1],\ t_i \in T$$

as a basis of clopens, X_T becomes a *spectral space* whose associated patch topology is as described above.

5.2.2 Real semigroups

Here, we will enrich the language $\{\cdot, 1, 0, -1\}$ with a ternary relation D. In agreement with 5.1.25, we shall write $a \in D(b, c)$ instead of $D(a, b, c)$. We also set:

$$a \in D^t(b, c) \Leftrightarrow a \in D(b, c) \wedge -b \in D(-a, c) \wedge -c \in D(b, -a). \qquad \text{(trans)}$$

The relations D and D^t are called *representation* and *transversal representation* respectivel.

Definition 5.2.10. *A real semigroup (abbreviated RS) is a ternary semigroup $(G, 1, 0, -1)$ together with a ternary relation D satisfying:*

RS0 - *$c \in D(a, b)$ if and only if $c \in D(b, a)$.*

RS1 - *$a \in D(a, b)$.*

RS2 - *$a \in D(b, c)$ implies $ad \in D(bd, cd)$.*

RS3 (Strong Associativity) - *If $a \in D^t(b, c)$ and $c \in D^t(d, e)$, then there exists $x \in D^t(b, d)$ such that $a \in D^t(x, e)$.*

RS4 - *$e \in D(c^2a, d^2b)$ implies $e \in D(a, b)$.*

RS5 - *If $ad = bd$, $ae = be$ and $c \in D(d, e)$, then $ac = bc$.*

RS6 - *$c \in D(a, b)$ implies $c \in D^t(c^2a, c^2b)$.*

RS7 (Reduction) - *$D^t(a, -b) \cap D^t(b, -a) \neq$ implies $a = b$.*

RS8 - *$a \in D(b, c)$ implies $a^2 \in D(b^2, c^2)$.*

A pre-real semigroup(abbreviated PRS) is a ternary semigroup $(G, 1, 0, -1)$ together with a ternary relation D satisfying [RS0]-[RS6], [RS8] and

RS7' - *$x \in D^t(0, a) \Leftrightarrow x = a$.*

Note that, as the special groups, the theory of real semigroups is a (finitary) first-order theory. Moreover, we will see later, as consequence of 5.2.14, that every pre-real semigroups is a real semigroup.

The definition of morphism is quite standard: $f : (G, \cdot, 1, 0-1) \to (H, \cdot, 1, 0-1)$ is an *RS-morphism* (respectively PRS) if $f : G \to H$ is a morphism of semigroups, (i.e, $f(ab) = f(a)f(b)$, $f(1) = 1$ and $f(0) = 0$); $f(-1) = -1$ and $a \in D(b, c) \Rightarrow f(a) \in D(f(b), f(c))$ (hence $a \in D^t(b, c) \Rightarrow f(a) \in D^t(f(b), f(c))$). The category of real semigroups (respectively pre-real semigroups) and their morphisms will be denoted by $\mathcal{RS}$ (respectively $\mathcal{PRS}$).

Example 5.2.11 (RS and Rings)**.** *For any semi-real ring A, let the set G_A consist of all functions $\overline{a} : Sper(A) \to \mathbf{3}$, for $a \in A$, where*

$$\overline{a}(\alpha) = \begin{cases} 1 \text{ if } a \in \alpha \setminus (-\alpha) \\ 0 \text{ if } a \in \alpha \cap -\alpha \\ -1 \text{ if } a \in (-\alpha) \cap \alpha. \end{cases}$$

with the operation induced by product in A is a TS. More generally, given a (proper) preorder T of a ring A one can relativize the definition above to T, by considering functions $\overline{a}$ defined on $Sper(A, T) = \{\alpha \in Sper(A) : \alpha \supseteq T\}$, instead of $Sper(A)$. The corresponding ternary semigroup will be denoted $G_{A,T}$.

Now, we will equip the ternary semigroup with the representation and transversal representation relations given by:

$$\overline{c} \in D_A(\overline{a}, \overline{b}) \Leftrightarrow \forall\, \alpha \in Sper(A)[\overline{c}(\alpha) = 0 \vee \overline{a}(\alpha)\overline{c}(\alpha) = 1 \vee \overline{b}(\alpha)\overline{c}(\alpha) = 1].$$
$$\overline{c} \in D^t_A(\overline{a}, \overline{b}) \Leftrightarrow \forall\, \alpha \in Sper(A)[(\overline{c}(\alpha) = 0 \wedge \overline{a}(\alpha) = \overline{-b}(\alpha)) \vee \overline{a}(\alpha)\overline{c}(\alpha) = 1 \vee \overline{b}(\alpha)\overline{c}(\alpha) = 1]$$

for $a, b, c \in A$. We have that G_A is a real semigroup. A similar definition with $Sper(A)$ replaced by $Sper(A, T)$ (T a proper preordering of A) also endows the ternary semigroup $G_{A,T}$ with a structure of real semigroup.

Example 5.2.12 (RS and RSG)**.** *The notion of a RS generalizes that of a reduced special group. Given a RSG G, we adding a absorbent element 0 to give raise to a ternary semigroup $G^* = G \cup \{0\}$. Extending the representation relation G to G^* by*

$$D_{G^*}(a, b) = \begin{cases} \{a, b\} \text{ if } a = 0 \text{ or } b = 0; \\ D_G(a, b) \cup \{0\} \text{ if } a, b \in G, \end{cases}$$

gives a representation relation to G^*. The axioms RS1-RS8 are immediate consequence of the special group axioms SG0-SG6 plus the following property: in a RSG we have

$$a \in D(b, c) \Rightarrow -b \in D(-a, c),$$

then D and D^t coincide on binary forms with entries in G.

Corollary 5.2.13. *There is an inclusion functor $R : \mathcal{RSG} \hookrightarrow \mathcal{RS}$.*

Proof. Follows by defining for a RSG $(G, \equiv, -1)$, $R(G, \equiv, -1) = (G^*, D_{G^*}, D^t_{G^*}, 0, 1, -1)$ and for a SG-morphism $f : (G, \equiv_G, -1) \to (H, \equiv_H, -1)$, $R(f) = f^*$, where $f^*(0) = 0$ and $f^*(a) = f(a)$ for all $a \in G^* \setminus \{0\}$. □

Proposition 5.2.14. *The properties below holds in any pre-real semigroup G, for all $a, b, c, d \in G$:*

1. $a \in D(b,c) \Leftrightarrow a \in D^t(a^2b, a^2c)$.
2. $a \in D^t(b,c) \Rightarrow -b \in D^t(-a,c)$.
3. $0 \in D(a,b)$.
4. $a \in D^t(b,c) \Rightarrow ad \in D^t(bd,cd)$.
5. $d \in D(ca,cb) \Rightarrow d = c^2d$. *In particular,* $D(0,a) \subseteq \{a^2x : x \in G\}$.
6. $a^2 \in D(1,b)$.
7. $a \in D(0,0) \Leftrightarrow a = 0$.
8. $1 \in D^t(1,a)$.
9. $D^t(1,-1) = G$.
10. $ab \in D(1,-a^2)$.
11. $D^t(a,b) \neq \emptyset$.
12. *(Weak Associativity)* $a \in D(b,c) \wedge c \in D(d,e) \Rightarrow \exists\, x[x \in D(b,d) \wedge a \in D(x,e)]$.

If G is a real semigroup, then:

13. $0 \in D^t(a,b) \Leftrightarrow a = -b$. *In particular, every real semigroup is a pre-real semigroup*[1].
14. $a \in D(0,1) \cup D(1,1) \Rightarrow a = a^2$.
15. $a \in D^t(b,b) \Leftrightarrow a = b$.

Proof.

1. $a \in D(a,b)$ implies $a \in D^t(a^2b, a^2c)$ by (RS6). Conversely, $a \in D^t(a^2b, a^2c)$ implies $a \in D(a^2b, a^2c)$ by (trans), and by (RS4) we have $a \in D(b,c)$.
2. By (trans), we have:
$$\begin{aligned} a \in D^t(b,c) &\Leftrightarrow a \in D(b,c) \wedge -b \in D(-a,c) \wedge -c \in D(b,-a) \\ &\Leftrightarrow -b \in D(-a,c) \wedge a \in D(b,c) \wedge -c \in D(b,-a) \\ &\overset{[RS0]}{\Leftrightarrow} -b \in D(-a,c) \wedge a \in D(b,c) \wedge -c \in D(-a,b) \\ &\Leftrightarrow -b \in D^t(-a,c). \end{aligned}$$
3. By axiom (RS1), $0 \in D(0,0) = D(0^2a, 0^2b)$. From (RS4) we get $0 \in D(a,b)$.
4. Again, by trans, we have
$$\begin{aligned} a \in D^t(b,c) &\Leftrightarrow a \in D(b,c) \wedge -b \in D(-a,c) \wedge -c \in D(b,-a) \\ &\overset{[RS2]}{\Rightarrow} ad \in D(bd,cd) \wedge -bd \in D(-ad,cd) \wedge -cd \in D(bd,-ad) \\ &\Leftrightarrow ad \in D^t(bd,cd). \end{aligned}$$

[1] In fact, $0 \in D^t(a,b) \Leftrightarrow a = -b$ is equivalent to RS7'.

5. By (RS8), $d \in D(ca, cb)$ implies $d^2 \in D(c^2a^2, c^2b^2)$. Since by (RS4) $D(c^2a^2, c^2b^2) \subseteq D(c^2, c^2)$, we get $d^2 \in D(c^2, c^2)$. Since $c^2 \cdot c^2 = 1 \cdot c^2$, (RS5)[2] gives $c^2d^2 = 1 \cdot d^2 = d^2$, and hence $c^2d^2 = d^2 \Rightarrow c^2d^3 = d^3 \Rightarrow c^2d = d$.

   Now, if $x \in D(0, b)$, then $x \in D(0 \cdot b^2, b \cdot b^2)$. Hence, the above argument gives us $x = b^2x$. Of course, if $x \in D(0, b)$, by RS6, $xb^2 \in D(0 \cdot b^2, b \cdot b^2) = D(0, b)$. Therefore, $D(0, b) = \{b^2x : x \in G\}$.

6. By (RS1), $a^2 \in D(a^2, a^2b)$, and by (RS4), $a^2 \in D(1, b)$.

7. $0 \in D(0, 0)$ by (RS1). Conversely, if $a \in D(0, 0) = D(0 \cdot 1, 0 \cdot 1)$, then by item (5) $a = a \cdot 0^2 = 0$.

8. By (RS1), $1 \in D^t(1, a)$, and by (RS6), $1 \in D^t(1 \cdot 1^2, a \cdot 1^2) = D^t(1, a)$.

9. Follow from item (1) and item (8).

10. Let $x \in G$. By item (9), $x \in D(1, -1)$, and from (RS6) we get $x \in D^t(1 \cdot x^2, -1 \cdot x^2) \subseteq D(x^2, -x^2)$. With $x = ab$ this yields $ab \in D(a^2b^2, -a^2b^2) = D((ab)^2, -a^2 \cdot b^2)$; using (RS4) we obtain $ab \in D(1, -a^2)$.

11. By the item (8), $1 \in D^t(a, 1)$ and $1 \in D^t(b, 1)$. By (RS3), there exist some $d \in D^t(a, b)$ such that $d \in D^t(d, 1)$.

12. Let $a \in D(b, c)$ and $c \in D(d, e)$. By (RS6), $a \in D^t(a^2b, a^2c)$ and $c \in D(c^2d, c^2e)$. Then, $a \in D^t(a^2b, a^2c)$ and $a^2c \in D(a^2c^2d, a^2c^2e)$. By (RS3), there exist $x \in D^t(a^2b, a^2c^2d)$ such that $a \in D^t(x, a^2c^2e)$. Since by (RS4) $D^t(a^2b, a^2c^2d) \subseteq D(a^2b, a^2c^2d) \subseteq D(b, d)$ and $D^t(x, a^2c^2e) \subseteq D(x, a^2c^2e) \subseteq D(x, e)$, we have the desired.

13. ($\Rightarrow$) By RS7 it suffices to prove $D^t(a, b) \cap D^t(-a, -b) \neq \emptyset$. But $0 \in D^t(a, b)$ implies $0 = -0 \in D^t(-a, -b)$.

14. If $a \in D(1, 1)$, by RS6 $a \in D^t(a^2, a^2)$, and then $-a^2 \in D^t(-a, a^2)$. On the other hand, $-a^2 \in D(-a^2, a^2)$ implies $-a \in D^t((-a^2)^2 \cdot (-a)^2, (-a^2)^2 \cdot a) = D^t(-a^2, a)$. Hence $-a^2 \in D^t(-a^2, a) \cap D^t(-a, a^2)$ and RS7 yields $a = a^2$.

    Next, if $a \in D(0, 1)$, by RS6 $a \in D^t(0, a^2)$, and then $0 \in D^t(-a, a^2)$. Scaling by -1 we obtain $-0 = 0 \in D^t(a, -a^2)$. Hence $0 \in D^t(-a^2, a) \cap D^t(-a, a^2)$ and applying again RS7 we have $a = a^2$.

15. $b \in D^t(b, b)$ is immediate from RS1 and RS6, so we just need to proof $\Rightarrow$. Let $a \in D^t(b, b)$. In particular, $a \in D(b, b)$, and item (5) yields $a = b^2a$. From (2) we also have $-b \in D^t(-a, b)$. On the other hand, from $-b \in D(-b, a)$ and RS6 we get $-b \in D^t((-b)^2(-b), (-b)^2a) = D^t(-b, b^2a) = D^t(-b, a)$. This shows that $-b \in D^t(-a, b) \cap D^t(-b, a)$, and then RS7 yields $a = b$.

□

Now, we are in condition to exhibt another axiomatization for real semigroups in terms of D^t: we will enrich the language $\{\cdot, 1, 0, -1\}$ with a ternary relation D^t. Now, we set

$$a \in D(b, c) \Leftrightarrow a \in D^t(a^2b, a^2c). \qquad \text{(rep)}$$

[2] setting $a' = c^2$, $b' = 1$, $c' = d^2$, $d' = c^2$, $e' = c^2$ and use RS5 on the new variables a', b', c', d', e'.

Definition 5.2.15. *A pre real semigroup (abbreviated PRS) is a ternary semigroup* $(G, 1, 0, -1)$ *together with a ternary relation* D^t *satisfying:*

DT0 - $a \in D^t(b, c)$ *if and only if* $a \in D^t(c, b)$.

DT1 - $a \in D^t(b, c)$ *implies* $-b \in D^t(-a, c)$.

DT2 - $1 \in D^t(1, a)$ *for all* $a \in G$.

DT3 - $a \in D^t(b, c)$ *implies* $ad \in D^t(bd, cd)$.

DT4 (Strong Associativity) - *If* $a \in D^t(b, c)$ *and* $c \in D^t(d, e)$, *then there exists* $x \in D^t(b, d)$ *such that* $a \in D^t(x, e)$.

DT5 - *If* $ad = bd$, $ae = be$ *and* $c \in D^t(c^2d, c^2e)$, *then* $ac = bc$.

DT6 - $e \in D^t(c^2e^2a, d^2e^2b)$ *implies* $e \in D^t(e^2a, e^2b)$.

DT7 - $c \in D(a, b)$ *implies* $c \in D^t(c^2a, c^2b)$.

DT8 - $a \in D^t(a^2b, a^2c)$ *implies* $a^2 \in D^t((ab)^2, (ac)^2)$.

DT9 - $x \in D^t(0, a) \Leftrightarrow x = a$.

A real semigroup (abbreviated RS) is a pre-real semigroup satisfying

DT10 (Reduction) - $D^t(a, -b) \cap D^t(b, -a) \neq$ *implies* $a = b$.

The definition of morphism is the same. Then, we have the following lemma:

Lemma 5.2.16. *The definition 5.2.10 and 5.2.15 are equivalent.*

Proof. We already proof 5.2.10⇒5.2.15 in proposition 5.2.14. The converse 5.2.15⇒5.2.10 is just an application of the definition of D in terms of D^t, as in rep. □

Corollary 5.2.17. *The ternary semigroup* $\mathbf{3} = \{1, 0, -1\}$ *has a unique structure of real semigroup with representation given by:*

$$\begin{cases} D_{\mathbf{3}}(0,0) = \{0\}; \\ D_{\mathbf{3}}(0,1) = D_{\mathbf{3}}(1,0) = D_{\mathbf{3}}(1,1) = \{0,1\}; \\ D_{\mathbf{3}}(0,-1) = D_{\mathbf{3}}(-1,0) = D_{\mathbf{3}}(-1,-1) = \{0,-1\}; \\ D_{\mathbf{3}}(1,-1) = D_{\mathbf{3}}(-1,1) = \mathbf{3}; \end{cases}$$

and transversal representation given by:

$$\begin{cases} D^t_{\mathbf{3}}(0,0) = \{0\}; \\ D^t_{\mathbf{3}}(0,1) = D^t_{\mathbf{3}}(1,0) = D^t_{\mathbf{3}}(1,1) = \{1\}; \\ D^t_{\mathbf{3}}(0,-1) = D^t_{\mathbf{3}}(-1,0) = D^t_{\mathbf{3}}(-1,-1) = \{-1\}; \\ D^t_{\mathbf{3}}(1,-1) = D^t_{\mathbf{3}}(-1,1) = \mathbf{3}. \end{cases}$$

Proof. Is just an analysis of cases approach for the verification of axioms RS0-RS8. □

Of course, the theory of real semigroups has the interpretation of the basic concepts and notation of quadratic forms theory: given a real semigroup G, an n-form is a tuple $\varphi = \langle a_1, ..., a_n \rangle$. If $\varphi = \langle a_1, ..., a_n \rangle$ is a form on G, define

- The *set of elements represented by* φ as

$$D_G(\varphi) = \bigcup\{D(a_1, b) : b \in D\langle a_2, ..., a_n\rangle\},$$

with the convention that $D(\langle a\rangle) = \{b^2a : b \in G\}$.

- The *set of elements transversaly represented by* φ as

$$D^t_G(\varphi) = \bigcup\{D^t(a_1, b) : b \in D^t\langle a_2, ..., a_n\rangle\},$$

with the convention that $D^t(\langle a\rangle) = \{a\}$.

- The *discriminant* of φ as $d(\varphi) = \prod_{i=1}^{n} a_i$.
- *Direct sum* as $\varphi \oplus \theta = \langle a_1, ..., a_n, b_1, ..., b_m\rangle$.
- *Tensor product* as $\varphi \otimes \theta = \langle a_1b_1, ..., a_ib_j, ..., a_nb_m\rangle$. If $a \in G$, $\langle a\rangle \otimes \varphi$ is written $a\varphi$.
- For forms φ, ψ over G, we set $\varphi \sim \psi \Leftrightarrow D_G(\varphi) = D_G(\psi)$ and $\varphi \sim^t \psi \Leftrightarrow D^t_G(\varphi) = D^t_G(\psi)$ with a subscript G, if necessary.

Proposition 5.2.18. *Let G be a real semigroup and let φ, ψ be forms with entries in G. Then:*

a - $D(\varphi)$ *and* $D^t(\varphi)$ *do not depend on the order of the entries of* φ*, i.e, for any permutation* σ *of those entries,* $\varphi \sim \varphi^\sigma$ *and* $\varphi \sim^t \varphi^\sigma$.

b - *For* $a, c \in G$, $a \in D(\varphi) \Rightarrow ac \in D(c\varphi)$ *and* $a \in D^t(\varphi) \Rightarrow ac \in D^t(c\varphi)$.

c - $a \in D(c\varphi) \Rightarrow a = c^2a$ *and* $a \in D(\varphi) \Rightarrow a \in D^t(a^2\varphi)$.

d - *If* $\varphi = \langle a_1, ..., a_n\rangle$ *and* $c_1, ..., c_n \in G$, *then* $D(\langle c_1^2a_1, ..., c_n^2a_n\rangle) \subseteq D(\varphi)$.

e - $a \in D(\varphi \oplus \psi) \Leftrightarrow$ *there are* $b \in D(\varphi)$, $c \in D(\psi)$ *such that* $a \in D(b, c)$. *A similar statement holds replacing* D *by* D^t.

f - *If* a *is a coefficient of* φ, *then* $a \in D(\varphi)$.

g - *The relations* $\sim$ *and* $\sim^t$ *are compatible with the sum of forms:*

$$\varphi_1 \sim \psi_1 \text{ and } \varphi_2 \sim \psi_2 \Rightarrow \varphi_1 \oplus \varphi_2 \sim \psi_1 \oplus \psi_2,$$

and similarly for $\sim^t$.

h - $\varphi \oplus \varphi \sim \varphi$ *and* $\varphi \oplus \varphi \sim^t \varphi$.

i - $a \in D(\varphi) \wedge b \in D(\psi) \Rightarrow ab \in D(\varphi \otimes \psi)$. *A similar statement holds replacing* D *by* D^t.

j - *Are equivalent:*

1 - $a \in D^t(\langle a_1, ..., a_n\rangle)$;

2 - $-a_i \in D^t(\langle a_1, ..., a_{i-1}, -a, a_{i+1}, ..., a_n\rangle)$ *for* $i = 1, ..., n$;

3 - $a \in D(\langle a_1, ..., a_n\rangle)$ *and* $-a_i \in D(\langle a_1, ..., a_{i-1}, -a, a_{i+1}, ..., a_n\rangle)$ *for* $i = 1, ..., n$.

k - *For* $b \in G$ *and* $n \geq 1$, $n\langle b\rangle = \langle b, ..., b\rangle \sim^t \langle b\rangle$.

Proof.

a - The statement for D^t follows by the statement for D. Next, we wil proceed by induction on n. If $n = 2$, the statement follow by RS0. Now, suppose that the statement holds for $n-1$ and let $\sigma \in S_n$, $\varphi = \langle a_1, ..., a_n \rangle$. We have two cases:

Case A - $\sigma(1) = 1$. Let $\theta = \langle a_2, ..., a_n \rangle$. Using the induction hypothesis we have

$$D(\varphi) = \bigcup \{D(a_1, b) : b \in D(\theta)\} \overset{\text{HI}}{=} \bigcup \{D(a_1, b) : b \in D(\theta^\sigma)\} = D(\varphi^\sigma).$$

Case B - $D(a_1, a_2, ..., a_n) = D(a_2, a_1, ..., a_n)$. The case $n = 2$ is RS0. For $n \geq 3$ we have

$$\begin{aligned} x \in D(a_1, a_2, ..., a_n) &\Rightarrow x \in D(a_1, b) \text{ for some } b \in D(a_2, ..., a_n) \\ &\Rightarrow x \in D(a_1, b) \text{ and } b \in D(a_2, c) \text{ for some } c \in D(a_3, ..., a_n). \end{aligned}$$

By weak associativity 5.2.19(12), there exist $y \in G$ such that $y \in D(a_1, c)$ and $x \in D(y, a_2)$. Reorganizing these informations we have

$$\begin{aligned} y \in D(a_1, c) \wedge x \in D(y, a_2) \wedge c \in D(a_3, ..., a_n) \Rightarrow \\ x \in D(a_2, y) \wedge [y \in D(a_1, c) \wedge c \in D(a_3, ..., a_n)] \Rightarrow \\ x \in D(a_2, y) \wedge y \in D(a_1, a_3, ..., a_n) \Rightarrow x \in D(a_2, a_1, ..., a_n). \end{aligned}$$

Hence $D(a_1, a_2, ..., a_n) \subseteq D(a_2, a_1, ..., a_n)$. Now, we repeat the same argument starting with $D(a_2, a_1, ..., a_n)$ to obtain $D(a_2, a_1, ..., a_n) \subseteq D(a_1, a_2, ..., a_n)$.

Case C - σ is a 2-cycle $(1, i)$ for some $i \geq 2$. Here, we have

$$\begin{aligned} D(a_1, a_2, ..., a_n) &= D(a_2, a_1, ..., a_n) \\ &= \bigcup \{D(a_2, b) : b \in D(a_1, a_3, ..., a_n)\} \\ &\overset{\text{HI}}{=} \bigcup \{D(a_2, b) : b \in D(\langle a_1, a_3, ..., a_n \rangle^\sigma\} \\ &= \bigcup \{D(a_2, b) : b \in D(\langle a_i, a_3, ...a_{i-1}, a_1, a_{i+1}, a_n \rangle\} \\ &= D(a_2, a_i, a_3, ...a_{i-1}, a_1, a_{i+1}, a_n) \\ &= D(a_i, a_2, a_3, ...a_{i-1}, a_1, a_{i+1}, a_n) = D(\varphi^\sigma). \end{aligned}$$

Cases A,B and C show that $\varphi \sim \varphi^\sigma$ for any transposition $\sigma \in S_n$. Since S_n is generated by transpositions and $\sim$ is transitive, we conclude the desired implication.

b - We use induction on $\dim(\varphi) = n$. If $n = 1$ there is nothing to show, and if $n = 2$, the assertion for D is consequence of RS0 and for D^t is consequence of proposition 5.2.14(4). Now, suppose that the assertion holds for $n-1$ and let $\varphi = \langle a_1, ..., a_n \rangle$. Let $a \in D(\varphi)$. Hence $a \in D(a_1, x)$, for some $x \in D(a_2, ..., a_n)$. By induction hypothesis, $ac \in D(a_1c, xc)$ and $xc \in D(a_2c, ..., a_nc)$, therefore $ac \in D(a_1c, ..., a_nc) = D(c\varphi)$. The assertion for D^t follows by the same argument.

c - Induction on $\dim(\varphi) = n$. For the first assertion, if $\varphi = \langle a_1 \rangle$, then $a \in D(c\varphi)$ means $a = b^2ca_1$ for some $b \in G$. Then $c^2a = c^3b^2a_1 = cb^2a_1 = a$. If $a \in D(c\varphi)$, the inductive definition of representation implies that $a \in D(ca_1, x)$ for some $x \in D(c\varphi')$. By inductive hypothesis, $x = c^2x$. Then $a \in D(ca_1, c^2x)$, and 5.2.14(5) yields $a = c^2a$.

For the second assertion, first we prove by induction on n that

$$a \in D(a_1, ..., a_n) \Rightarrow a \in D^t(c_1^2 a_1, ..., c_n^2 a_n) \text{ for some } c_1, ..., c_n \in G.$$

In fact, if $n = 1$ there is nothing to show, and the case $n = 2$ is just 5.2.14(1). Now, suppose that the claim holds for $(n-1) \geq 3$, and let $a \in D(a_1, ..., a_n)$.

$$\begin{aligned} a \in D(a_1, ..., a_n) &\Rightarrow a \in D(a_1, x) \text{ for some } x \in D(a_2, ..., a_n) \\ &\overset{\text{HI}}{\Rightarrow} a \in D^t(c_1^2 a_1, c_1^2 x) \text{ and } x \in D^t(c_2^2 a_2, ..., c_n^t a_n) \end{aligned}$$

so $a \in D^t(c_1^2 a_1, c_1^2 x)$ and $c_1^2 x \in D^t(c_1^2 c_2^2 a_2, ..., c_1^2 c_n^t a_n)$, then $a \in D^t(c_1^2 a_1, c_1^2 c_2^2 a_2, ..., c_1^2 c_n^t a_n)$ and the claim is proved.

Now, for the proof of second assertion, if $\varphi = \langle a_1 \rangle$, then $a \in D(\varphi)$ means $a = b^2 a_1$ for some $b \in G$. So $a^2 a_1 = b^2 a_1^3 = b^2 a_1 = a$, and by definition, $a \in D^t(a^2 \varphi)$. If $\dim(\varphi) = 2$, the assertion is axiom RS6. Now, suppose that the claim holds for $(n-1) \geq 3$, and let $a \in D(a_1, ..., a_n)$. By the claim, $a \in D^t(c_1^2 a_1, ..., c_n^2 a_n)$, so $a \in D^t(c^2 a_1, x)$ for some $x \in D^t(c_2^2 a_2, ..., c_n^2 a_n)$. Thus $a \in D(a_1, x)$ therefore $a \in D(a^2 a_1, a^2 x)$. Since $a^2 x \in D^t(a^2 c_2^2 a_2, ..., a^2 c_n^2 a_n)$, this proves $a \in D^t(a^2 a_1, a^2 c_2^2 a_2, ..., a^2 c_n^2 a_n)$. Now permute the entries of $\langle a^2 a_1, a^2 c_2^2 a_2, ..., a^2 c_n^2 a_n \rangle$ putting $a^2 c_2^2 a_2$ in the first position and repeat the argument (using the fact that $a^2 a^2 = a^2$). At the end of the process, we shall obtain $a \in D^t(a^2 a_1, ..., a^2 a_n)$.

d - Induction on $\dim(\varphi) = n$. If $\varphi = \langle a_1 \rangle$, the definition of $D(\langle a_1 \rangle)$ is suffice to show that $D(\langle c_1^2 a_1 \rangle) \subseteq D(\langle a_1 \rangle)$. Suppose that holds for $n-1$ and let $\varphi = \langle a_1 \rangle \oplus \langle a_2, ..., a_n \rangle$. Given $x \in D(c_1^2 a_1, ..., c_n^2 a_n)$, the inductive definition of representation provides $x \in D(c_1^2, a_1, y)$ for some $y \in D(c_2^2 a_2, ..., c_n^2 a_n)$, and from the induction hypothesis we get $y \in D(a_2, ..., a_n)$. Since $y = y^2 \cdot y$, axiom RS4 yields $x \in D(a_1, y)$, and hence $x \in D(\varphi)$.

e - Let $\varphi = \langle a_1, ..., a_k \rangle$ and $\psi = \langle a_{k+1}, ..., a_n \rangle$. We prove the both implications ($\Rightarrow$ and $\Leftarrow$) by induction on k:

($\Rightarrow$) If $k = 1$, $c \in D(\langle a_1 \rangle \oplus \langle a_2, ..., a_n \rangle)$ implies $c \in D(a_1, b)$ for some $b \in D(a_2, ..., a_n)$, so we can take $a = a_1$. Now, suppose the assertion valid for $k - 1 \geq 2$ and let $c \in D(\varphi \oplus \psi)$. Then $c \in D(a_1, d)$ for some $d \in D(\varphi' \oplus \psi)$, $\varphi' = \langle a_2, ..., a_k \rangle$. By induction, we have $d \in D(e, f)$, $e \in D(\varphi')$, $f \in D(\psi)$. By weak associativity we have $c \in D(g, f)$ for some $g \in D(a_1, e)$. Thus $g \in D(\varphi)$ so we can take $a = g$, $b = f$.

($\Leftarrow$) If $k = 1$ then $c \in D(a, b)$ with $a \in D(a_1)$ $b \in D(\psi)$ implies $a = d^2 a_1$ for some $d \in G$, so $c \in D(a_1, b)$ with $b \in D(\psi)$, hence $c \in D(\varphi \oplus \psi)$. Now, suppose the assertion valid for $k - 1 \geq 2$ and let $c \in D(a, b)$ with $a \in D(\varphi)$, $b \in D(\psi)$. Then $a \in D(a_1, d)$ for $d \in D(\varphi')$, $\varphi' = \langle a_2, ..., a_k \rangle$. By weak associativity $c \in D(a_1, e)$ for some $e \in D(d, b)$. By induction on k, $e \in D(\varphi' \oplus \psi)$. This proves $c \in D(\varphi \oplus \psi)$.

To proof the afirmation for D^t, just use the same argument replacing weak associativity by RS3.

f - Induction on $\dim(\varphi)$ using item (e).

g - First, note that by item (a) and transitivity of $\sim$ it suffices to prove the statement for $\varphi_2 = \psi_2 = \theta$. Further, by symmetry it suffices to show $D(\varphi_1 \oplus \theta) \subseteq D(\psi_1 \oplus \theta)$., which follows immediately from item (e). The same argument works in the case of D^t.

h - The inclusion $D^t(\varphi) \subseteq D^t(\varphi \oplus \varphi)$ is immediate from definition of representation and item (e). For the other inclusion we proceed by induction on $\dim(\varphi) = n$. If $\varphi = \langle b \rangle$ then $D^t(\varphi \oplus \varphi) = D^t(b, b)$, and the result follows from 5.2.14(15). Now, suppose that holds for $n-1$ and let $\varphi = \langle b \rangle \oplus \varphi'$. Since D^t does not depend on the order of the entries, $D^t(\varphi \oplus \varphi) = D^t(\langle b, b \rangle \oplus (\varphi' \oplus \varphi'))$. Let $a \in D^t(\varphi \oplus \varphi)$. By item (e), $a \in D^t(c, d)$ with $c \in D^t(b, b)$ and $d \in D^t(\varphi' \oplus \varphi')$. From 5.2.14(15) we get $c = b$, and the induction hypothesis gives $d \in D^t(\varphi')$. By item (e) again, $a \in D^t(\varphi)$.

The inclusion $D(\varphi) \subseteq D(\varphi \oplus \varphi)$ follows at once from $a \in D(a, a)$ and item (e). For the other inclusion, let $a \in D(\varphi \oplus \varphi)$. Item (c) implies that $a \in D^t(a^2\varphi \oplus a^2\varphi)$, which – by the above – coincides with $D^t(a^2\varphi)$. But $D^t(a^2\varphi) \subseteq D(a^2\varphi) \subseteq D(\varphi)$, and so $a \in D(\varphi)$, as required.

i - Induction on $\dim(\psi) = m$. Let $a \in D^t(\varphi)$, and $b \in D^t(\psi)$. If $\psi = \langle c \rangle$, then $b = c$, and item (b) implies $ac = ab \in D^t(c\varphi) = D^t(\varphi \otimes \psi)$. Now, suppose that holds for $n-1$ and let $\psi = \langle c \rangle \otimes \psi'$. Then, $b \in D^t(c, d)$ for some $d \in D^t(\psi')$, which frm $ab \in D^t(ac, ad)$. By induction hypothesis we also have $ad \in D^t(\varphi \otimes \psi')$. Hence $ab = D^t(\langle ac \rangle \oplus (\varphi \otimes \psi')) \subseteq D^t(c\varphi \oplus (\varphi \otimes \psi')) = D^t(\varphi \otimes \psi)$, as required. This fact and item (c) imply at once the same result for D.

j - (1)⇒(2) As the representation does not depend on the order of the entries, it suffices to show $-a_1 \in D^t(-a, a_2, ..., a_n)$. From $a \in D^t(a_1, ..., a_n)$ we get $a \in D^t(a_1, c)$ for some $c \in D^t(a_2, ..., a_n)$. Then by 5.2.14(2)

$$-a_1 \in D^t(-a, c) \text{ and } c \in D^t(a_2, ..., a_n),$$

so $-a_1 \in D^t(-a, a_2, ..., a_n)$.

(2)⇒(1) By symmetry, using the argument in (1)⇒(2) above.

(2)⇒(3) Is immediate from the definition of D and D^t.

(3)⇒(1) Since $-a_i \in D(\langle a_1, ..., a_{i-1}, -a, a_{i+1}, ..., a_n \rangle)$,

$$-a_i = -a_i a_i^2 \in D^t(a_1 a_i^2, ..., a_{i-1} a_i^2, -a a_i^2, a_{i+1} a_i^2, ..., a_n a_i^2)$$

so, using the implication (i)⇒(ii), $a a_i^2 \in D^t(a_1 a_i^2, ..., a_n a_i^2)$, for all $i = 1, ..., n$.

k - Induction on n, using 5.2.14(15) and 5.2.18(e).

□

Observe that the itens (a)-(g), (i) and the implications (1)⇔(2), (2)⇒(3) in the item (j) are valid on a pre-real semigroup.

Corollary 5.2.19. *The properties below holds in any real semigroup G, for arbitrary $a, b, c, x, y \in G$:*

a - $a \in D(b, c) \wedge b, c \in D(x, y) \Rightarrow a \in D(x, y)$.

b - $a \in D(b, c) \Leftrightarrow ab \in D(1, bc) \wedge ac \in D(1, bc) \wedge a^2 \in D(b^2, c^2)$.

Proof.

a - By assumption and by proposition 5.2.18(a), $a \in D(b, c) \subseteq D(x, y, x, y) = D(x, x, y, y)$. By 5.2.18(e) there are $p \in D(x, x)$ and $q \in D(y, y)$ such that $a \in D(p, q)$. From proposition

5.2.14(5) $p = x^2p$. Further, $xp \in D(x^2, x^2) \subseteq D(1, 1)$, and by 5.2.14(14) xp is an idempotent. Hence, we have

$$p = x^2p = x(xp) = x(x^2p^2) = x^3p^2 = xp^2.$$

Likewise, $q = yq^2$. Using RS4 we obtain $a \in D(p, q) = D(xp^2, yq^2) \subseteq D(x, y)$.

b - ($\Rightarrow$) Assume $a \in D(b, c)$. By RS8 and symmetry, only $ab \in D(1, bc)$ needs proof. Scaling by b in the assumption and using RS4 we get $ab \in D(b^2, bc) \subseteq D(1, bc)$.

($\Leftarrow$) Multiplying the first conjunction on the right-hand side by b and the second by c, gives $ab^2 \in D(b, b^2c)$ and $ac^2 \in D(c, bc^2)$. By RS4 both these sets are included in $D(b, c)$. Scaling $a^2 \in D(b^2, c^2)$ by a we obtain $a = a^3 \in D(ab^2, ac^2)$. Now use item (a) to conclude the desired.

□

5.2.3 RS-characters

Next we shall proceed to the construction of RS-characters with specific properties. These constructions will play a key role in the next sections.

Definition 5.2.20. *Let G be a PRS. A subset $S \subseteq G$ is saturated iff for all $a, b \in S$, $D_G(a, b) \subseteq S$.*

If $h : G \to H$ is a RS-homomorphism, $h^{-1}[0]$ is a saturated prime ideal of G, and if $H = \mathbf{3}$, then $h^{-1}[\{0, 1\}]$ is a saturated prime subsemigroup of G. The following lemma establishes some consequences of the definition of saturation.

Lemma 5.2.21. *Let G be a RS.*

a - If I is a saturated ideal of G and $a_1, ..., a_n \in I$ then $D_G(a_1, ..., a_n) \subseteq I$.

b - If S is a saturated subsemigroup of G then $a_1, ..., a_n \in S$ then $D_G(a_1, ..., a_n) \subseteq S$.

c - For any saturated subsemigroup S of G, $Id(G) = D_G(1, 1) \subseteq S$.

d - Any set of the form $D_G(a, b)$ is saturated. Those of the form $D_G(1, b)$ are, in addition, subsemigroups of G.

Proof. Itens (a) and (b) follows by induction on n, and item (c) is an immediately consequence of item (b). For the item (d), we have that $D_G(a, b)$ is saturated by 5.2.19(a). For the secont assertion in item (d), let $x, y \in D_G(a, b)$. By 5.2.18(i), $xy \in D_G(1, b, b, b^2)$. Hence by 5.2.18(e) there are elements $p \in D_G(1, b)$ and $q \in D_G(b, b^2)$ such that $xy \in D_G(p, q)$. From RS4 we get $q \in D_G(b, b^2) = D_G(1^2 \cdot b, b^2 \cdot 1) \subseteq D_G(1, b)$. Then, saturatedness entails $xy \in D_G(1, b)$. □

Of course, all the contents of lemma 5.2.21 holds on a PRS, except the fact that $\mathrm{Id}(G) = D_G(1, 1)$.

Proposition 5.2.22. *Let G be a RS.*

a - If $I \subseteq G$ is an ideal, then $[I] = \bigcup\{D_G(\varphi) : \varphi$ is a form with entries in $I\}$ is the smallest saturated ideal containing I.

b - If $S \subseteq G$ is a subsemigroup, then $[S] = \bigcup\{D_G(\varphi) : \varphi$ is a form with entries in $S\}$ is the smallest saturated subsemigroup containing S.

c - Let I be a saturated ideal and $x \in G$. Then

$$[I \cup x \cdot G] = \bigcup \{D_G(\langle i \rangle \oplus x\varphi) : i \in I \text{ and } \varphi \text{ is a form over } G\}.$$

d - Let S be a saturated subsemigroup and $x \in G$. Then

$$[S \cup x \cdot S] = \bigcup \{D_G(s, xt) : s, t \in S\}.$$

Proof. We shall write $I(x)$ for $X \cup x \cdot G$, and $S(x)$ for $S \cup x \cdot S$. For $A \subseteq G$, the expression "form over A" means a form with entries in A.

a - Let $J = \bigcup \{D(\varphi) : \varphi \text{ a form with entries in } I\}$. J is an ideal containing I. If $a, b \in J$ and φ, ψ are forms over I such that $a \in D(\varphi)$, $b \in D(\psi)$, then $D(a, b) \subseteq D(\varphi \oplus \psi)$ (by 5.2.18(e)) and $\varphi \oplus \psi$ is also a form over I, so that $D(a, b) \subseteq J$. Follow by 5.2.21(a) that any ideal containing I also contains J.

b - The proof is similar to that of item (a). To prove that the set on the right-hand side is multiplicative use 5.2.18(i).

c - We just need to prove $\subseteq$. It follows from item (a) that $a \in [I(x)]$ iff $a \in D(\varphi)$ for some form φ over $I(x)$. Since $D(\varphi)$ does not depend on the order of the entries of φ, there are forms φ_1 over I and φ_2 so that $D(\varphi) = D(\varphi_1 \oplus x\varphi_2)$. Let $a \in D(\varphi_1 \oplus x\varphi_2)$. Id $\dim(\varphi_1) = 0$ then $a \in D(x\varphi_2) \subseteq D(\langle 0 \rangle \oplus x\varphi_2)$, and a belongs to the right-hand side of the equation of item (c). If $\dim(\varphi_2) = 0$, then $a \in I$ because I is saturated and φ_1 has entries in I. If both φ_i's have positive dimension, then $a \in D(b, c)$ for some $b \in D(\varphi_1)$, $c \in D(x\varphi_2)$. Since I is saturated, $b \in I$, and a is in the right-hand side of the equation of item (c).

d - We just need to prove $\subseteq$. Arguing as in item (c), $a \in [S(x)]$ iff there are forms φ_1 and φ_2 over S such that $a \in D(\varphi_1 \oplus x\varphi_2)$. Then, $a \in D(b, c)$ for some $b \in D(\varphi_1)$, $c \in D(x\varphi_2)$. By letting $b = 1$, $c = a$ if $\dim(\varphi_1) = 0$ and $b = a$, $c = x$ if $\dim(\varphi_2) = 0$, and invoking saturatedness and 5.2.18(c) otherwise, in all cases we have $b \in S$ and $c = x^2c = x(xc)$. Since $xc \in D(x^2\varphi_2)$ and $x^2 \in S$, $x^2\varphi_2$ is a form over S and, by saturatedness again, $xc \in S$. Then, with $s = b$ and $t = xc$, the inclusion $\subseteq$ holds.

Note that all this also holds in a pre-real semigroup. □

Corollary 5.2.23. *Let M be a multiplicative subset of a RS, G, and let I be a saturated ideal disjoint from M. Let J be a saturated ideal containing I and maximal for being disjoint from M. Then J is prime. In particular, a saturated ideal maximal for not containing a given element is prime.*

Proof. Assume, towards a contradiction, that there are $a, b \notin J$ such that $ab \in J$. By the maximality assumption, $[J(a)] \cap M \neq \emptyset$ and $[J(b)] \cap M \neq \emptyset$. Let x and y be, respectively, in these sets. By proposition 5.2.22(c) there are $i, j \in J$ and forms φ_1, φ_2 such that $x \in D(\langle i \rangle \oplus a\varphi_1)$ and $y \in D(\langle j \rangle \oplus b\varphi_2)$. Hence

$$xy \in D((\langle i \rangle \oplus a\varphi_1) \oplus (\langle j \rangle \oplus b\varphi_2)).$$

Since $ab \in J$, all entries of the latter form are in J, which from, by saturatedness, $xy \in J$. But we also have $xy \in M$, contradictiong that $M \cap J = \emptyset$.

For the last assertion, let $M = D^t(\langle a^2 \rangle) = \{a^2\}$, where a is the element of G to be avoided. □

The following lemma is the analog of Lemma 5.2.5 for RS. This result, together with Lemma 5.2.6 below, are the main tools in constructing RS-characters.

Lemma 5.2.24. *Let G be a RS. Let $I \subseteq G$ be a saturated prime ideal. Let $S \subseteq G$ be a saturated subsemigroup maximal for the condition $S \cap -S = I$. Then, $S \cup -S = G$. Such an S determines a RS-character $h : G \to \mathbf{3}$, such that $h^{-1}[0] = I$ and $h^{-1}[0,1] = S$.*

Proof. Assume, towards a contradiction, that there is $a \in G \setminus (S \cup -S)$. By maximality of S we have $[S(a)] \cap -[S(a)] \supseteq I$ and $[S(-a)] \cap -[S(-a)] \supseteq I$. Let $x_1, x_2 \in G \setminus I$ be such that $\pm x_1 \in [S(a)]$ and $\pm x_2 \in [S(-a)]$; then $-x_1^2 \in [S(a)]$ and $-x_2^2 \in [S(-a)]$. By proposition 5.2.22(d) there are elements $s_1, s_2, t_1, t_2 \in S$ such that $-x_1^2 \in D^t(s_1, s_2 a)$ and $-x_2^2 \in D^t(t_1, t_2(-a))$. From RS6 we get $-x_1^2 \in D^t(x_1^2 s_1, x_1^2 s_2 a)$ and $-x_2^2 \in D^t(x_2^2 t_1, -x_2^2 t_2 a)$, which from, $-x_1^2 s_2 a \in D^t(x_1^2, x_1^2 s_1)$ and $x_2^2 t_2 a \in D^t(x_2^2, x_2^2 t_1)$. Since $a^2 \in S$, it follows that $x_1^2 x_2^2 s_2 t_2 a^2 \in S \cap -S = I$. Since I is prime and $x_1, x_2, a \notin I$, one of s_2 or t_2 must be in I. Suppose, for example, that $s_2 \in I$; then $s_2 a \in I \subseteq S$, and from $-x_1^2 \in D(s_1, s_2 a)$ we get $-x_1^2 \in S$. Thus, $x_1^2 \in S \cap -S = I$, a contradiction. Likewise, $t_2 \in I$ leads to a contradiction.

Now, to finalize the proof, get $h = h_S$ as the character constructed for the Lemma 5.2.5. □

Lemma 5.2.25. *Let G be a RS and let $a \in G$. If S is a saturated subsemigroup of G maximal for the condition $a \notin S$, then S is a prime subsemigroup. Such an S determines a RS-character $h : G \to \mathbf{3}$ such that $h^{-1}[0,1] = S$ and $h(a) = -1$.*

Proof. The strategy here, is use 5.2.24 with $I = S \cap -S$.

Claim 1. $-a^2 \notin S$. If $-a^2 \in S$, then

$$a \in D(1, -1) \Rightarrow a = a^3 \in D(a^2, -a^2) \subseteq S$$

a contradiction.

Claim 2. S is prime, i.e, if $b, c \notin S$ then $bc \notin S$. For this, suppose $bc \in S$. Since $b, c \notin S$, then by 5.2.22(d), there exists $r, s, t, v \in S$ such that $-a^2 \in D(r, bs)$ and $-a^2 \in D(t, cv)$. So $-a^2 \in D^t(a^2 r, a^2 bs)$ and $-a^2 \in D^t(a^2 t, a^2 cv)$, and $-a^2 bs \in D^t(a^2, a^2 r)$ and $-a^2 cv \in D^t(a^2, a^2 t)$. Then

$$bca^2 sv \in D^t(-a^2 rcv, -a^2 cv) \subseteq D^t(a^2 r, a^2 tr, a^2, a^2 t).$$

Thus, $bca^2 sv \in D^t(a^2 r, w)$ for some $w \in D^t(a^2 tr, a^2, a^2 t)$. Thus $w \in S$ and $-a^2 \in D^t(bca^2 sv, w) \subseteq S$, contradicting Claim 1.

The result now follows from Claim 2 and 5.2.24. □

5.2.4 Duality

Theorem 5.2.26 (The Duality Theorem)**.** *There is a functorial duality between the category $\mathcal{RS}$ of real semigroups with RS-morphisms and $\mathcal{ARS}$ of abstract real spectra with ARS-morphisms. Moreover, the duality establishes an equivalence between the categories $\mathcal{RS}$ and $\mathcal{ARS}^{op}$, the opposite category of $\mathcal{ARS}$.*

Theorem 5.2.27. *Let G be a RS and let $a \in G$. Then:*

a - If I is a saturated ideal of G not containing the element a, then there exists a RS-character h such that $h(a) \neq 0$ and $h(x) = 0$ for all $x \in I$.

b - If S is a saturated subsemigroup of G not containing the element a, then there exists a RS-character h such that $h(a) = -1$ and $h(x) \in \{0, 1\}$ for all $x \in S$.

Proof.

a - Using Zorn's Lemma get a saturated ideal J containing I and maximal for the condition $a \notin J$; $J$is prime (corollary 5.2.23). Let S be the saturated subsemigroup generated by $J \cup \mathrm{Id}(G)$. We claim that $S \cap -S = J$.

To see this, let $x \in S \cap -S$; then $-x^2 \in S$. By proposition 5.2.22, $-x^2 \in D_G(j, y^2)$ for some $j \in J$, $y \in G$. It follows that $-x^2 \in D^t_G(jx^2, y^2x^2)$. Scaling by y^2 we obtain $-x^2y^2 \in D^t_G(jx^2y^2, x^2y^2)$, and then $-jx^2y^2 \in D^t(x^2y^2, x^2y^2) = \{x^2y^2\}$, which from $x^2y^2 \in J$. Since J is prime, we have either $x \in J$ or $y \in J$. If $y \in J$, then saturatedness of J and the condition $-x^2 \in D_G(j, y^2)$ yield $x \in J$, as claimed.

Let T be a saturated subsemigroup containing S and maximal for the property $T \cap -T = J$. By lemma 5.2.24, h_T is a RS-character such that $h_T^{-1}[0] = J$. Since $a \notin J$, it follows that $h_T(a) \neq 0$.

b - Is an immediate consequence of Lemma 5.2.25.

□

Theorem 5.2.28. *Let G be a RS, and let $a, b \in G$. Then:*

a - If $a \notin D_G(1, b)$, then there is a RS-character $h \in X_G$ such that $h(b) \in \{0, 1\}$ and $h(a) = -1$.

b - If $a^2 \notin D_G(b^2, c^2)$, then there is a RS-character $h \in X_G$ such that $h(b^2) = h(c^2) = 0$ and $h(a^2) = 1$.

Proof.

a - Assume that $a \notin D(1, b)$. Since this set is a saturated subsemigroup of G, by theorem 5.2.27(b) there is a RS-character h such that $h(a) = -1$ and $h(x) \in \{0, 1\}$ for all $x \in D(1, b)$. In particular, $h(b) \in \{0, 1\}$.

b - Assume that $a^2 \notin D(b^2, c^2)$. Let I be the saturated ideal generated by b^2 and c^2. If $a \in I$, there are elements $x_1, ..., x_n, y_1, ..., y_k \in G$ such that $a \in D(b^2x_1, ..., b^2x_n, c^2y_1, ..., c^2y_k)$. Squaring this representation we obtain

$$a^2 \in D(b^2x_1^2, ..., b^2x_n^2, c^2y_1^2, ..., c^2y_k^2) \subseteq D(b^2, ..., b^2, c^2, ..., c^2) \subseteq D(b^2, c^2),$$

in contradiction to our assumption. Hence $a \notin I$. Theorem 5.2.27(a) gives a RS-character h such that $h(a) \neq 0$ and $h(x) = 0$ for all $x \in I$. In particular, $h(a^2) = I$ and $h(b) = h(c) = 0$.

□

Finally, the separation result that we actually need in the proof of theorem 5.2.26 is a consequence of the foregoing theorem, and takes the following form:

Theorem 5.2.29 (Separation theorem)**.** *Let G be a RS, and let $a, b, c \in G$. Then:*

a - $a \in D_G(a, b)$ iff for all $h \in X_G$, $h(a) \in D_{\mathbf{3}}(h(b), h(c))$.

b - $a \in D^t_G(a, b)$ iff for all $h \in X_G$, $h(a) \in D^t_{\mathbf{3}}(h(b), h(c))$.

c - *If $a \neq b$, there is $h \in X_G$ such that $h(a) \neq h(b)$.*

Proof.

a - We only need to prove the non-trivial implication $\Leftarrow$. Assume $a \notin D_G(b,c)$. By 5.2.19(b) this is equivalent to $ab \notin D(1,bc)$ or $ac \notin D(1,bc)$ or $a^2 \notin D(b^2,c^2)$. In the first case, 5.2.28(a) yields a character $h \in X_G$ such that $ab = -1$ and $h(bc) \in \{0,1\}$. The assumption $h(a) \in D_{\mathbf{3}}(h(b),h(c))$ yields $h(ab) = h(a)h(b) \in D_{\mathbf{3}}(h(b^2),h(bc))$. Note that $h(ab) = -1$ implies $h(b) \neq 0$, which from $h(b^2) = 1$. Thus, we have $-1 \in D_{\mathbf{3}}(1,h(bc))$ with $h(bc) \in \{0,1\}$, contrary to corollary 5.2.17. A similar argument also excludes the case $ac \notin D_G(1,bc)$. Finally, if $a^2 \notin D_G(b^2,c^2)$, 5.2.28(b) gives a character h such that $h(a^2) = 1$ and $h(b^2) = h(c^2) = 0$. The assumption $h(a) \in D_{\mathbf{3}}(h(b),h(c))$ yields, then, $\pm 1 \in D_{\mathbf{3}}(0,0)$, again in contradiction with corollary 5.2.17.

b - Is just consequence of item (a), using the definition of D^t in terms of D.

c - We consider two cases:

Case 1 - $a^2 = b^2$.

First remark that either $a \notin D_G(1,b)$ or $b \notin D_G(1,a)$. Oterwise, RS6 would imply $a \in D^t_G(a^2,a^2b) = D^t_G(b^2,b)$ and $b \in D^t_G(b^2,b^2a) = D^t_G(b^2,a)$, which from $-b^2 \in D^t_G(-a,b)$ and $-b^2 \in D^t_G(a,-b)$, respectively. From RS7 we conclude $a = b$, contrary to hypothesis.

Theorem 5.2.28(a) yields a character $h \in X_G$ such that $h(a) = -1$ and $h(b) \in \{0,1\}$ or $h(b) = -1$ and $h(a) \in \{0,1\}$. In both cases, $h(a) \neq h(b)$.

Case 2 - $a^2 \neq b^2$.

In this case we note that either $a^2 \notin D_G(b^2,b^2)$ or $b^2 \in D_G(a^2,a^2)$; otherwise, from RS6 we would have $a^2 \in D^t_G(a^2b^2,a^2b^2)$ and $b^2 \in D^t_G(a^2b^2,a^2b^2)$ and from 5.2.14(15), $a^2 = a^2b^2 = b^2$, absurd. In either case Theorem 5.2.28(b) yields a character h so that $h(b) = 0$ and $h(a^2) = 1$ or $h(b) = 1$ and $h(a) = 0$, as required.

□

We divide the assertion of theorem 5.2.26 in two minors theorems. The reason for this, is because the functorial analysis in the next sections.

Theorem 5.2.30. *Let $(G,\cdot,1,0,-1,D,D^t)$ be a RS. Let X_G be the set of RS-characters of G and $\overline{G}$ be the image under the evaluation map, i.e, $\overline{G} = \{\overline{a} : a \in G\}$, where $\overline{a} \in \mathbf{3}^{X_G}$ denotes the evaluation at a, i.e, for $\sigma \in X_G$, $\overline{a}(\sigma) = \sigma(a)$. Then $(X_G,\overline{G})$ is an ARS.*

Proof. Verification of the axioms for ARSs becomes an easy matters once it is establishes that our (axiomatically given) relation D_G coincides with the representation relation D_{X_G} defined in terms of X_G by the formula

$$\overline{c} \in D_{X_G}(\overline{a},\overline{b}) \Leftrightarrow \forall\, x \in X_G[\overline{c}(x) = 0 \vee \overline{a}(x)\overline{c}(x) = 1 \vee \overline{b}(x)\overline{c}(x) = 1], \qquad ([\mathrm{R}])$$

for $a,b,c \in G$. That is,

$$a \in D_G(b,c) \Leftrightarrow \overline{a} \in D_{X_G}(\overline{b},\overline{c}), \qquad (D)$$

or equivalently,

$$a \in D^t_G(b,c) \Leftrightarrow \text{ For every } h \in X_G(h(a) \in D_{\mathbf{3}}(h(b),h(c))).$$

This condition is precisely item (a) of theorem 5.2.29. Note that the corresponding condition for transversal representation, namely

$$a \in D^t_G(b,c) \Leftrightarrow \overline{a} \in D^t_{X_G}(\overline{b},\overline{c}). \qquad (D^t)$$

follows readily from item (b) of theorem 5.2.29 and the characterization of $D^t_{\mathbf{3}}$ in corollary 5.2.17.

Now we have:

AX1 - Follow by 5.2.29(c).

AX2 - This axiom says, in our terminology, that if S is a saturated subsemigroup of G verifying $-1 \notin S$, $S \cup -S = G$ and $S \cap -S$ is a prime ideal, then there is $h \in X_G$ such that $S = h^{-1}[\{0,1\}]$. This is just the last assertion of Lemma 5.2.24.

AX3 - Is simply our axiom RS3. The equivalence D^t is used here.

□

Corollary 5.2.31. *The correspondence* $(G,\cdot,1,0,-1,D,D^t) \mapsto (X_G,\overline{G})$ *provides a functor* $\Phi : \mathcal{RS} \to \mathcal{ARS}$.

Proof. We just need to treat about morphisms. The functor Given a RS-morphism $f : G \to H$, its dual $\Phi(f) = f^*$ is defined by composition: given $\sigma \in X_H$, we set $f^*(\sigma) = \sigma \circ f$.

The map $f^* : (X_H,\overline{H}) \to (X_G,\overline{G})$ is, indeed, a morphism of ARSs: for $a \in G$, we have

$$\overline{a} \circ f^* = \overline{f(a)}; \qquad (*)$$

in fact, for $\sigma \in X_H$,

$$(\overline{a} \circ f^*)(\sigma) = \overline{a}(f^*(\sigma)) = \overline{a}(\sigma \circ f) = (\sigma \circ f)(a) = \sigma(f(a)) = \overline{f(a)}(\sigma),$$

and the proof is complete. □

Theorem 5.2.32. *Let* (X,G) *be an ARS. Then the semigroup* $(G,\cdot,1,0,-1)$ *endowed with the representation relation* D_X *defined by [R] above (with* X_G *replaced by* X*) is a RS.*

Proof. The representation relation here is

$$\overline{c} \in D_X(\overline{a},\overline{b}) \Leftrightarrow \forall\, x \in X[\overline{c}(x) = 0 \vee \overline{a}(x)\overline{c}(x) = 1 \vee \overline{b}(x)\overline{c}(x) = 1],$$

for $a,b,c \in G$. Now, we will verify some axioms of RS:

RS 0 - Immediate.

RS 1 - Is just the fact that $\overline{a}(x)\overline{a}(x) = \overline{a}(x)^2 \in \{0,1\}$.

RS 2 - Let $\overline{c} \in D_X(\overline{a},\overline{b})$. Suppose that $\overline{c}(x)\overline{a}(x) = 1$ (the other cases are similar). Hence,

$$\overline{c}(x)\overline{d}(x)\overline{a}(x)\overline{d}(x) \in \{0,1\},$$

and this implies that $\overline{c}\overline{d} \in D_X(\overline{a}\overline{d},\overline{b}\overline{d})$.

RS 3 - Is just AX3.

The axioms RS4-RS8 follows by straightforward calculation as consequence of the fact that $\overline{a}(x)^2 \in \{0.1\}$ for all $a \in G$ and all $x \in X$ (as we make in RS2 case). □

Corollary 5.2.33. *The correspondence* $(X, G) \mapsto (G, \cdot, 1, 0, -1, D_X, D_X^t)$ *provides a functor* $\Psi : \mathcal{ARS} \to \mathcal{RS}$.

Proof. Again, we just need to treat about morphisms. We know that every ARS morphism $g : (Y, H) \to (X, G)$ induces a RS-morphism $g^* : G \to H$: for $a \in G$ put

$$g^*(a) = \text{ the unique } b \in H \text{ such that } a \circ g = b.$$

Now, the desired is consequence of making $\Psi(g) = g^*$. □

Proof of theorem 5.2.26. After 5.2.32, 5.2.30 and their corollaries, we just need to proof that $\Psi \circ \Phi \cong Id_{\mathcal{RS}}$ and $\Phi \circ \Psi \cong Id_{\mathcal{RS}}$. Of course, from 5.2.32 and 5.2.30 is immediate that $\Psi \circ \Phi = Id_{\mathcal{RS}}$ and $\Phi \circ \Psi = Id_{\mathcal{RS}}$ on objects of both categories. Then, we just need to prove this on the morphisms.

Let $f : G \to H$ be a RS-morphism. We must show that $\Phi(f^*) = f$, where $\Phi(f) = f^8 : (X_H, \overline{H}) \to (X_G, \overline{G})$, as defined in 5.2.33. Let $\Psi(f^*) = f'$. From the definition of Ψ on morphisms we have

$$\overline{a} \circ f^* = \overline{f'(a)} \text{ for } a \in G.$$

This equality, together with (*), yields $\overline{f(a)} = \overline{f'(a)}$ for $a \in G$. Since the evaluation map $a \mapsto \overline{a}$ is injective (theorem 5.2.29(c)) we get $f(a) = f'(a)$ for all $a \in G$, i.e, $f = f'$.

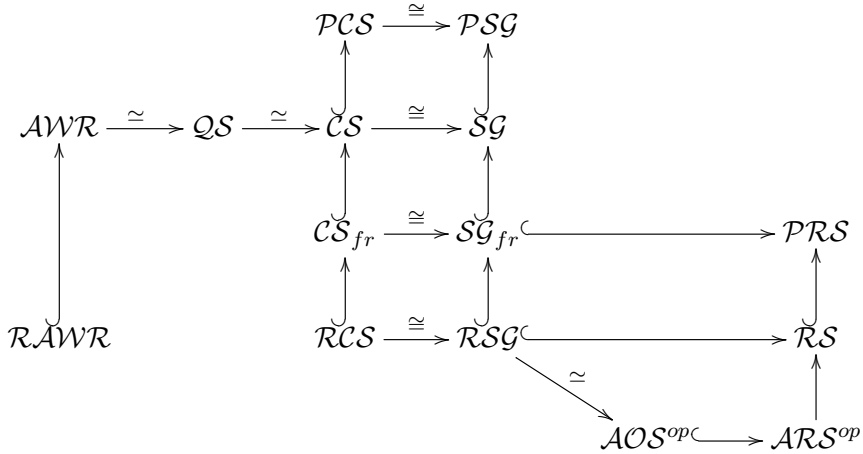
Let $f : (X, G) \to (Y, H)$ be an ARS-morphism. Given $x \in X$, we have

$$\Phi \circ \Psi(f)(x) = \Phi(b \circ f(x)) \overset{(*)}{=} \overline{f(x)} \cong f(x).$$

Here, $b \in H$ is the unique such that $b = a \circ f$ and $\overline{f(x)} \in \Phi(\Psi(H)) \cong H$. Hence, $\Psi \circ \Phi \cong Id_{\mathcal{RS}}$ and $\Phi \circ \Psi \cong Id_{\mathcal{ARS}}$, as desired. □

5.3 The Third Functorial Picture

At this moment, our functorial picture is like this:



Here $\mathcal{SG}_{fr}$ is the category of formally real special groups and and $\mathcal{CS}_{fr}$ the category of formally

real Cordes schemes. For us, $\mathcal{CS}_{fr}$ is just the image of the restriction

$$(\mathcal{SG} \xrightarrow{\cong} \mathcal{CS}) \restriction_{\mathcal{SG}_{fr}} .$$

The situation in the ring-theoretic case is drastically harder than the field case. We could observe that the axioms of real semigroups are more techinical and difficult to deal in comparison with the special group ones. Because this, there is less intuition and less space to work. We propose a new approach to this in the next chapter.

Chapter 6

New lands to explore

In this last chapter, we will witness which is, maybe, the most beauty aspect of quadratic forms theory: the capacity of abstractness the main theorems of the theory. In other words,

The change of point of view again, would produce a new first-order theory of quadratic forms!

Then, over this perspective, we will present the theory of multirings and multifields and "open the Chamber of The Secrets"!

6.1 An introduction to the Multivalued World

Here, we will present a new theory of Multirings and Multifields, created by M. Marshall and presented to us in his article [Mar06]. Multirings are just "rings with a multivalued addition". With this new approach, many ideas of the ring theory can be imported. We cover and present the entire article [Mar06].

6.1.1 Multigroups, Multirings and Multifields

Multigroups are a generalization of groups. We can think that a multigroup is a group with a multivalued operation:

Definition 6.1.1. *A multigroup is a quadruple $(G, *, r, 1)$, where G is a non-empty set, $* : G \times G \to \mathcal{P}(G) \setminus \{\emptyset\}$ and $r : G \to G$ are functions, and 1 is an element of G satisfying:*

i - *If $z \in x * y$ then $x \in z * r(y)$ and $y \in r(x) * z$.*

ii - *$y \in 1 * x$ iff $x = y$.*

iii - *With the convention $x * (y * z) = \bigcup_{w \in y*z} x * w$ and $(x * y) * z = \bigcup_{t \in x*y} t * z$,*

$$x * (y * z) = (x * y) * z \text{for all } x, y, z \in G.$$

A multigroup is said to be commutative if

iv - *$x * y = y * x$ for all $x, y \in G$.*

Example 6.1.2. *Suppose $(G, \cdot, 1)$ is a group. Defining $*(a, b) = \{c \in G : c = a \cdot b\}$ and $r(g) = g^{-1}$, we have that $(G, *, r, 1)$ is a multigroup.*

We have too, an another description to multigroups, due by Marshall in [Mar06]:

Definition 6.1.3. *A multigroup is a quadruple* $(G, \Pi, r, \mathfrak{i})$ *where* G *is a non-empty set,* Π *is a subset of* $G \times G \times G$*,* $r : G \to G$ *is a function and* $\mathfrak{i}$ *is an element of* G *satisfying:*

I - *If* $(x, y, z) \in \Pi$ *then* $(z, r(y), x) \in \Pi$ *and* $(r(x), z, y) \in \Pi$.

II - $(x, \mathfrak{i}, y) \in \Pi$ *iff* $x = y$.

III - *If* $\exists p \in G$ *such that* $(u, v, p) \in \Pi$ *and* $(p, w, x) \in \Pi$ *then* $\exists q \in G$ *such that* $(v, w, q) \in \Pi$ *and* $(u, q, x) \in \Pi$.

A multigroup is said to be commutative if

IV - $(x, y, z) \in \Pi$ *iff* $(y, x, z) \in \Pi$.

In fact, these definitions decribes the same object, and that connection is estabilished by the following lemma:

Lemma 6.1.4. *For any multigroup* G *as in the second version, we have:*

a - $r(\mathfrak{i}) = \mathfrak{i}$.

b - $r(r(x)) = x$.

c - $(x, y, z) \in \Pi$ *iff* $(r(y), r(x), r(z)) \in \Pi$.

d - $(\mathfrak{i}, x, y) \in \Pi$ *iff* $x = y$.

e - *If* $\exists q \in G$ *such that* $(v, w, q) \in \Pi$ *and* $(u, q, x) \in \Pi$ *then* $\exists p \in G$ *such that* $(u, v, p) \in \Pi$ *and* $(p, w, x) \in \Pi$.

f - *For each* $a, b \in G$*, there exists* $c \in G$ *such that* $(a, b, c) \in \Pi$.

Proof. a - As $i = i$, $(i, i, i) \in \Pi$ by II. By I, $(r(i), i, i) \in \Pi$ and by II, $r(i) = i$.

b - $x = x \overset{II}{\Rightarrow} (x, \mathfrak{i}, x) \in \Pi \overset{I}{\Rightarrow} (r(x), x, \mathfrak{i}) \in \Pi \overset{I}{\Rightarrow} (r(r(x)), \mathfrak{i}, x) \in \Pi \overset{II}{\Leftrightarrow} r(r(x)) = x$.

c - $(x, y, z) \overset{I}{\Leftrightarrow} (z, r(y), x) \in \Pi \overset{I}{\Leftrightarrow} (r(z), x, r(y)) \in \Pi \overset{I}{\Leftrightarrow} (r(y), r(x), r(z)) \in \Pi$.

d - Let $(\mathfrak{i}, x, y) \in \Pi$.

$$\begin{aligned}(\mathfrak{i}, x, y) \in \Pi &\overset{I}{\Rightarrow} (y, r(x), \mathfrak{i}) \in \Pi \overset{I}{\Rightarrow} (r(y), \mathfrak{i}, r(x)) \in \Pi \\ &\overset{I}{\Rightarrow} r(y) = r(x) \overset{(b)}{\Rightarrow} y = r(r(y)) = r(r(x)) = x.\end{aligned}$$

Conversely, suppose $x = y$.

$$\begin{aligned}x = y \Rightarrow r(x) = r(y) &\overset{II}{\Rightarrow} (r(y), \mathfrak{i}, r(x)) \in \Pi \\ &\overset{I+(b)}{\Rightarrow} (y, r(x), \mathfrak{i}) \in \Pi \overset{I}{\Rightarrow} (\mathfrak{i}, x, y) \in \Pi.\end{aligned}$$

e - $(u,q,x) \in \Pi \overset{I}{\Rightarrow} (x,r(q),u) \in \Pi \overset{(c)}{\Rightarrow} (q,r(x),r(u)) \in \Pi$. Then, $(v,w,q) \in \Pi$ and $(q,r(x),r(u)) \in \Pi$, so by axiom III, there exists $t \in G$ such that $(w,r(x),t) \in \Pi$ and $(v,t,r(u)) \in \Pi$.

$$(w,r(x),t) \in \Pi \overset{(b)}{\Rightarrow} (x,r(w),t) \in \Pi \overset{I}{\Rightarrow} (r(t),w,x) \in \Pi, \text{ and}$$
$$(v,t,r(u)) \in \Pi \overset{(b)}{\Rightarrow} (r(t),r(v),u) \in \Pi \overset{I}{\Rightarrow} (u,v,r(t) \in \Pi.$$

Hence Defining $p = r(t)$, we have $(u,v,p) \in \Pi$ and $(p,w,x) \in \Pi$.

f - Hence $(b,r(b),\mathfrak{i}) \in \Pi$ and $(a,\mathfrak{i},a) \in \Pi$, by (e), there exists $c \in G$ such that $(a,b,c) \in \Pi$ and $(c,r(b),a) \in \Pi$.

□

Now, let $(G,*,r,1)$ a multigroup in the sense 6.1.1. We can define a multigroup $(G,\Pi_*,r,\mathfrak{i})$ taking $\mathfrak{i} = 1$ and $\Pi_* = \{(a,b,c) : c \in a * b\}$. The validate of the axioms I,II, III (and IV) for $(G,\Pi_*,r,\mathfrak{i})$ are direct consequence of axioms i,ii, iii and (iv) in $(G,*,r,1)$.

Conversely, let $(G,\Pi,r,\mathfrak{i})$ a multigroup in the sense 6.1.3. By 6.1.4(f), the function $*_\Pi : A \times A \to \mathcal{P}(A) \setminus \{\emptyset\}$, gives by $*_\Pi(a,b) = a *_\Pi b := \{c \in G : (a,b,c) \in \Pi\}$ is well defined. Hence, Let $(G,*_\Pi,1)$ with $1 = \mathfrak{i}$. Then, the validate of the axioms i,ii (and iv) for $(G,*_\Pi,1)$ are direct consequence of I,II (and IV) for $(G,\Pi,r,\mathfrak{i})$. For the axiom iii, let $x \in a *_\Pi (b *_\Pi c)$. Then $x \in a *_\Pi q$ for some $q \in b *_\Pi c$. As $(b,c,q) \in \Pi$ and $(a,q,x) \in \Pi$, by 6.1.4(e), there exists $p \in \Pi$ such that $(a,b,p) \in \Pi$ and $(p,c,x) \in \Pi$ and then, $x \in p *_\Pi c$ with $p \in a *_\Pi b$ that imply $x \in (a *_\Pi b) *_\Pi c$. Finally, let $y \in (a *_\Pi b) *_\Pi c$. So $y \in p *_\Pi c$ for some $p \in a *_\Pi b$, then and $(a,b,p) \in \Pi$ and $(p,c,y) \in \Pi$. By III, there exists $q \in \Pi$ such that $(b,c,q) \in \Pi$ and $(a,q,y) \in \Pi$. Hence $y \in a *_\Pi q$ and $q \in b *_\Pi c$, that imply $y \in a *_\Pi (b *_\Pi c)$. Therefore, $(G,*_\Pi,1)$ is a multigroup in the sense 6.1.1.

From here, we will define multirings and study this structure with more details:

Definition 6.1.5. *A multiring is a sextuple $(R,+,\cdot,-,0,1)$ where R is a non-empty set, $+ : R \times R \to \mathcal{P}(R) \setminus \{\emptyset\}$, $\cdot : R \times R \to R$ and $- : R \to R$ are functions, 0 and 1 are elements of R satisfying:*

i - *$(R,+,-,0)$ is a commutative multigroup;*

ii - *$(R,\cdot,1)$ is a commutative monoid;*

iii - *$a0 = 0$ for all $a \in R$;*

iv - *If $c \in a + b$, then $cd \in ad + bd$. Or equivalently, $(a+b)d \subseteq ab + bd$. If the equality holds, i.e, $(a+b)d = ab + bd$, we said that R is an **hyperring**.*

R is said to be a multidomain if do not have zero divisors, and R will be a multifield if $1 \neq 0$ and every non-zero element of R has multiplicative inverse. We will use two conventions: if $Z, W \subseteq R$ and $x \in R$, $Z + W = \bigcup\{x + y : x \in Z,\ y \in W\}$ and $Z + x = Z + \{x\} = \bigcup\{z + x : z \in Z\}$.

Example 6.1.6.

a - *As in example 6.1.2(a), every ring, domain and field is a multiring, multidomain and multifield respectively.*

b - $Q_2 = \{-1, 0, 1\}$[1] *is a multifield with the usual product and the multivalued sum defined by relations*

$$\begin{cases} 0 + x = x + 0 = x, \text{ for every } x \in Q_2 \\ 1 + 1 = 1,\ (-1) + (-1) = -1 \\ 1 + (-1) = (-1) + 1 = \{-1, 0, 1\} \end{cases}$$

c - *Let* $K = \{0, 1\}$ *with the usual product and the sum defined by relations* $x + 0 = 0 + x = x$, $x \in K$ *and* $1 + 1 = \{0, 1\}$. *This is a multifield called Krasner's multifield [Jun18].*

Example 6.1.7. *Let be* $V \subseteq \mathbb{R}^n$ *an algebraic set and* A *as the coordinate ring of* V, *i.e, the ring* $\mathbb{R}[V]$ *of polinomial functions* $f : V \to \mathbb{R}$. *Define an equivalence relation* $\sim$ *on* A *by* $f \sim g \Leftrightarrow f(x)$ *and* $g(x)$ *has the same sign for all* $x \in V$. *Thus,* $Q_{red}(A) = A/\sim$ *is called the real reduced multiring. The operations are defined by:*

$$\begin{cases} \overline{f} \in \overline{g} + \overline{h} \Leftrightarrow \exists f', g', h' \in A \\ \qquad\qquad \text{such that } f' = g' + h',\ \overline{f'} = \overline{f},\ \overline{g'} = \overline{g},\ \text{and } \overline{h'} = \overline{h} \\ \overline{g}\overline{h} = \overline{gh},\ -\overline{f} = \overline{-f},\ 0 = \overline{0},\ 1 = \overline{1} \end{cases}$$

Taking $n = 1$, *we have a counter-example to show that* $ad + bd \subsetneq (a + b)d$ *in general:* $\overline{x^2 + x^3} \in \overline{x}\overline{x} + \overline{x}\overline{1}$ *but* $\overline{x^2 + x^3} \notin \overline{x}(\overline{x} + \overline{1})$, *and this not happen because* $x^2 + x^3 > 0$ *and* $x(x + 1) < 0$ *for* x *near to* 0 *with* $x \neq 0$ *(see [Mar06]).*

Example 6.1.8. *In the set* $\mathbb{R}_+$ *of positive real numbers, we define* $a \bigtriangledown b = \{c \in \mathbb{R}_+ : |a - b| \leq c \leq a + b\}$. *We have that* $\mathbb{R}_+$ *with the usual product and* $\bigtriangledown$ *multivalued sum is a multifield, called (real) triangle multifield [Vir10]. We denote this multifield by* $\mathcal{T}\mathbb{R}_+$. *Note that* $a \bigtriangledown 0 = \{a\}$ *and* $a \bigtriangledown a = \{x \in \mathbb{R}_+ : |x| \leq a\}$.

We have some different ways to generalize this construction. If $(F, \leq)$ *is an ordered field, we can define the triangle multifield* $\mathcal{T}F = (F_+, \bigtriangledown, \cdot, 0, 1)$, *by the same prescription,* $a \bigtriangledown b = \{c \in F_+ : |a - b| \leq c \leq a + b\}$. *Here,* $F_+ = \{a \in F : a \geq 0\}$. *If* (R, P) *is an ordered ring with* $supp(P) = \{0\}$ *(for example,* $\mathbb{Z}$*), we can define the triangle multiring* $\mathcal{T}R = (R_+, \bigtriangledown, \cdot, 0, 1)$, $a \bigtriangledown b = \{c \in R_+ : |a - b| \leq c \leq a + b\}$. *Again,* $R_+ = \{x \in R : x \geq 0\}$.

Example 6.1.9. *Let* $n \in \mathbb{N}$ *and define* $X_n = \{-n, ..., 0, ..., n\}$. *We define* $+ : X_n \times X_n \to \mathbb{P}(X_n) \setminus \{\emptyset\}$ *by:*

$$a + b = \begin{cases} \{sgn(ab) \max\{|a|, |b|\}\} \text{ if } a, b \neq 0 \\ \{a\} \text{ if } b = 0 \\ \{b\} \text{ if } a = 0 \\ \{-a, ..., 0, ..., a\} \text{ if } b = -a \end{cases},$$

and $\cdot : X_n \times X_n \to \mathbb{P}(X_n) \setminus \{\emptyset\}$ *by:*

$$a \cdot b = \begin{cases} sgn(ab) \max\{|a|, |b|\} \text{ if } a, b \neq 0 \\ 0 \text{ if } a = 0 \text{ or } b = 0 \end{cases}.$$

We will verify that $(X_n, +, \cdot, 0, 1)$ *is a multiring.*

i - *By construction,* $a + b = b + a$, $a + 0 = \{a\}$ *and* $0 \in a - a$ *for all* $a, b \in X_n$.

[1] According Marshall's notation in [Mar06].

ii - $d \in a+b \Leftrightarrow b \in d-a$: *We divide the proof in cases. Let* $a \neq -b$ *and suppose without loss of generality that* $|a| < |b|$. *Thus* $a+b = \{b\}$ *and* $a, b \in X_b = b-b$. *If* $a = -b$ *and* $d \in a-a$ *then* $|d| \leq |a|$. *Then* $a \in a+d$ *and* $-a \in -a+d$. *This proves* $\Rightarrow$. *For the converse* $\Leftarrow$, *just rewrite the above argument.*

iii - $(a+b)+c = a+(b+c)$: *Again we divide in cases. We suppose without loss of generality that* $a, b, c \neq 0$. *If* $a \neq -b$ *and* $b \neq -c$, $(a+b)+c = a+(b+c) = \{sgn(abc)\max\{|a|, |b|, |c|\}\}$.

Now let $a = -b$. *We want to prove that* $(a-a)+c = a+(-a+c)$. *If* $|a| \leq |c|$, $(a-a)+c = X_a + c = \{c\}$ *and* $a+(-a+c) = a+c = \{c\}$. *If* $|c| < |a|$, *then* $(a-a)+c = X_a + c = X_a$ *and* $a+(-a+c) = a-a = X_a$. *The case* $b = -c$ *is analogous.*

iv - *Again, by construction* $(X_n, \cdot, 1)$ *is a commutative monoid and* $a \cdot 0 = 0$ *for all* $a \in X_n$.

v - $d(a+b) \subseteq da+db$: *If* $d = 0$ *there is nothing to prove. Let* $d \neq 0$. *If* $a \neq -b$, *suppose without loss of generality that* $|a| < |b|$. *Then* $a+b = \{b\}$ *and* $d(a+b) = \{db\} = db+db$.

Now let $a = -b$. *We have two cases:*

(a) $|d| \leq |a|$: *since* $da = sgn(da)|a|$, *we have* $da-da = X_{da} = X_a$ *and* $d(a-a) = dX_a \subseteq X_a$.

(b) $|d| > |a|$: *since* $da = sgn(da)|d|$, *we have* $da-da = X_{da} = X_d$ *and* $d(a-a) = dX_a \subseteq X_d$.

Thus X_n *is a multiring (that is not a hyperring if* $n \geq 1$*!). In fact,* X_n *is a real reduced multiring for all* $n \geq 1$. *Now define* $X_{\mathbb{N}} = \bigcup_{n\in\mathbb{N}} X_n$. $X_{\mathbb{N}}$ *is a real reduced multiring too, and we can think that this is a "graded multiring".*

Lemma 6.1.10. *Let* F *be a multifield. Then* $(a+b)d = ad+bd$ *for every* $a, b, d \in F$.

Proof. We have $(a+b)d \subseteq ad+bd$ already. For the other inclusion, if $d = 0$, it is done. If $d \neq 0$, we have:

$$(ad+bd)d^{-1} \subseteq (ad)d^{-1} + (bd)d^{-1} = ad+bd \Rightarrow$$
$$ad+bd = [(ad+bd)d^{-1}]d \subseteq (a+b)d.$$

□

Now, we treat about morphisms:

Definition 6.1.11. *Let* A *and* B *multirings. A map* $f : A \to B$ *is a morphism if for all* $a, b, c \in A$:

i - $c \in a+b \Rightarrow f(c) \in f(a)+f(b)$;

ii - $f(-a) = -f(a)$;

iii - $f(0) = 0$;

iv - $f(ab) = f(a)f(b)$;

v - $f(1) = 1$.

For multirings, there are various sorts of "substrucutre" that one can consider. If A, B are multirings, we say A is embedded in B by the morphism $\iota : A \to B$ if ι is injective. We say A is strongly embedded in B if A is embedded in B and, for all $a, b, c \in A$, $\iota(c) \in \iota(a)+_B\iota(b) \Rightarrow c \in a+_Ab$. We say A is a submultiring of B if A is strongly embedded in B and, for all $a, b \in A$ and all $c \in B$, $c \in \iota(a) +_B \iota(b) \Rightarrow c \in \iota(A)$. Note that in the rings case, these all definitions coincide.

The category of multifields (respectively multirings) and theirs morphisms will be denoted by $\mathcal{MF}$ (respectively $\mathcal{MR}$).

Some of the properties of rings morphisms are not extend to multirings morphisms. Next, are some counterexamples:

Example 6.1.12.

a - *Let $f : A \to B$ be a multiring morphism. Define*

$$Ker(f) := \{a \in A : f(a) = 0\}.$$

$Ker(f)$ is a submultiring of A.

b - *Let $f : A \to B$ be a multiring morphism. If f is injective, them $Im(f) := \{f(a) : a \in A\}$ is embedded in B, but is not a strong embedding and $Im(f)$ is not a submultiring of B in general. For example, let R be a ring and define a very trivial multioperation $*$ by $a * 0 = \{a\}$ for all $a \in R$ and $a * b = R$ if $a, b \neq 0$. $(R, *, \cdot, 0, 1)$ is a multiring, and considering R as a multiring, the embedding $(R, +, \cdot, 1, 0) \hookrightarrow (R, *, \cdot, 0, 1)$ is a bijective multiring morphism that is a strong embedding but $(R, +, \cdot, 1, 0)$ is not a submultiring of $(R, *, \cdot, 0, 1)$. If we consider K as in 6.1.6(b), the inclusion $K \hookrightarrow (R, *, \cdot, 0, 1)$ is a multiring morphism that is an embedded and is not a strong embedding.*

c - *Let $f : \mathbb{R} \to Q_2$ be $f(x) = sgn(x)$, (with convention that $sgn(0) = 0$). f is a multiring morphism, but f is not injective and $Ker f = \{0\}$. Also $\mathbb{R}/Ker f$ is not isomorphic to Q_2.*

d - *The inclusions functions $Q_2 \hookrightarrow \mathbb{R}$ and $\mathcal{T}\mathbb{R}_+ \hookrightarrow \mathbb{R}$ are not multiring morphisms.*

e - *The inclusion function $\iota : K \to Q_2$ (K as in 6.1.6(b)) is not a multiring morphism.*

6.1.2 Commutative Multialgebra

In the sequel, we will extend some terminology of commutative algebra from multirings and multifields. As expected, many concepts such that morphisms, ideals, fractions and localizations has a natural generalization for multirings. We treat of them and explain some pathologies that appears in the multivalued world.

Definition 6.1.13. *An ideal of a multiring A is a non-empty subset of A such that $\mathfrak{a} + \mathfrak{a} \subseteq \mathfrak{a}$ and $A\mathfrak{a} = a$. An ideal $\mathfrak{p}$ of A is said to be prime if $1 \notin \mathfrak{p}$ and $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. An ideal $\mathfrak{m}$ is maximal if $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A \Rightarrow \mathfrak{a} = \mathfrak{m}$ or $\mathfrak{a} = A$. We will denote $Spec(A) = \{\mathfrak{p} \subseteq A : \mathfrak{p}$ is a prime ideal$\}$.*

With the notion of ideal, we can define some new multirings structures with the language of commutative algebra in mind:

Definition 6.1.14.

a - *If $\{A_i\}_{i \in I}$ is a family of multirings, then the product $\Pi_{i \in I} A_i$ is a multiring in the natural (componentwise) way.*

b - *Let $\mathfrak{a} \subseteq A$ an ideal. Elements of $A/\mathfrak{a}$ are cosets $\overline{a} = a + \mathfrak{a}$, $a \in A$. We define a multiring structure on $A/\mathfrak{a}$ by $\overline{a} + \overline{b} = \{\overline{c} : c \in a + b\}$, $-\overline{a} = \overline{-a}$, the zero and the unit element of $A/\mathfrak{a}$ are $0 = \overline{0}$ and $1 = \overline{1}$ respectively and mutiplication on $A/\mathfrak{a}$ is defined by $\overline{a}\overline{b} = \overline{ab}$.*

c - Let S be a multiplicative set in A. Elements of $S^{-1}A$ have the form a/s, $a \in A$, $s \in S$, $a/s = b/t$ iff $atu = bsu$ for some $u \in S$. $0 = 0/1$, $1 = 1/1$ and the operations are defined by $(a/s) \cdot (b/t) = ab/st$, and $c/u \in a/s + b/t$ iff $cstv \in atuv + bsuv$ for some $v \in S$.

d - If D is a multidomain, we define the multifield of fractions $ff(D) := (D \setminus \{0\})^{-1}D$.

Now, we present a construction that will be used several times below:

Definition 6.1.15. *Fix a multiring A and a multiplicative subset S of A. Define an equivalence relation $\sim$ on A by $a \sim b$ iff $as = bt$ for some $s, t \in S$. Denote by $\overline{a}$ the equivalence class of a and set $A/_m S = \{\overline{a} : a \in A\}$. Defining $\overline{a} + \overline{b} = \{\overline{c} : cv \in as + bt$, for some $s, t, v \in S\}$, $-\overline{a} = \overline{-a}$, and $\overline{a}\overline{b} = \overline{ab}$ we have that $(A/_m S, +, \cdot, -, \overline{0}, \overline{1})$ is a multiring, called **the Marshall's quotient** of A by S. When A is a multifield and $S = \sum A^{*2}$, we will denote $A/_m \sum A^{*2} = Q_{red(A)}$.*

Let S be a non-empty subset of a multiring A. We define the **ideal generated by** S as $\langle S \rangle := \bigcap \{\mathfrak{a} \subseteq A \text{ ideal} : S \subseteq \mathfrak{a}\}$. If $S = \{a_1, ..., a_n\}$, we easily check that

$$\langle a_1, ..., a_n \rangle = \sum Aa_1 + ... + \sum A_n, \text{ where } \sum Aa = \bigcup_{n \geq 1} \{\underbrace{a + ... + a}_{n \text{ times}}\}.$$

If A satisfy the second-half distributive, then $\sum Aa = Aa$.

Lemma 6.1.16.

a - An ideal $\mathfrak{p}$ of a multiring A is prime iff $A/\mathfrak{p}$ is a multidomain.

b - An ideal $\mathfrak{m}$ of a multiring A is maximal iff $A/\mathfrak{m}$ is a multifield.

c - Every ideal maximal is prime.

Proof. The proof is the same of the ring case. □

We cite the following proposition:

Proposition 6.1.17. *For any multiring A, $Spec(A)$ has a natural topology giving it the structure of a spectral space [Hoc69]. Basic open sets have the form $D(a) := \{\mathfrak{p} \in Spec(A) : a \notin \mathfrak{p}\}$.*

We do not deal with spectral spaces here, but there is an excellente and recent book about this subject [DST19].

6.1.3 Ordering Structures and Artin-Schreier

The standart Artin-Schreier theory (as presented in chapter 2) can be extended to the multifield theory.

Definition 6.1.18. *Let F be a multifield. A subset P of F is called an ordering if $P + P = \subseteq P$, $P \cdot P \subseteq P$, $P \cup -P = F$ and $P \cap -P = \{0\}$. The real spectrum of a multifield F, denoted $Sper(F)$, is defined to be the set of all orderings of F.*

Proposition 6.1.19. *$Sper(F)$ has a natural topology giving it the structure of a Boolean space. The sets $U(a) := \{P \in Sper(F) : a \notin P\}$, $a \in F$, are a subbasis for the topology.*

Proof. Analogous to proposition 6.1.17. □

Definition 6.1.20. *A preordering of a multifield F is defined to be a subset T of F satisfying $T+T \subseteq T$, $T \cdot T \subseteq T$ and $F^2 \subseteq T$. Here, $F^2 := \{a^2 : a \in F\}$. A multifield F is said to be real if $-1 \notin \sum F^2$. If F is real, then $-1 \neq 1$. A preordering T of F is said to be proper if $-1 \notin T$.*

Lemma 6.1.21. *Suppose F is a multifield with $-1 \neq 1$. For a preordering T of F, the following are equivalent:*

i - T is proper.

ii - $T \neq F$.

Proof. $(i) \Rightarrow (ii)$ is just the definition. For $(ii) \Rightarrow (i)$, suppose that $-1 \in T$ and let $a \in F$. If $a = 0$ then $a \in T$. Suppose $a \neq 0$. Fix $b \in 1+a$. Then $b^2 \in 1+a+a+a^2$, so $b^2 \in 1+u+a^2$, $u \in a+a$. Then $u \in b^2 - 1 - a^2 \in T$. $u/a \in 1+1$, so $u/a \in T$. Since $-1 \neq 1$, $u \neq 0$ and $\dot{T}$ is a subgroup of $\dot{F}$, then $a/u = (u/a)^{-1} \in T$. Hence $a = (a/u)u \in T$. □

Lemma 6.1.22.

a - A preordering which is maximal and proper is an ordering.

b - F has ordering if and only if F is real.

Proof. a - Let P be a preordering of the multifield F which is maximal and proper. If $a \in F$, then $P - aP$ is also a preordering. If $-1 \in P - aP$, then there exists $s, t \in P$ such that $-1 \in s - at$. If $t = 0$, then $-1 = s \in P$, a contradiction. Thus $t \neq 0$. Then $at \in 1+s$, so $a \in 1/t + s/t \subseteq P$. If $-1 \notin P - aP$, then by maximality of P, $-a \in P$. This proves that $P \cup -P = F$. If $s \in P \cap -P$, $s \neq 0$, then $s = -t \in P$, so $-1 = s/t \in P$, contradiction. This proves that $P \cap -P = \{0\}$.

b - By Zorn's lemma, every preordering is containing in an ordering. This fact with the item (a) proves the desired.

□

For a preordering T of F, we will denote by X_T the set of all orderings of F with $T \subseteq F$.

Proposition 6.1.23. *Let F be an multifield and T a proper preordering of F. Then $T = \bigcap_{P \in X_T} P$, where $X_T = \{P \in Sper(F) : T \subseteq P\}$.*

Proof. The inclusion "$\subseteq$" is immediate. For the inclusion "$\supseteq$", fix $a \in F$, $a \notin T$. Then $T - aT$ is a proper preordering of F (the argument is the same of 6.1.22). By the Zorn's lemma, there exists a maximal and proper preordering P such that $T - aT \subseteq P$. By 6.1.22, P is an ordering, and $-a \in P$, so $a \notin P$. □

6.1.4 Real Reduced Multifields

Consider the multifield Q_2. $\{0, 1\}$ is an ordering on Q_2. For any ordering P on a multifield F, $Q_P(F) = F/mP \cong Q_2$ by a unique isomorphism. Orderings of a multifield F correspond bijectively to a multiring homomorphism $\sigma : F \to Q_2$ via $P = \sigma^{-1}(\{0, 1\})$.

Proposition 6.1.24. *For a real multifield F are equivalent:*

a - The multiring morphism $F \to Q_{red}(F)$ is an isomorphism;

b - $\sum F^2 = \{0, 1\}$;

c - For all $a \in F$, $a^3 = a$ and $(a \in 1+1) \Rightarrow (a = 1)$.

Proof. (a)⇔(b) Is just the general fact that if $\sigma : F \to K$ is a morphism of real multifields, then $\sigma\left(\sum F^2\right) \subseteq \sum K^2$ and that $\sum Q_{red}(F)^2 = \{0,1\}$.

(a)⇒(c) $Q_{red}(F)$ already satisfy $a^3 = a$ for all a and $1+1 = \{1\}$.

(c)⇒(b) We have $a^2 = 1$ for all $a \neq 0$ and $\underbrace{1+1+...+1}_{n} = \{1\}$ by induction on n. It follows that $\sum F^2 = F^2 = \{0,1\}$. □

Definition 6.1.25. *A multifield F is said to be real reduced if satisfies the equivalent conditions of proposition 6.1.24.*

A morphism of real reduced multifield is just a morphism of multifields. The category of real reduced multifields will be denoted by $\mathcal{MF}_{red}$.

Corollary 6.1.26. *A multifield F is real reduced if and only if $a^3 = a$ for all $a \in F$ and $a \in 1+1 \Rightarrow a = 1$.*

Proof. (⇒) is already done. For (⇐), by proposition 6.1.24 is suffice to prove that F is real. Therefore, suppose that $a^3 = a$ for all $a \in F$ and $a \in 1+1 \Rightarrow a = 1$. Then $\sum F^2 = \{0,1\}$. If $-1 \in \{0,1\}$, then $-1 = 0$, so $1 = 0$ or $-1 = 1$, so $0 \in 1+1 = \{1\}$. In both cases, we conclude that $1 = 0$, contradiction. Thus $-1 \notin \sum F^2$, then F is real. □

For any proper preordering T of a real reduced multifield F, $Q_T(F)$ is a real reduced multifield. In particular, $Q_{red}(F)$ is a real reduced multifield. If $p : F_1 \to F_2$ is a multiring homomorphism of real multifields, then p induces a morphism $Q_{red}(F_1) \to Q_{red}(F_2)$. In this way, Q_{red} defines a functor (a reflection) from the category of real multifields onto the subcategory of real reduced multifields.

Proposition 6.1.27. *Let F be a real reduced multifield, $T = \sum F^2$. For any $a, b \in \dot{F}$,*

$$(a+b)^* = (Ta+Tb)^* = \{c \in \dot{F} : \forall\, \sigma \in \mathit{Sper}(F),\ \sigma(c) = \sigma(a),\ \mathit{or}\ \sigma(c) = \sigma(b)\}.$$

Proof. Since F is a real reduced multifield, $T = \{0,1\}$, so $Ta+Tb = \{0,a,b\} \cup (a+b)$. In particular, $F = T-T = \{0,1,-1\} \cup (1-1)$. To prove $(a+b)^* = (Ta+Tb)^*$, it remais to show $a, b \in a+b$. By symmetry, it suffices to show $a \in a+b$. If $a \neq \pm b$, then $b/a \neq \pm 1$ so $b/a \in 1-1$, i.e, $b \in a-a$ and so $a \in a+b$. If $a = b$, $1 \in 1+1 \Rightarrow a \in a+a = a+b$, and if $a = -b$, $-b \in -b-b \Rightarrow a \in a-b \Rightarrow a \in a+b$. Therefore $(a+b)^* = (Ta+Tb)^*$.

If $c \in Ta+Tb$, then $\sigma(a) = \sigma(b)$ implies that $\sigma(c) = \sigma(a)$. Thus $\sigma(c) = \sigma(a)$ or $\sigma(c) = \sigma(b)$ for any $\sigma \in \mathrm{Sper}(F)$. Conversely suppose this holds for any σ. Then $\sigma(b/a) = 1$ implies $\sigma(c/a) = 1$ for any σ, so by proposition 6.1.23, $c/a \in T + T(b/a)$. Multiplying by a, this yields $c \in Ta+Tb$ as required. □

Real reduced multifields have a natural representation in terms of functions:

Theorem 6.1.28 (Local-Global principle)**.** *For any real reduced multifield F, the natural embedding $F \hookrightarrow Q_2^{\mathit{Sper}(F)}$ is a strong embedding.*

Proof. Let F be a real reduced multifield and $T = \sum F^2 = \{0,1\}$. By proposition 6.1.23, $\{0,1\} = \bigcap_{P \in X_T} P$ (in other words, 1 is the unique element that is positive in all orderings). Hence, if $\sigma(a) = \sigma(b)$ for all $\sigma \in X_T$, then ab is positive in all orderings, so $ab = 1$ and as $a^2 = 1$, we have

$a = b$. Therefore, the multiring morphism from F to $Q_2^{\mathrm{Sper}(F)}$ defined by $a \mapsto (\sigma(a))_{\sigma \in \mathrm{Sper}(F)}$ is injective.

It remais to show that if $\sigma(c) \in \sigma(a) + \sigma(b)$ for all $\sigma \in \mathrm{Sper}(F)$ then $c \in a + b$. If $a = 0$, then $\sigma(c) = \sigma(b)$ for all $\sigma \in X_T$, so by the argument above. $b = c$. Similarly, if $b = 0$ then $c = a$ and if $c = 0$, then $b = -a$. Suppose now that a, b, c are not zero. Then $c \in a+b$ by proposition 6.1.27. □

In particular, for any real reduced multifield, $\mathrm{Sper}(F)$ separate points of F and $c \in a + b \subseteq F$ if and only if, for every $\sigma : F \to Q_2$, $\sigma(c) \in \sigma(a) + \sigma(b)$.

6.1.5 The Positivstellensatz

We define the real spectrum of a multiring and prove an abstract version of the positivstellensatz.

Let A be a multiring. A subset P of A is an *ordering* if $P + P \subseteq P$, $PP \subseteq P$, $P \cup -P = A$ and $P \cap -P$ is a prime ideal of A (called the *support* of A). Orderings of a multiring A correspond bijectively to multiring homomorphisms $\sigma : A \to Q_2$ via $P = \sigma^{-1}(\{0, 1\})$. For a prime ideal $\mathfrak{p}$ of A, orderings on A having support contained in $\mathfrak{p}$ (resp., containing $\mathfrak{p}$, resp., equal to $\mathfrak{p}$) correspond bijectively to orderings on the localization of A (resp., on $A/\mathfrak{p}$, on $ff(A/\mathfrak{p})$). The *real spectrum* of A, denoted $\mathrm{Sper}(A)$, is the set of all orderings of A.

Proposition 6.1.29. *Sper(A) is endowed with a natural topology making it a spectral space. The sets $U(a) := \{\sigma \in Sper(A) : \sigma(a) = 1\}$, $a \in A$, are a subbasis for the topology.*

Proof. Analogous to proposition 6.1.17. □

A *preordering* of a multiring A is a subset T of A satisfying $T + T \subseteq T$, $TT \subseteq T$ and $A^2 \subseteq T$. A preordering T of A is said to be *proper* if $-1 \notin T$. Every ordering is a proper preordering. $\sum A^2$ us a preordering, and is the unique smallest preordering of A. A multiring A is said to be *semireal* if $-1 \notin \sum A^2$.

Fix a preordering T of A. Define $X_T := \{\sigma \in \mathrm{Sper}(A) : \sigma(T) = \{0, 1\}\}$. A *$T$-module* in A is defined to be a subset M of A satisfying $M + M \subseteq M$, $TM \subseteq M$, and $1 \in M$ (so $T \subseteq M$).

Proposition 6.1.30. *Suppose T is a preordering of A and M is a T-module in A which is maximal subject to $-1 \notin M$. Then $M \cap (-M)$ is a prime ideal of A, and $M \cup (-M) = A$.*

Proof. First we show that $\mathfrak{p} = M \cap -M$ is an ideal. Let $M' = \{a \in A : (a + a) \cap M \neq \emptyset\}$. Then $M' \supseteq M$ and M' is a T-module. If $-1 \in M'$, then $(-1 - 1) \cap M \neq \emptyset$, say $a \in (-1 - 1) \cap M$. Then $-1 \in 1 + a \subseteq M$, a contradiction. Thus $-1 \notin M'$. By maximality of M, $M = M'$. By construction, we have $\mathfrak{p} + \mathfrak{p} \subseteq \mathfrak{p}$, $-\mathfrak{p} = \mathfrak{p}$ and $T\mathfrak{p} \subseteq \mathfrak{p}$. Suppose $a \in A$, $b \in \mathfrak{p}$ are given. Fix $c \in 1 + a$. Then $c^2 \in 1 + a + a + a^2$, so $c^2 \in 1 + d + a^2$ for some $d \in a + a$. Then $d \in c^2 - 1 - a^2$, so $db \in c^2b - b - a^2b \subseteq \mathfrak{p} \subseteq M$. At same time, $db \in (a + a)b \subseteq ab + ab$. This proves $ab \in M' = M$. A similar argument shows that $ab \in -M$. Thus $ab \in M \cap -M = \mathfrak{p}$. This proves that $\mathfrak{p}$ is an ideal of A.

Next we show that $\mathfrak{p}$ is prime. Suppose $ab \in \mathfrak{p}$, $a \notin \mathfrak{p}$, $b \notin \mathfrak{p}$. Replacing a by $-a$ and b by $-b$ if necessary, we can assume $a \notin M$, $b \notin M$. Thus -1 lies in the T-module $M + \sum aT$ and also in the T-module $M + \sum bT$. Then $-b^2 \in Mb^2 + \sum ab^2T \subseteq M$ (using the fact that $ab \in \mathfrak{p}$), so $b^2 \in \mathfrak{p}$. Writing $-1 \in q + c$, $q \in M$, $c \in \sum bt_i$, $t_i \in T$, we have $-c \in 1 + q$, so $c^2 \in 1 + q + q + q^2$. on the other hand, $c^2 \in \sum b^2t_it_j \subseteq \mathfrak{p}$. This implies $-1 \in -c^2 + q + q + q^2 \subseteq M$, a contradiction. This proves that $\mathfrak{p}$ is a prime ideal.

Finally, we prove that $A = M \cup -M$. Suppose $a \in A$ with $a \notin M$ and $a \notin -M$. Then $-1 \in M + \sum aT$ and $-1 \in M - \sum aT$. Multiplying by a^2, and noting that $a(\sum aT) \subseteq T$, this yelds $-a^2 \in M + t_1 a - a^2$ and $-a^2 \in M - t_2 a$, for some $t_1, t_2 \in T$. Then $-t_1 a \in a^2 + M \subseteq M$, and $t_2 a \in a^2 + M \subseteq M$, so $t_1 t_2 a \in \mathfrak{p}$. This is not possible. If either of t_1 or t_2 is in $\mathfrak{p}$, then $-a^2 \in M$, so $-1 \in M + \sum aT \Rightarrow a \in -M + \sum(-a^2)T$, and $-1 \in M - \sum aT \Rightarrow -a \in M + \sum(-a^2)T$, then $a \in \mathfrak{p}$. If $a \in \mathfrak{p}$, then $a \in M$ (and also $a \in -M$), which contradiction our assumption. This proves $A = M \cup -M$. □

Corollary 6.1.31. *Sper$(A) \neq \emptyset$ if and only if $-1 \notin \sum A^2$. For a preordering T of A, $X_T \neq \emptyset$ if and only if T is proper.*

Proof. The first assertion follows from the second. If $X_T \neq \emptyset$ then clearly T is proper. Suppose now that T is proper. Use Zorn's lemma to choose a maximal proper preordering P in A with $T \subseteq P$, and a P-module M of A maximal subject to $-1 \notin M$. If $P \neq M$ then for any $a \in M \setminus P$, $P + \sum aP$ is a preordering and $P + \sum aP \subseteq M$, so $P + \sum aP$ is proper. This contradicts the maximality of P. It follows that $P = M$. Proposition 6.1.30 implies that P is an ordering. □

For a fixed preordering T of A we have a multiring homomorphism $A \to Q_2^{X_T}$ (the product multiring), given by $a \mapsto \overline{a}$, where $\overline{a}$ is defined by $\overline{a}(\sigma) = \sigma(a)$ for all $\sigma \in X_T$.

Proposition 6.1.32. *Suppose $c, d \in A$. Then $\overline{c} \geq 0 \Rightarrow \overline{d} = 0$ holds on X_T (i.e, $\sigma(c) \geq 0 \Rightarrow \sigma(d) = 0$) if and only if $-d^{2k} \in T + \sum A^2 c$ for some integer $k \geq 0$.*

Proof. ($\Rightarrow$) Let $B = S^{-1}A$, $T' = S^{-1}T$, where $S := \{d^{2k} : k \geq 0\}$, and consider the T-module $T + \sum A^2 c$ and the T'-module $T' + \sum B^2 c$. If $-S \cap (T + \sum A^2 c) = \emptyset$, then $-1 \notin T' + \sum B^2 c$, so there is a T'-module M in B containing $T' + \sum B^2 c$ and maximal subject to $-1 \notin M$. By proposition 6.1.30, $\mathfrak{p} := M \cap -M$ is a prime ideal. Also, $T' \subseteq M$, so $(T' + \mathfrak{p}) \cap (-T' + \mathfrak{p}) = \mathfrak{p}$. It follows that the preordering $T'' := \{(a + \mathfrak{p})/(b + \mathfrak{p}) : a, b \in T',\ b \notin p\}$ is a proper preordering in the multifield $F := ff(A/\mathfrak{p})$. Since $d \notin \mathfrak{p}$ (d is invertible in B), it follows from our assumption that $c + \mathfrak{p} \in\notin P$ for all orderings P of F containing T''. According to proposition 6.1.23, this implies that $c + \mathfrak{p} \in -T''$. This yields elements $s, t \in T' + \mathfrak{p}$ with $s, t \notin \mathfrak{p}$ such that $-sc = t$. Then $st \in T' + \mathfrak{p} \subseteq M$ and $-st = s^2 c \in \sum B^2 c \subseteq M$, so $st \in M \cap -M = \mathfrak{p}$, a contradiction.

($\Leftarrow$) We already know that $\sigma(d^{2k}) \geq 0$ for all $\sigma \in X_T$. If $-d^{2k} \in T + \sum A^2 c$, then $-\sigma(d^{2k}) \geq 0$ for all $\sigma \in X_T$. Hence $\sigma(d^{2k}) = -\sigma(d^{2k}) = 0$ for all $\sigma \in X_T$, and this implies that $\sigma(d) = 0$ for all $\sigma \in X_T$. □

Corollary 6.1.33.

a - *$\overline{a} = 0$ on X_T if and only if $-a^{2k} \in T$ for some $k \geq 0$.*

b - *$\overline{a} = 1$ on X_T if and only if $-1 \in T - \sum A^2 a$.*

c - *$\overline{a} \geq 0$ on X_T if and only if $-a^{2k} \in T - \sum A^2 a$ for some $k \geq 0$.*

d - *Fix $a \in b^2 + c^2$. Then $\overline{b} = \overline{c}$ on X_T if and only if $-a^{2k} \in T - \sum A^2 bc$ for some $k \geq 0$.*

Proof. Apply proposition 6.1.32 as follows: (a) take $c = 0$, $d = a$. (b) Take $c = -a$, $d = 1$. (c) Take $c = -a$, $d = a$. (d) Take $c = -bc$, $d = a$. □

6.1.6 Real Ideals

We indicate briefly how the theory of real ideals and real prime ideals extends to multirings. An ideal $\mathfrak{a}$ in a multiring A is said to be *real* if $(\sum a_i^2) \cap \mathfrak{a} \neq \emptyset \Rightarrow a_i \in \mathfrak{a}$ for each i. Every real ideal is *radical* in the sense that $a^2 \in \mathfrak{a} \Rightarrow a \in \mathfrak{a}$, i.e, $\mathfrak{a}$ is the intersection of prime ideals of A. The converse is not true.

Proposition 6.1.34. *For a prime ideal $\mathfrak{p}$ in a multiring A, the following are equivalent:*

a - $\mathfrak{p}$ is real.

b - The residue multifield $ff(A/\mathfrak{p})$ is real.

c - $\mathfrak{p}$ is the support of some ordering of A.

Proof. (a)⇒(b) If $-1 + \mathfrak{p} \in \sum a_i^2 + \mathfrak{p}$, then $0 \in 1 + \sum a_i^2 + \mathfrak{p}$, and $(1 + \sum a_i^2) \cap \mathfrak{p} \neq \emptyset$. As $\mathfrak{p}$ is real, $1 \in \mathfrak{p}$, contradiction. Then $-1 \notin \sum (A/\mathfrak{p})^2$, and therefore $-1 \notin \sum ff(A/\mathfrak{p})^2$.

(b)⇒(c) By proposition 6.1.22, $ff(A/\mathfrak{p})$ has an ordering P. Let $\tilde{P} = \{a_i, b_i : a_i/b_i \in P\}$ and $Q = q^{-1}[\tilde{P}]$, where $q : A \to A/\mathfrak{p}$ is the canonical projection. Then Q is the desired ordering.

(c)⇒(a) Is just the fact that an ordering P contains $\sum A^2$. □

Definition 6.1.35. *The real radical of an ideal $\mathfrak{a}$ in A is*

$$\sqrt[R]{\mathfrak{a}} := \left\{ a \in A : \exists\, b_i \in A \text{ and } k \geq 0 \text{ such that } \left(a^{2k} + \sum b_i^2 \right) \cap \mathfrak{a} \neq \emptyset \right\}.$$

Proposition 6.1.36. *$\sqrt[R]{\mathfrak{a}}$ is the intersection of all real prime ideals of A containing $\mathfrak{a}$.*

Proof. The inclusion $\subseteq$ is immediate because $\sqrt[R]{\mathfrak{a}}$ is real. For $\supseteq$, we use corollary 6.1.33(a). Suppose that $a \in \mathfrak{p}$ for each real prime ideal $\mathfrak{p}$ with $\mathfrak{a} \subseteq \mathfrak{p}$. Consider $T = \sum A^2 + \mathfrak{a}$ (the preordering in A generated by a). Then $\overline{a} = 0$ on X_T so, by corollary 6.1.33(a), $-a^{2k} \in T$ for some $k \geq 0$. Then $\left(a^{2k} + \sum b_i^2\right) \cap \mathfrak{a} \neq \emptyset$ for some b_j, and $a \in \sqrt[R]{\mathfrak{a}}$. □

Proposition 6.1.37. *For an ideal $\mathfrak{a}$ of a multiring A, the following are equivalent:*

a - $\mathfrak{a}$ is real.

b - $\sqrt[R]{\mathfrak{a}} = a$.

c - $\mathfrak{a}$ is the intersection of real prime ideals.

d - $\mathfrak{a}$ is radical and every minimal prime ideal over $\mathfrak{a}$ is real.

Proof. We already have (a)⇔(b), and (b)⇔(c) is consequence of proposition 6.1.36. If $\mathfrak{a}$ is radical, then $\mathfrak{a}$ is the intersection of the minimal prime ideals over $\mathfrak{a}$, so (d)⇒(3). It remains to show that (c)⇒(d). Suppose $\mathfrak{q}$ is a minimal prime ideal over $\mathfrak{a}$ which is not real. Thus, for every real prime ideal $\mathfrak{p}$ of A which $\mathfrak{a} \subseteq \mathfrak{p}$, there exists $a_\mathfrak{p} \in \mathfrak{p}$ such that $a_\mathfrak{p} \notin \mathfrak{q}$. By the compactness of $\mathrm{Sper}(A)$ in the patch topology, there exist finitely many elements $a_1, ..., a_n$ of A such that $a_i \notin \mathfrak{q}$ for each i, and for each real prime ideal $\mathfrak{p}$ with $\mathfrak{a} \subseteq \mathfrak{p}$, $a_i \in \mathfrak{p}$ for some i. Let $a = a_1 \cdot ... \cdot a_n$. Then $a \in \mathfrak{p}$ for each real prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ so, by (c), $a \in \mathfrak{a}$. This contradicts $a \notin \mathfrak{q}$. □

Definition 6.1.38. *A multiring A (with $1 \neq 0$) is said to be real if the ideal $\{0\}$ is real.*

If $\mathfrak{a}$ is a real proper ideal of A, then $A/\mathfrak{a}$ is real. In particular, if $-1 \notin \sum A^2$, then $A/\sqrt[R]{\{0\}}$ is real.

6.1.7 Real Reduced Multirings

We assume that A is a multiring with $-1 \notin \sum A^2$ and T is a proper preordering of A. We use the notation of section 8.4, where we define the multiring homomorphism $A \to Q_2^{X_T}$, given by $a \mapsto \overline{a}$, where $\overline{a}$ is defined by $\overline{a}(\sigma) = \sigma(a)$ for all $\sigma \in X_T$. We want to prove that the image of A in $Q_2^{X_T}$ is a multiring which is strongly embedded in $Q_2^{X_T}$. Now, we will introduce some notation:

Definition 6.1.39. *For $a_1, ..., a_n \in A$, we define the value set of $\phi = (\overline{a}_1, ..., \overline{a}_n)$ to be*

$$D(\phi) = D(\overline{a}_1, ..., \overline{a}_n) = \left\{ \overline{b} : b \in \sum Ta_1 + ... + \sum Ta_n \right\}.$$

We say that $\overline{b}$ is represented by ϕ if $\overline{b} \in D(\phi)$.

Lemma 6.1.40.

i - $D(\overline{a}) = \{\overline{b}^2\overline{a} : b \in A\} = \{\overline{t}\overline{a} : t \in A, \overline{t} \geq 0\} =$
$\{\overline{b} : \text{for each } \sigma \in X_T \text{ either } \overline{b}(\sigma) = 0 \text{ or } \overline{a}(\sigma)\overline{b}(\sigma) > 0\}$.

ii - $D(\overline{a}, \overline{b}) = \{\overline{c} : \text{for each } \sigma \in X_T, \text{ either } \overline{c}(\sigma) = 0 \text{ or } \overline{a}(\sigma)\overline{c}(\sigma) > 0 \text{ or } \overline{b}(\sigma)\overline{c}(\sigma) > 0\}$.

iii - If $n \geq 3$, $D(\overline{a}_1, ..., \overline{a}_n) = \bigcup_{\overline{c} \in D(\overline{a}_2, ..., \overline{a}_n)} D(\overline{a}_1, \overline{c})$.

iv - $D(\overline{a}_1, ..., \overline{a}_n)$ *depends only on* $\overline{a}_1, ..., \overline{a}_n$ *(not on the particular representatives* $a_1, ..., a_n$*).*

Proof. i - Is immediate from definition of $D(\overline{a})$.

ii - If $c \in \sum Ta + \sum Tb$, then $c^2 \in \sum Tac + \sum Tbc$. Follow this, that for any $\sigma \in X_T$, either $\overline{c}(\sigma) = 0$ of one of $\overline{a}(\sigma)\overline{c}(\sigma), \overline{b}(\sigma)\overline{c}(\sigma)$ is strictly positive, so $\overline{c}$ belongs to the second set. Now pick c such that $\overline{c}$ belongs to the second set. Denote by A' the localization of A and the multiplicative set $S = \{c^{2k} | k \geq 0\}$ and let T' be the preordering in A' defined by $T' = \{t/2^{2k} : k \geq 0\}$. Let $a' = ac$, $b' = bc$. On $X_{T'-\sum T'a'}$, $\overline{b} > 0$, so by corollary 6.1.33(b), $-1 \in T' - \sum T'a' - \sum A'^2 b'$. Multiplying by c^{2m+1}, m sufficiently large, $-c^{2m+1} \in Tc - \sum Ta - \sum Tb$. This yields $c_1 \in (\sum Ta + \sum Tb) \cap (c^{2m+1} + Tc)$. It follows that $\overline{c} = \overline{c}_1 \in D(\overline{a}, \overline{b})$.

iii - This folloes from (ii) by induction. Note that $D(\overline{a}, \overline{c})$ depends only on $\overline{c}$, not on the particular representative of c.

iv - For $n = 1$ and 2, this is immediate from (i) and (ii). For $n \geq 3$, it follows by induction on n using (iii).

□

Lemma 6.1.41. *For $a_0, ..., a_n \in A$, the following are equivalent:*

i - *There exists $a_i' \in A$ such that $\overline{a'}_i = \overline{a}_i$ and $0 \in a_0' + ... + a_n'$.*

ii - $\overline{-a}_i \in D(\overline{a}_1, ..., \overline{a}_{i-1}, \overline{a}_{i+1}, ..., \overline{a}_n)$ *for* $i = 0, ..., n$.

Proof. (i)⇒(ii) By symmetry, it is suffice to show $-\overline{a}_0 \in D(\overline{a}_1, ..., \overline{a}_n)$. Since $0 \in a_0' + ... + a_n'$, $-a_0' \in a_1' + ... + a_n'$, so $\overline{a}_0 = \overline{a'}_0 \in D(\overline{a'}_1, ..., \overline{a'}_n) = D(\overline{a}_1, ..., \overline{a}_n)$, using lemma 6.1.40(iii).

(ii)⇒(i) We have a_i' with $\overline{a'}_i = \overline{a}_i$ such that $0 \in a_i' + \sum_{i \neq j} \sum Ta_j$. Then $0 \in 0 + ... + 0 \subseteq \sum_{i=0}^n (a_i' + \sum_{i \neq j} \sum Ta_j) = \sum_{i=0}^n (a_i' + \sum Ta_i)$, so there exist $a_i'' \in a_i' + \sum Ta_i$ such that $0 \in a_0'' + ... + a_n''$. Hence $\overline{a''}_i = \overline{a}_i$. □

Denote the image of A in $Q_2^{X_T}$ by $Q_T(A)$. Addition on $Q_T(A)$ is defined by $\overline{a}+\overline{b} := \{\overline{c} : c \in a+b\}$, $\overline{a}\overline{b} := \overline{ab}$, $-\overline{a} := \overline{-a}$. The zero element of $Q_T(A)$ is $\overline{0}$.

Proposition 6.1.42 (Local-Global principle)**.** *Let A be a multiring with $-1 \notin \sum A^2$ and T a proper preordering of A. Then:*

i - *$Q_T(A)$ is a multiring.*

ii - *$Q_T(A)$ is strong embedded in $Q_2^{X_T}$.*

Proof.

i - Everything is straightforward calculations except the associativity. Let $x, u, v, w, p \in A$ such that $\overline{p} \in \overline{u} + \overline{v}$ and $\overline{x} \in \overline{p} + \overline{w}$. Then $\overline{x} \in D(\overline{p}, \overline{w})$ and $\overline{p} \in D(\overline{u}, \overline{v})$, so $\overline{x} \in D(\overline{u}, \overline{v}, \overline{w})$. Also $-\overline{w} \in -\overline{x}+\overline{p}$, so $-\overline{w} \in D(-\overline{x}, \overline{p})$, i.e, $-\overline{w} \in D(-\overline{x}, \overline{u}, \overline{v})$. Also $-\overline{u} \in -\overline{p}+\overline{v}$ and $-\overline{p} \in -\overline{x}+\overline{w}$, so $-\overline{u} \in D(-\overline{p}, \overline{v})$ and $-\overline{p} \in D(-\overline{x}, \overline{w})$ i.e., $-\overline{u} \in D(-\overline{x}, \overline{v}, \overline{w})$. According to lemma 6.1.41, this implies there exist $x', u', v', w' \in A$ such that $\overline{x'} = \overline{x}$, $\overline{u'} = \overline{u}$, $\overline{v'} = \overline{v}$, $\overline{w'} = \overline{w}$ and $x' \in u' + v' + w'$. Pick $q \in v' + w'$ such that $x' \in u' + q$. Then $\overline{q} \in \overline{v} + \overline{w}$ and $\overline{x} \in \overline{u} + \overline{q}$.

ii - Let $a, b, c \in A$. According to lemma 6.1.41, $\overline{c} \in \overline{a} + \overline{b}$ iff $\overline{c} \in D(\overline{a}, \overline{b})$, $-\overline{a} \in D(-\overline{c}, \overline{b})$ and $-\overline{b} \in D(-\overline{c}, \overline{a})$. According to lemma 6.1.40(ii), this occurs iff for all $\sigma \in X_T$, $\overline{c}(\sigma)\overline{a}(\sigma) > 0$ or $\overline{c}(\sigma)\overline{b}(\sigma) > 0$ or $\overline{a}(\sigma)\overline{b}(\sigma) < 0$ or $\overline{a}(\sigma) = \overline{b}(\sigma) = \overline{c}(\sigma) = 0$, i.e., iff for all $\sigma \in X_T$, $\overline{c}(\sigma) \in \overline{a}(\sigma) + \overline{b}(\sigma)$.

□

The real spectrum of $Q_T(A)$ is naturally identified with X_T. Now that we know that addition is a well-defined associative operation on subsets of $Q_T(A)$, we have another more intrinsic description of value sets:

Corollary 6.1.43. *Let $\overline{T} = \{\overline{t} : t \in T\} = \{\overline{t} : t \in A, \overline{t} \geq 0\}$. Then:*

i - *$\overline{T}\overline{a}_1 + .. + \overline{T}\overline{a}_n = \{\overline{b} : b \in \sum Ta_1 + ... + \sum Ta_n\}$.*

ii - *$\overline{0} \in \overline{a}_1 + ... + \overline{a}_n \Leftrightarrow -\overline{a}_i \in \sum_{j \neq i} \overline{T}\overline{a}_j$, for $i = 0, ..., n \Leftrightarrow$ there exists $a'_0, ..., a'_n$ such that $0 \in a'_1 + ...a'_n$ and $\overline{a}'_i = \overline{a}_i$, $i = 0, ..., n$.*

Proof. (i) is direct consequence of lemma 6.1.40 and (ii) is direct consequence of 6.1.41. □

We restrict our attention now to the case where $T = \sum A^2$ and consider the multiring morphism $a \mapsto \overline{a}$ from A into $Q_2^{\mathrm{Sper}(A)}$. We denote $Q_{\sum A^2}(A)$ by $Q_{red}(A)$ which we refer to as the *real reduced multiring* associated to A. The multirings A such that the morphism $A \to Q_{red}(A)$ is an isomorphism are obviously of special interest.

Proposition 6.1.44. *For a multiring A with $-1 \notin \sum A^2$, the map $a \mapsto \overline{a}$ from A onto $Q_{red}(A)$ is an isomorphism if and only if A satisfies the following properties:*

a - $a^3 = a$.

b - $a + ab^2 = \{a\}$.

c - $a^2 + b^2$ *contains a unique element.*

Proof. ($\Rightarrow$) By construction we have (a) and (b) (since $\overline{a} + \overline{a} = \overline{a}$ and $\overline{b}^2 = \overline{1}$ or $\overline{b}^2 = 0$ in $Q_{red}(A)$). For (c), if $c \in a^2 + b^2$, then $c^2 \in (a^2 + b^2)(a^2 + b^2) \subseteq a^4 + a^2b^2 + a^2b^2 + b^4 = (a^2 + a^2b^2) + (b^2 + a^2b^2)$. Since $a^2 + a^2b^2 = \{a^2\}$ and $b^2 + a^2b^2 = \{b^2\}$, this implies $c^2 \in a^2 + b^2$. Consequently, $c^2 = c$, i.e., the unique element of $a^2 + b^2$ is necessarily a square. It follows by induction that, for any $a_1, ..., a_n \in A$, $a_1^2 + ... + a_n^2$ contains a unique element, which is a square. In particular, $\sum A^2 = A^2$.

($\Leftarrow$) Let $T = \sum A^2 = A^2$. suppose that $\overline{a} = \overline{b}$. Let $c \in a^2 + b^2$. Thus $-c^{2k} \in A^2 - \sum A^2ab$. Since $c^3 = c$, $c^{2k} = c^2$. Thus, there exists $d \in \sum A^2ab$ with $d \in c^2 + A^2$. $ac \in a(a^2 + b^2) \subseteq a^3 + ab^2 = a + ab^2 = a$, so $ac = a$. Similarly, $bc = b$ and $cd = c$. Thus, $ad = (ac)d = a(cd) = ac = a$ and, similarly, $bd = b$. Say $d \in \sum e_i^2 ab$. Then $ab = abd \in \sum e_i^2 a^2b^2 \subseteq A^2$. This implies $ab \in A^2$, so $ab = a^2b^2$. Thus, $a^2 = a^2d \in \sum e_i^2 a^3 b = \sum e_i^2 ab = \sum e_i^2 a^2b^2$ and, similarly, $b^2 \in \sum e_i^2 a^2b^2$. Since $\sum e_i^2 a^2b^2$ is a singleton set, this implies $a^2 = ab = b^2$. Finally,

$$a = a^3 = aa^2 + ab^2 = a(ab) + ab^2 = a^2b + ab^2 = (ab)b + ab^2 = (ab)b = b^2b = b^3 = b,$$

as required. □

Definition 6.1.45. *A multiring satisfying* $-1 \notin \sum A^2$ *and the equivalent conditions of proposition 6.1.44 will be called real reduced multiring. A morphism of real reduced multirings is just a morphism of multirings. The category of real reduced multirings will be denoted by* $\mathcal{MR}_{red}$.

Corollary 6.1.46. *A multiring A is real reduced if and only if the following properties holds for all* $a, b, c, d \in F$*:*

i - $1 \neq 0$;

ii - $a^3 = a$;

iii - $c \in a + ab^2 \Rightarrow c = a$;

iv - $c \in a^2 + b^2$ *and* $d \in a^2 + b^2$ *implies* $c = d$.

Proof. As noted above, (ii),(iii) and (iv) imply $\sum A^2 = A^2$. If $-1 \in \sum A^2$, then $-1 = a^2$ for some a, so $0 \in 1 + a^2$. By (iii), $0 = 1$ and this contradicts (i). Thus $-1 \notin \sum A^2$. Now apply proposition 6.1.44 to conclude that A is a real reduced multiring. The converse is immediate. □

6.2 Opening the Chamber of The Secrets: The Final Functorial Picture

In the very end of the work the Chamber of The Secrets is opening: here we connect the new theory of multirings and multifields with the most significant theories of quadratic forms. This is (in some way) a new picture: despites of the Marshall's and Miraglia's observation about these connections, it is the first time that this is made explicit. So, because this, the implications of the multirings and multifieds theory in the abstract theory of quadratic forms are a road to discover.

6.2.1 Multirings, Abstract Ordering Spaces and Special Groups

Theorem 6.2.1. *Let* (X, G) *a space of orderings and set* $M(G) = G \cup \{0\}$ *where* $0 := \{G\}$. *Then* $(M(G), +, \cdot, -, 0, 1)$ *is a real reduced multifield with the extended operations:*

- $a \cdot b = \begin{cases} 0 \text{ if } a = 0 \text{ or } b = 0 \\ a \cdot b \text{ otherwise} \end{cases}$
- $-(a) = (-1) \cdot a$
- $a + b = \begin{cases} \{b\} \text{ if } a = 0 \\ \{a\} \text{ if } b = 0 \\ M(G) \text{ if } a = -b, \text{ and } a \neq 0 \\ D(a,b) \text{ otherwise} \end{cases}$

Proof. Firstly, observe that $+$ is well-defined. Then, we will verify the conditions of definition 6.1.5:

i - For this, we will check the conditions of definition 6.1.1.

a - If $a = 0$ or $a = -b$, then $d \in a+b$ implies trivially that $a \in d+(-b)$ and $b \in (-a)+d$. Now, let $a, b \neq 0$ with $a \neq -b$ (this implies $d \neq 0$). We prove that $(d(x) \in \{a(x), b(x)\} \forall\, x \in X) \Rightarrow (a(x) \in \{d(x), -b(x)\} \forall\, x \in X)$, and it is suffice for prove that $a \in d + (-b)$ and $b \in (-a) + d$. Let $x \in X$. If $c(x) = a(x)$ is done. If $c(x) \neq a(x)$ then $c(x) = b(x)$. If $c(x) = b(x) = 1$, then $a(x) = -1 = -b(x)$, and if $c(x) = b(x) = -1$, then $a(x) = 1 = -b(x)$, finalizing the argument.

b - $(y \in x + 0) \Leftrightarrow (x = y)$ is direct consequence of the definition of sum.

c - $a + 0 = 0 + a$ and $a + (-a) = M(G) = (-a) + a$. Let $a, b \in M(G)$, $a, b \neq 0$ and $a \neq -b$. How $D(a, b) = D(b, a)$, we have $a + b = b + a$. Then, the commutativity holds.

d - Now we prove the associativity. Let $a = 0$ (the cases $b = 0$ and $c = 0$ are analogous). Then $0 + (b + c) = \{0 + g : g \in b + c\} = b + c$ and $(0 + b) + c = (\{b\}) + c = b + c$.
Now, let $a, b, c \neq 0$ with $a = -c$.

$$(a + b) + (-a) = \bigcup \{g + (-a) : g \in a + b\} = M(G) \text{ (I)}$$

because $a \in a + b$; and

$$a + (b + (-a)) = \bigcup \{a + h : h \in b + (-a)\} = M(G) \text{ (II)}$$

because $-a \in b + (-a)$. So (I) = (II) and $(a + b) + (-a) = a + (b + (-a))$. For the case $a, b, c \neq 0$, $a = -b$ (the cases $b \neq -c$ is analogous) we have

$$(a + (-a)) + c = \bigcup \{g + c : g \in M(G)\} = M(G) \text{ (III)}$$

and

$$a + ((-a) + c) = \bigcup \{a + h : h \in (-a) + c\} = M(G) \text{ (IV)}$$

because $-a \in (-a) + c$. So (III) = (IV) and $(a + (-a)) + c = a + ((-a) + c)$. Finally, let $a, b, c \neq 0$, $a \neq -b$, $b \neq -c$ and $a \neq -c$.

$$(a + b) + c = c + (a + b) = \bigcup \{c + g : g \in a + b\} = \bigcup_{g \in D(a,b)} D(c, g) \text{ (V)}$$

and

$$a+(b+c)=\bigcup\{h+a : h\in b+c\}=\bigcup_{h\in D(b,c)} D(h,a)\,(\text{VI})$$

By the inductive description of the value sets (as in 2.2 of [Mar96]) we have (V) = (VI). Then $(a+b)+c=a+(b+c)$ for all $a,b,c\in M(G)$.

ii - We conclude that $(M(G),\cdot,1)$ is a commutative monoid as consequence of $(G,\cdot,1)$ is an abelian group and the extended definition of $\cdot$ to $M(G)$. Beyond this, we have that every nonzero element of $M(G)$ has an inverse.

iii - $a\cdot 0=0$ for all $a\in M(G)$ is a consequence of the extended definition of multiplication to $M(G)$.

iv - If $a=0$ or $a\neq -b$, then $(d\in a+b)\Rightarrow\forall g(gd\in ga+gb)$ is direct consequence of the definition of sum. Next this, let $a,b\neq 0$ with $a\neq -b$ and $d\in a+b=D(a,b)$. Then $d(x)=a(x)$ or $d(x)=b(x)$ for all $x\in X$. Hence, $g(x)d(x)=g(x)a(x)$ or $g(x)d(x)=g(x)b(x)$ for all $x\in X$ and $gd\in ga+bg$. Thus we have $g(a+b)\subseteq ga+gb$ for all $a,b,g\in M(G)$.

Then, $(M(G),+,-,\cdot,0,1)$ is a multifield. As G is a subgroup of $\{-1,1\}^X$, we have that G is a group of exponent 2, i.e, $g^2=1$ for all $g\in G$ and then, $a^3=a$ for all $a\in M(G)$. If $a\in 1+1$, then $a(x)=x$ for all $x\in X$. This implies $a=1$. Consequently, $M(G),+,-,\cdot,0,1)$ is a real reduced multifield. □

Corollary 6.2.2. *The correspondence $G\mapsto M(G)$ defines a contravariant functor $M:\mathcal{AOS}^{op}\to\mathcal{MF}_{red}$.*

Proof. Let (X,G) and (Y,H) abstract ordering spaces and $\alpha:Y\to X$ be an AOS-morphism. By definition 4.1.9, α induces a group homomorphism $\varphi:G\to H$ given by $\varphi(g)=g\circ\alpha$. Define $M(\alpha)=\tilde{\varphi}:M(G)\to M(H)$ extending this morphism φ to $M(G)$ making $\tilde{\varphi}(0)=0$. Note that we alread have $\varphi(1)=1$ and $\varphi(-1)=-1$.

Then, we just need to prove that for all $a,b,c\in G$, $c\in a+b\Rightarrow\tilde{\varphi}\in\tilde{\varphi}+\tilde{\varphi}$. We can suppose $a,b,c\neq 0$ and $a\neq -b$ without loss of generality. Hence, we will prove that $c\in D(a,b)\Rightarrow\varphi(c)\in D(\varphi(a),\varphi(b))$.

$$\begin{aligned} c\in D(a,b)\Rightarrow c(x)=a(x)\vee c(x)=b(x)\,\forall\, x\in X\Rightarrow\\ c(\alpha(y))=a(\alpha(y))\vee c(\alpha(y))=b(\alpha(y))\,\forall\, y\in Y\Rightarrow\\ c\circ\alpha\in D(a\circ\alpha,b\circ\alpha)\Rightarrow D(\varphi(a),\varphi(b))\end{aligned}$$

therefore $M(\varphi)$ is a MF-morphism. If $(Z,K)\xrightarrow{\beta}(Y,H)\xrightarrow{\alpha}(X,G)$ are AOS-morphism, with $\varphi:G\to H$ and $\tau:H\to K$ the respectively induced group homomorphisms, the fact of $M(\alpha\beta)=M(\beta)M(\alpha)$ is direct consequence of $\alpha\beta$ be an AOS-morphism. □

Let F be an real reduced multifield. Observe that by the local-global principle for multifield 6.1.28 we have the following identities:

- $a\in a+b$;
- If $a\neq 0$, then $a+(-a)=F$;
- $a\neq 0\Rightarrow\sigma(a)\neq 0$ for all $\sigma\in\mathrm{Sper}(F)$.

Now, let $\chi(F) = \{\sigma \in \{-1,1\}^F : \sigma(ab) = \sigma(a)\sigma(b)\}$ and define

$$\begin{cases} X = \{x \in \chi(F) : x(-1) = -1 \text{ and } a, b \in Ker(x) \Rightarrow a + b \subseteq Ker(x)\} \\ G = \{\sigma \in \{-1,1\}^X : \exists\, f \in F \text{ such that } \sigma(x) = x(f),\ \forall\, x \in X\} \end{cases}$$

Lemma 6.2.3. *There are bijective correspondences $X \to Sper(F)$ and $G \to F$.*

Proof. We will proof that the correspondence $x \mapsto x' : F \to Q_2$, $x'(f) = x(f)$ if $f \neq 0$ and $x'(0) =)$ define a bijection $A : X \to \mathrm{Sper}(F)$ and the correspondence $\sigma \mapsto f_\sigma$ when $\sigma(x) = x(f_\sigma)$ for all $x \in X$ define a bijection $B : G \to F$.

- A and B are well-defined. We need to prove that $x' : F \to Q_2$ is a multifield morphism and that $\bigcap_{x\in X} \mathrm{Ker}(x) = \{1\}$, hence by this, $x(f) = x(g)$ for all $x \in X$ implies that $fg^{-1} \in \bigcap \mathrm{Ker}(x) = \{1\}$ and then, $f = g$.

  i - x' is a morphism. In fact, we just need to prove that $a \in b + c \Rightarrow x(a) \in x(b) + x(c)$. How the zero case is undefined, let $a, b, c \neq 0$. If $x(b) \neq x(c)$, then $x(b) + x(c) = Q_2$ and it is done. If $x(b) = x(c) = 1$, $a \in (b + c)^* \subseteq \mathrm{Ker}(x) \Rightarrow x(a) \in x(b) + x(c)$. If $x(b) = x(c) = -1$, then $-a \in (-b - c)^* \subseteq \mathrm{Ker}(x) \Rightarrow x(a) \in x(b) + x(c)$.

  ii - $\bigcap_{x\in X} \mathrm{Ker}(x) = \{1\}$. Let $a \neq 1$ in F^*. How F is a real reduced multifield,

  $$a \notin \{0, 1\} = \sum F^2 = \bigcap_{P \in \mathrm{Sper}(F)} P.$$

  Let P an ordering such that $a \notin P$ and $\sigma : F \to Q_2$ its associate morphism. Note that $\sigma(a) = -1$ and $\sigma|_{F^*} \in X$, because

  $$a, b \in \mathrm{Ker}(\sigma) \Rightarrow \sigma(a + b) \subseteq \sigma(a) + \sigma(b) = \{1\} \Rightarrow (a + b)^* \subseteq \mathrm{Ker}(\sigma|_{F^*})$$

  Therefore $a \notin \bigcap_{x\in X} \mathrm{Ker}(x)$.

- A and B are injective.

  $$x \neq y \in X \Rightarrow \exists\, f \in F^* \text{ such that } x(f) \neq y(f) \Rightarrow x'(f) = x(f) \neq y(f) = y'(f).$$

  $$\sigma \neq \gamma \in G \Rightarrow \exists\, x \in X \text{ such that } \sigma(x) \neq \gamma(x) \Rightarrow x(f_\sigma) \neq x(f_\gamma) \Rightarrow f_\sigma \neq f_\gamma.$$

- A and B are surjective. Given $\sigma \in \mathrm{Sper}(F)$, we already proof that $\sigma|_{F^*} \in X$ and so $A(\sigma|_{F^*}) = \sigma$. For B, let $f \in F^*$, define $\sigma_f \in \{-1,1\}^X$ given by $\sigma_f(x) = x(f)$ for all $x \in X$. Then $\sigma_f \in G$ and $B(\sigma_f) = f$.

□

Theorem 6.2.4. *With the above notation, (X, G) is an abstract ordering space.*

Proof. Notation: if $\sigma \in G$, $f_\sigma = B(\sigma)$ and if $f \in F^*$, $\sigma_f = B^{-1}(f)$. Given $\sigma, \gamma \in G$, define

$D(\sigma,\gamma) = \{\tau \in G : \forall\, x \in X,\, \tau(x) \in \{\sigma(x), \gamma(x)\}\}$. We have $D(\sigma,\gamma) = \{\tau : f_\tau \in (f_\sigma + f_\gamma)^*\}$.

$$\begin{aligned} \tau \in D(\sigma,\gamma) &\Leftrightarrow \tau(x) = \sigma(x) \vee \tau(x) = \gamma(x) \Leftrightarrow \\ &\forall\, x \in X, \tau(x) \in \sigma(x) + \gamma(x) \\ &\overset{\text{lemma 6.2.3}}{\Leftrightarrow} K \in \mathrm{Sper}(F), K(f_\tau) \in K(f_\sigma) + (f_\gamma) \\ &\overset{\text{local-global principle 6.1.28}}{\Leftrightarrow} f_\tau \in (f_\sigma + f_\gamma). \end{aligned}$$

Now, we will check each axiom of definition 4.1.6:

AX1 - $G \subseteq \{-1,1\}^X$ is a subgroup, because $\sigma_f\sigma_g = \sigma_{fg}$, $1 \in G$ and $(\sigma_f)^{-1} = \sigma_{f^{-1}}$. Moreover, $-1 = \sigma_{-1} \in G$, because $x(-1) = -1$ for all $x \in X$. We alread have that G separate points.

AX2 - Let $\Pi \in \chi(G)$ with $\Pi(\sigma_{-1}) = -1$ and $\sigma, \gamma \in Ker(\Pi) \Rightarrow D(\sigma,\gamma) \subseteq Ker(\Pi)$. We need to find $x \in X$ such that $\Pi(\sigma) = \sigma(x)$ for all $\sigma \in G$.

Define $x : F^* \to \{-1,1\}$ by $x(f) = \Pi(\sigma_f)$. Note that $x \in \chi(F)$ and $x(-1) = -1$. To proof that $x \in X$ we need that $a, b \in Ker(x) \Rightarrow (a+b)^* \subseteq Ker(x)$.

$$a, b \in Ker(x) \Rightarrow \sigma_a, \sigma_b \in Ker(\Pi) \Rightarrow D(\sigma_a, \sigma_b) \subseteq Ker(\Pi)$$

Then

$$c \in (a+b)^* \Rightarrow \sigma_c \in D(\sigma_a, \sigma_b) \subseteq Ker(\Pi) \Rightarrow c \in Ker(x)$$

Therefore, $x \in X$. Moreover, given $\sigma = \sigma_f \in G$, we have

$$\Pi(\sigma) = \Pi(\sigma_f) = x(f) = \sigma_f(x) = \sigma(x)$$

finalizing the argument for AX2.

AX3 - Given $\sigma, \gamma, \tau \in G$, let $i \in D(\sigma, j)$ with $j \in D(\gamma, \tau)$. We will show that $i \in D(\sigma, j)$, $j \in D(\gamma,\tau) \Rightarrow f_i \in (f_\sigma + f_\tau)^*$ and $f_j \in (_\gamma + f_\tau)^*$. How the sum in F is associative, there exist $l \in f_\sigma + f_\gamma$ with $f_i \in f_l + f_\gamma$.

If $l = 0$, we have $f_\sigma = -f_\gamma$ and $f_i - f_\gamma$ and then, $f_i \in (1 + f_\gamma)^*$ and $1 \in (f_\sigma + f_\gamma)^* \Rightarrow i \in D(\sigma_1, \gamma)$ and $\sigma_1 \in D(\sigma,\gamma)$. If $l \neq 0$, $i \in D(\sigma_l, \gamma)$ with $\sigma_l \in D(\sigma,\gamma)$.

□

Theorem 6.2.5. *There is an equivalence of categories between $\mathcal{AOS}^{op}$ and $\mathcal{MF}_{red}$.*

Proof. Define $M : \mathcal{AOS}^{op} \to \mathcal{MF}_{Red}$ and $\mathrm{Spec} : \mathcal{MF}_{Red} \to \mathcal{AOS}^{op}$ as we already defined in corollary 6.2.2 and theorem 6.2.4. Follow that $M \circ \mathrm{Spec} \cong Id_{\mathcal{MF}_{Red}}$ and $\mathrm{Spec} \circ M \cong Id_{\mathcal{AOS}^{op}}$. □

Proposition 6.2.6. *Let $(G, \equiv, -1)$ be a special group and define $M(G) = G \cup \{0\}$ where $0 := \{G\}$[2]. Then $(M(G), +, -, \cdot, 0, 1)$ is a multifield, where*

- $a \cdot b = \begin{cases} 0 \text{ if } a = 0 \text{ or } b = 0 \\ a \cdot b \text{ otherwise} \end{cases}$
- $-(a) = (-1) \cdot a$

[2]Here, the choice of the zero element was ad hoc. Indeed, we can define $0 := \{x\}$ for any $x \notin G$.

- $a+b=\begin{cases}\{b\}\ \textit{if}\ a=0\\ \{a\}\ \textit{if}\ b=0\\ M(G)\ \textit{if}\ a=-b,\ \textit{and}\ a\neq 0\\ D_G(a,b)\ \textit{otherwise}\end{cases}$

Proof. Firstly, observe that $+$ is well-defined. Then, we will verify the conditions of definition 6.1.5:

i - For this, we will check the conditions of definition 6.1.1.

a - $d\in a+0=\{a\}$ imply $d=a$, and by this, follow that $a\in d+(-0)$ and $0\in(-a)+d$. Let $a=-b$ and $d\in a+(-a)=M(G)$. If $d=0$, then $a\in d+(-(-a))=0+a$ and $-a\in(-a)+0$. If $d\neq 0$, then $a\in D_G(d,a)$ and $-a\in D_G(-a,d)$ so $a\in d+(-(-a))=d+a$ and $-a\in(-a)+d$. Finally, let $a,b\neq 0$ with $a\neq -b$, and $d\in a+b$. Then there exist $g\in M(G)\setminus\{0\}$ such that $\langle d,g\rangle\equiv\langle a,b\rangle$. By SG4, $\langle d,-a\rangle\equiv\langle -g,b\rangle$ (and $\langle b,-g\rangle\equiv\langle -a,d\rangle$ by SG1). So $a\in d+(-b)$ and $b\in(-a)+d$.

b - $(y\in x+0)\Leftrightarrow(x=y)$ is direct consequence of the definition of sum.

c - $a+0=0+a$ and $a+(-a)=M(G)=(-a)+a$. Let $a,b\in M(G)$, $a,b\neq 0$ and $a\neq -b$. How $D_G(a,b)=D_G(b,a)$, we have $a+b=b+a$. Then, the commutativity holds. Observe that if $a,b\neq 0$ with $a\neq -b$, then $0\notin a+b$.

d - Now we prove the associativity. Let $a=0$ (the cases $b=0$ and $c=0$ are analogous). Then $0+(b+c)=\{0+g:g\in b+c\}=b+c$ and $(0+b)+c=(\{b\})+c=b+c$.
Now, let $a,b,c\neq 0$ with $a=-c$.

$$(a+b)+(-a)=\bigcup\{g+(-a):g\in a+b\}=M(G)\,(\text{I})$$

because $a\in a+b$, and

$$a+(b+(-a))=\bigcup\{a+h:h\in b+(-a)\}=M(G)\,(\text{II})$$

because $-a\in b+(-a)$. So (I) = (II) and $(a+b)+(-a)=a+(b+(-a))$. For the case $a,b,c\neq 0$, $a=-b$ (the cases $b\neq -c$ is analogous) we have

$$(a+(-a))+c=\bigcup\{g+c:g\in M(G)\}=M(G)\,(\text{III})$$

and

$$a+((-a)+c)=\bigcup\{a+h:h\in(-a)+c\}=M(G)\,(\text{IV})$$

because $-a\in(-a)+c$. So (III) = (IV) and $(a+(-a))+c=a+((-a)+c)$. Finally, let $a,b,c\neq 0$, $a\neq -b$, $b\neq -c$ and $a\neq -c$.

$$(a+b)+c=c+(a+b)=\bigcup\{c+g:g\in a+b\}=\bigcup_{g\in D_G(a,b)}D_G(c,g)\,(\text{V})$$

and

$$a+(b+c)=\bigcup\{h+a:h\in b+c\}=\bigcup_{h\in D_G(b,c)}D_G(h,a)\,(\text{VI})$$

By SG7 (applying SG5) we have (V) = (VI). Then $(a+b)+c=a+(b+c)$ for all $a,b,c\in M(G)$.

ii - We conclude that $(M(G), \cdot, 1)$ is a commutative monoid as consequence of $(G, \cdot, 1)$ is an abelian group and the extended definition of $\cdot$ to $M(G)$. Beyond this, we have that every nonzero element of $M(G)$ has an inverse.

iii - $a \cdot 0 = 0$ for all $a \in M(G)$ is a consequence of the extended definition of multiplication to $M(G)$.

iv - If $a = 0$ or $a \neq -b$, then $(d \in a+b) \Rightarrow \forall g(gd \in ga + gb)$ is direct consequence of the definition of sum. Next this, let $a, b \neq 0$ with $a \neq -b$ and $d \in a + b$. By SG5 $gd \in ga + bg$. Thus we have $g(a + b) \subseteq ga + gb$ for all $a, b, g \in M(G)$.

Then, $(M(G), +, -, \cdot, 0, 1)$ is a multifield. □

Corollary 6.2.7. *The correspondence $G \mapsto M(G)$ defines a full and faithful functor $M : \mathcal{SG} \to \mathcal{MF}$.*

Proof. Let $f : G \to H$ be a SG-morphism. We will extend f to $M(f) : M(G) \to M(H)$ by $M(f) \restriction_G = f$ and $M(f)(0) = 0$. By the definition of SG-morphism we have $M(f)(1) = 1$, $M(f)(-a) = -a$ and $M(f)(ab) = M(f)(a)M(f)(b)$. As $d \in D_G(a, b)$ implies $f(d) \in D_H(f(a), f(b))$ we have $d \in a + b \Rightarrow M(f)(d) \in M(f)(a) + M(f)(b)$ for all $a, b \in M(G)$. So $M(f)$ is a multiring morphism. Now, let $G \xrightarrow{f} H \xrightarrow{g} K$ be SG-morphisms. How $M(f \circ g) \restriction_G = f \circ g = M(f) \restriction_G \circ M(g) \restriction_G$ and $M(f \circ g)(0) = 0 = M(f) \circ M(g)(0)$, we have $M(f \circ g) = M(f) \circ M(g)$. Then $M : \mathcal{SG} \to \mathcal{MF}$ is a functor.

This functor is faithful, because if G and H are special groups and $f, g : G \to H$ are SG-morphisms such that $M(f), M(g) : M(G) \to M(H)$ are equal, then

$$M(f)|_{M(G)\setminus\{0\}} = M(g)|_{M(G)\setminus\{0\}}$$

and therefore $f = g$, since $M(G) \setminus \{0\} = G$. □

Proposition 6.2.8. *Let G be an SG and $M(G)$ as above. Then:*

i - $a^2 = 1$ *for all* $a \in M(G)^\bullet$;

ii - $1 \in 1 + a$ *for all* $a \in M(G)$;

iii - $1 + a$ *is closed by multiplication for all* $a \in M(G)$;

iv - *If there exists* $x, y, z \in \dot{M}(G)$ *such that*

$$\begin{cases} ax = cy \\ a = xz \\ d = yz \end{cases} \quad \text{and} \quad \begin{cases} a \in c + y \\ b \in x + z \\ c \in y + z \end{cases}$$

then there exists $t, v, w \in \dot{M}(G)$ *such that*

$$\begin{cases} bt = cv \\ b = tw \\ c = vw \end{cases} \quad \text{and} \quad \begin{cases} b \in c + v \\ a \in t + w \\ d \in v + w \end{cases}$$

Proof.

i - Is just the fact of G be a group of exponent 2.

ii - Trivial.

iii - If $a = 0$ or $a = -1$ it is trivial. If $a \neq 0, -1$, given $x, y \in 1 + a = D_G(1, a)$, we have $\langle x, xa\rangle \equiv \langle 1, a\rangle$ and $\langle y, ya\rangle \equiv \langle 1, a\rangle$. Multiplying the first equality by one, we have $\langle xy, xya\rangle \equiv \langle y, ya\rangle \equiv \langle 1, a\rangle$ and then $xy \in D_G(1, a) = 1 + a \equiv_G$.

iv - Is the 3-transitivity.

□

Definition 6.2.9. *A multifield F satisfying the properties i-iv of proposition 6.2.8 will be called a special multifield (SMF). Note that, if G is a SG, then $M(G)$ is a SMF.*

Theorem 6.2.10. *If F is a special multifield the $(F^\bullet, \equiv, -1)$ is a special group where $\langle a, b\rangle \equiv \langle c, d\rangle \Leftrightarrow ab = cd$ and $a \in c + d$.*

Proof. By (i), we have that $(F^\bullet, 1)$ is a group of exponent 2. Now, we will check each axiom of definition 4.2.1:

SG0 - By (ii) $1 \in 1 + ab$, so $ab \in 1 + ab$ and $a \in b + a$. As $ab = ab$, then $\langle a, b\rangle \equiv \langle a, b\rangle$, i.e, $\equiv$ is reflexive. If $\langle a, b\rangle \equiv \langle c, d\rangle$, then $ab = cd$ and $a \in c + d$. Then $ab \in cb + db$, so by $ab = cd$, we have $cd \in ad + db$ and then $c \in a + b$. So $\langle c, d\rangle \equiv \langle a, b\rangle$ and $\equiv$ is symmetric. Finally, suppose that $\langle a, b\rangle \equiv \langle c, d\rangle$ and $\langle c, d\rangle \equiv \langle e, f\rangle$. First, $ab = cd$ and $cd = ef$ implies $ab = ef$. Second, in order to show that $a \in e + f$, note that $a \in c + d \Rightarrow ac \in 1 + cd = 1 + ef$ and $c \in e + f \Rightarrow ce \in 1 + ef$; then by (iii), we have $ae \in 1 + ef$ and so $a \in e + f$. Therefore $\langle a, b\rangle \equiv \langle e, f\rangle$.

SG1 - As F is a multifield, $ab = ba$. By (ii), $1 \in 1 + ab$, then $ab \in 1 + ba$ and $b \in a + b$. Therefore $\langle a, b\rangle \equiv \langle b, a\rangle$.

SG2 - Since $1 \in 1 - a$, we have $a \in 1 - 1$. Therefore $\langle a, -a\rangle \equiv \langle 1, -1\rangle$.

SG3 - Follow by definition.

SG4 - $\langle a, b\rangle \equiv \langle c, d\rangle \Rightarrow ab = cd$ and $a \in c + d$.

$$ab = cd \Rightarrow -abbc = -bccd \Rightarrow -ac = -bd \tag{6.1}$$

$$a \in c + d \Rightarrow ad \in 1 + cd = 1 + ab \Rightarrow d \in a + b \Rightarrow a \in -b + d \tag{6.2}$$

so by 6.1 and 6.2 follow that $\langle a, -c\rangle \equiv \langle -b, d\rangle$.

SG5 - $\langle a, b\rangle \equiv \langle c, d\rangle \Rightarrow ab = cd$ and $a \in c + d \overset{I}{\Rightarrow} (ga)(gb) = (gc)(gd)$ and $ga \in gc + gd \Rightarrow \langle ga, gb\rangle \equiv \langle gc, gd\rangle$.

SG6 - We use the equivalences in theorem 4.2.17. $\langle a, b, ab\rangle \equiv \langle c, d, cd\rangle \Rightarrow$ there exists $x, y, t \in F^\bullet$ such that

$$\begin{cases} \langle a, x\rangle \equiv \langle c, y\rangle \\ \langle b, ab\rangle \equiv \langle x, z\rangle \\ \langle d, cd\rangle \equiv \langle y, z\rangle \end{cases} \Rightarrow \begin{cases} ax = cy \text{ and } a \in c + y \\ a = xz \text{ and } b \in x + z \\ c = yz \text{ and } d \in y + z \end{cases}$$

then by (v) there exists $t, v, w \in F^\bullet$ such that

$$\begin{cases} bt = cv \text{ and } b \in c + v \\ b = tw \text{ and } a \in t + w \\ d = vw \text{ and } d \in v + w \end{cases} \Rightarrow \begin{cases} \langle b, t\rangle \equiv \langle c, v\rangle \\ \langle a, ab\rangle \equiv \langle t, w\rangle \\ \langle d, cd\rangle \equiv \langle v, w\rangle \end{cases}$$

this implies $\langle b, a, ab\rangle \equiv \langle c, d, cd\rangle$.

□

Corollary 6.2.11. *There is a functor $S : \mathcal{SMF} \to \mathcal{SG}$.*

Proof. In the objects of $\mathcal{SMF}$, we define $S(F) = F^\bullet$ how the special group as stated in theorem 6.2.10. Now, let $\sigma : F \to K$ be a SMF-morphism. Define $S(\sigma) = \sigma|_{F^\bullet}$. We have that $S(\sigma)$ is a group homomorphism with $S(\sigma)(-1) = -1$. If $a, b \neq 0$ and $c \in a + b$, $c \neq 0$, then there exists $d \in F^\bullet$ such that $\langle a, b\rangle \equiv_{S(F)} \langle c, d\rangle$, and as $c \in a + b \to \sigma(c) \in \sigma(a) + \sigma(b)$, we have $\langle \sigma(a), \sigma(b)\rangle \equiv_{S(K)} \langle \sigma(c), \sigma(d)\rangle$. Therefore:

$$(c \in a + b \to \sigma(c) \in \sigma(a) + \sigma(b)) \Rightarrow (c \in D_{S(F)}(a, b) \to \sigma(c) \in D_{S(K)}(\sigma(a), \sigma(b)))$$

And $S(\sigma)$ is a SG-morphism. Applying the same argument, we proof that $S(\sigma\tau) = S(\sigma)S(\tau)$. Hence, S is a morphism. □

Theorem 6.2.12. *There exist an equivalence of categories between $\mathcal{SG}$ and $\mathcal{SMF}$.*

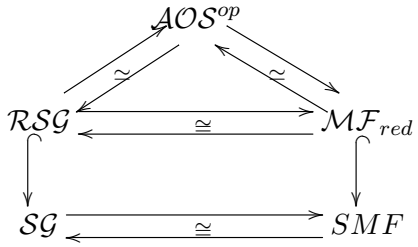
Proof. By the corollaries 6.2.7 and 6.2.11, we have functors $M : \mathcal{SG} \to \mathcal{SMF}$ and $S : \mathcal{SMF} \to \mathcal{SG}$. We will proof that $M \circ S \cong Id_{\mathcal{SMF}}$ and $S \circ M \cong Id_{\mathcal{SG}}$.

i - $M \circ S \cong Id_{\mathcal{SMF}}$. Let F be a SMF. How $S(F) = F^\bullet$ and $M(S(F)) = S(F) \cup \{0\}$, we have $M(S(F)) = F$. Next, let $\sigma : F \to K$ be a SMF-morphism. We have that $S(\sigma) = \sigma|_{F^\bullet}$ and $M(S(\sigma))$ is defined with the extension $S(\sigma)(0) = 0$. Therefore $M(S(\sigma)) = \sigma$ and $M \circ S \cong Id_{\mathcal{SMF}}$.

ii - $S \circ M \cong Id_{\mathcal{SG}}$. Let G be a SG. Again, $M(G) = G \cup \{0\}$ and $S(M(G)) = M(G) \setminus \{0\}$. Hence $S(M(G)) = G$. Next, let $f : G \to H$ be a SG-morphism. How $M(f)$ is defined with the extension $f(0) = 0$ and
$S(M(f)) = M(f)|_{M(G)\setminus\{0\}}$, we have that $S(M(f)) = f$ and $S \circ M \cong Id_{\mathcal{SG}}$, finalizing the proof.

□

We can summarize the functors obtained by the following diagram:



Theorem 6.2.13. *Let $M : \mathcal{SG} \to \mathcal{SMF}$ the functor defined in 6.2.7.*

i - M preserves products.

ii - M preserves quotients.

iii - M preserves directed limits.

Proof.

i - Firstly, observe that $\mathcal{SMF}$ has products, because the categorical equivalence with $\mathcal{SG}$. However, this product is not the restriction of the product in $\mathcal{MF}$.

Now, let $\{G_i\}_{i\in I}$ be a family of special groups. The product $G = \prod_{i\in I}^{n} G_i$ is defined with the operation and special relation given pontwise, and $-1 = (-1, -1, ...)$, i.e,

$$\langle (a_i)_{i\in I}, (b_i)_{i\in I}\rangle \equiv_G \langle (c_i)_{i\in I}, (d_i)_{i\in I}\rangle \Leftrightarrow \langle a_i, b_i\rangle \equiv_{G_i} \langle c_i, d_i\rangle, \forall\, i \in I.$$

This implies that $(a_i)_{i\in I} D_G((c_i)_{i\in I}, (d_i)_{i\in I})$ iff $a_i \in D_{G_i}(c_i, d_i)$ for all $i \in I$. This argument shows that

$$M\left(\prod_{i\in I}^{n} G_i\right) = \prod_{i\in I}^{n} M(G_i).$$

ii - More specifically, we want to show that if G is a special group and $\Delta \subseteq G$ is a satured subgroup [3] then $M(G/\Delta) \cong M(G)/\tilde{\Delta}$, when $\tilde{\Delta} = \{M(\delta) : \delta \in \Delta\}$. The isometry relation on the quotient group G/Δ is:

$$\langle a/\Delta, b/\Delta\rangle \equiv^{*}_{G} \langle c/\Delta, d/\Delta\rangle \text{ iff } \begin{cases} \exists\, a', b', c', d' \in G \text{ such that} \\ aa', bb', cc', dd' \in \Delta \text{ and} \\ \langle a', b'\rangle \equiv_G \langle c', d'\rangle. \end{cases}$$

This implies that $a/\Delta \in D_{G/\Delta}(c/\Delta, d/\Delta)$ iff there exist $r, s, t \in G$ such that $r \in D_G(s, t)$, with $ar, cs, dt \in \Delta$. Multiplying this by $arcsdt \in \Delta$, we have $a(csdt) \in D_G(c(ardt), d(arcs))$, and $csdt, ardt, arcs \in \Delta$. Aplying the functor, we have $\overline{a} \in \overline{c} + \overline{d}$ in $M(G)/\tilde{\Delta}$, and the desired follow by this.

iii - Let $\mathcal{G} = (G_i, \{f_{ij} : i \leq j\}, I)$ be an inductive system of special groups. Let G be the inductive limit of $\mathcal{G}$ and let $f_i : G_i \to G$ the correspondent SG-morphism associated to this construction. Then given $\langle a, b\rangle \equiv_G \langle c, d\rangle$ iff there exist $i \in I$ and $a_i, b_i, c_i, d_i \in G_i$ such that $\langle a_i, b_i\rangle \equiv_{G_i} \langle c_i, d_i\rangle$ and $\langle f_i(a_i), f_i(b_i)\rangle = \langle a, b\rangle$, $\langle f_i(c_i), f_i(d_i)\rangle = \langle c, d\rangle$ (both over G). This is suffice to show that

$$M\left(\varinjlim_{i\in I} G_i\right) = \varinjlim_{i\in I} M(G_i).$$

□

6.2.2 Multirings, Abstract Real Spectra and Real Semigroups

Theorem 6.2.14. *Let (X, G) an abstract real spectra and define $a + b = \{d \in G : d \in D^t(a, b)\}$. Then $(G, +, \cdot, -, 0, 1)$ is a real reduced multiring.*

[3] We say that Δ is *saturated* if for all $a \in G$, $a \in \Delta \Rightarrow D_G(1, a) \subseteq \Delta$.

Proof. Firstly, observe that $+$ is well-defined. Then, we will verify the conditions of definition 6.1.5. Commutativity, associativity and neutral element ($a \in D^t(0,b) \Leftrightarrow a = b$) are immediate. In fact, the unique non-trivial part of the proof is

$$a \in D^t(b,c) \Rightarrow b \in D^t(a,-c) \text{ and } c \in D^t(-b,a).$$

We will prove that $b \in D^t(a,-c)$ and the case $c \in D^t(-b,a)$ analogous. Let $x \in X$ and $a \in D^t(b,c)$. Remember that $a \in D^t(b,c)$ means that $a(x)b(x) > 0$ or $a(x)c(x) > 0$ or $a(x) = 0$ and $b(x) = c(x)$ happens for all $x \in X$.

If $a(x)b(x) > 0$, then $b(x)a(x) > 0$ and it is done. If $a(x)c(x) > 0$, we have some cases:

- $a(x) = c(x) = 1$. We can suppose that $a(x)b(x) \leq 0$ and $b(x) \in \{0,1\}$. If $b(x) = 0$ it is done. If $b(x) = 1$, then $b(x)[-c(x)] > 0$.
- $a(x) = c(x) = 1$. Again, we will suppose that $a(x)b(x) \leq 0$ and $b(x) \in \{0,1\}$. If $b(x) = 0$ it is done. If $b(x) = 1$, then $b(x)[-c(x)] > 0$.
- $a(x) = 0$ and $b(x) = c(x)$. If $b(x) = c(x) = 0$ then $b(x) = 0$ and $a(x) = c(x)$. If $b(x) = c(x) \neq 0$, then $b(x)c(x) > 0$.

Hence G is a multiring. For the real reduced part, we have immediatelly that $1 \neq 0$ and $a^3 = a$ for all $a \in G$.

$$c \in D^t(a, ab^2) \Leftrightarrow c(x)a(x) = 0 \vee (c(x) = 0 \wedge a(x) = 0) \Leftrightarrow c = a$$

and

$$c \in D^t(a^2, b^2) \Leftrightarrow \forall\, x \in G(c(x) = 1 \vee (c(x) = 0 \wedge a(x)b(x) = 0))$$

This implies that c is uniquely determined. Therefore, G is a real reduced multiring. □

Corollary 6.2.15. *There is a functor $M : \mathcal{ARS}^{op} \to \mathcal{MR}_{red}$.*

Proof. Let (X,G) and (Y,H) be abstract real spectras and $\tau : Y \to X$ be a ARS-morphism. Define $M(X)$ how the real reduced multiring as in theorem 6.2.14 and $M(\tau) = f$ when $f : G \to H$ is the group homomorphism induced by τ. We have tat $c \in a + b \Rightarrow c \in D^t(a,b) \Rightarrow f(c) \in D^t(f(a), f(b)) \Rightarrow f(c) \in f(a) + f(b)$ by an argument analogous to the corollary 6.2.19. Then $M(\tau)$ is a multiring morphism and this is suffice to prove that M is a (contravariant) functor. □

Theorem 6.2.16. *Let A be an real reduced multiring and consider the strong embedding $i : A \to Q_2^{Sper(A)}$ given by $i(a) = \hat{a} : Sper(A) \to Q_2$ when $\hat{a}(\sigma) = \sigma(a)$. Define $\hat{A} = i(A)$. Then $(Sper(A), \hat{A})$ is an abstract real spectra.*

Proof. We will check each definition of 5.1.25:

AX1 - Is consequence of $\hat{A}$ be a submultiring of $Q_2^{\mathrm{Sper}(A)}$.

AX2 - Let P be a submonoid of $\hat{A}$ such that $P \cup -P = \hat{A}$, $-1 \notin P$, $a, b \in P \Rightarrow D(a,b) \subseteq P$ and $ab \in P \cap -P \Rightarrow a \in P \cap -P$ or $b \in P \cap -P$. First, Fora Temer. Second, observe that

$$D^t(a,b) = \{d : d \in a + b\}. \tag{6.3}$$

In fact, $d \in D^t(a,b)$ if and only if $\forall \sigma \in \mathrm{Sper}(A)$, $\sigma(d)\sigma(a) > 0$ or $\sigma(d)\sigma(b) > 0$ or $\sigma(d) = 0$, and $\sigma(a) = -\sigma(b)$ if and only if $\sigma(d) \in \sigma(a) + \sigma(b)$ for all $\sigma \in \mathrm{Sper}(A)$. By the local-global principle for multirings 6.1.42 we have that this happens if and only if $d \in a + b$.

AX3 - This is consequence of 6.3 and associativity.

□

Theorem 6.2.17. *There exist an equivalence of categories between $\mathcal{ARS}^{op}$ and $\mathcal{MR}_{red}$.*

Proof. Define $M : \mathcal{ARS}^{op} \to \mathcal{MR}_{\mathrm{Red}}$ and $\mathrm{Spec} : \mathcal{MR}_{\mathrm{Red}} \to \mathcal{ARS}^{op}$ as we already defined in corollary 6.2.15 and theorem 6.2.16. Follow that $M \circ \mathrm{Spec} \cong Id_{\mathcal{MR}_{Red}}$ and $\mathrm{Spec} \circ M \cong Id_{\mathcal{ARS}^{op}}$. □

Theorem 6.2.18. *Let $(G, \cdot, 1, 0, -1, D)$ be a realsemigroup and define $+ : G \times G \to \mathcal{P}(G) \setminus \{\emptyset\}$, $a + b = \{d \in G : d \in D^t(a,b)\}$ and $- : G \to G$ by $-(g) = -1 \cdot g$. Then $(G, +, \cdot, -, 0, 1)$ is a real reduced multiring.*

Proof. Firstly, observe that by 5.2.14(xv) the sum is well-defined, i.e, $D^t(a,b) \neq \emptyset$ for all $a, b \in G$.

Now, we will check that G is a multiring: of course, by RS0 we have $a + b = b + a$ (i.e, $D^t(a,b) = D^t(b,a)$) and

$$\begin{cases} d \in D^t(a,b) \Leftrightarrow d \in D(a,b) \wedge -a \in D(-d,b) \wedge -b \in D(a,-d) \\ a \in D^t(d,-b) \Leftrightarrow a \in D(d,-b) \wedge -d \in D(-a,-b) \wedge b \in D(d,-a) \\ b \in D^t(-a,d) \Leftrightarrow b \in D(-a,d) \wedge a \in D(-b,d) \wedge -d \in D(-a,-b) \end{cases}$$

So $d \in D^t(a,b) \Rightarrow a \in D^t(d,-b) \wedge b \in D^t(-a,d)$, or in other words, $d \in a+b \Rightarrow a \in d+(-b) \wedge b \in (-a)+d$. If $x = y$, by RS1 $x \in 0 + y$. Conversely, let $x \in 0 + y$. We just proved that $0 \in x - y$ and $0 \in y - x$ then by RS7, $x = y$. How RS3 states the associativity (like 6.1.3) we have that G is a commutative multigroup.

Because the commutative semigroup structure of $(G, \cdot, -1, 0, 1)$, we have that $(G, \cdot, 1)$ is a commutative monoid and $a \cdot 0 = 0$ for all $a \in G$. The distributive law is just 5.2.14(iii), we have that G is a multiring.

Finally, we prove that G is real reduced. We alread have that $-1 \neq 0$ and $a^3 = a$. We have too, that $1 \in D^t(1, b^2)$ by 5.2.14(ix) then by 5.2.14(iii) $a \in D^t(a, ab^2)$. Now, how $t^3 = t$ we have

$$\begin{aligned} t \in D^t(v^2x, w^2y) \Leftrightarrow \\ t \in D(v^2x, w^2y) \wedge -v^2x \in D(-t^3, w^2y) \wedge -w^2y \in D(v^2x, -t^3) \\ \overset{\text{RS4}}{\Leftrightarrow} t \in D(x,y) \wedge -v^2x \in D(-t,y) \wedge -w^2y \in D(x,-t) \end{aligned} \tag{6.4}$$

Hence, how by RS1 $-a \in D(-a,-x)$ for all $a, x \in G$, follow

$$\begin{aligned} x \in D^t(a, ab^2) \Leftrightarrow x \in D^t(a^2 \cdot a, (ab)^2 \cdot a) \overset{6.4}{\Leftrightarrow} \\ x \in D(a,a) \wedge -a \in D(-x,a) \wedge -ab^2 \in D(a,-x) \Leftrightarrow \\ [x \in D(a,a) \wedge -a \in D(-x,a) \wedge -a \in D(a,-x)] \wedge -ab^2 \in D(a,-x) \Leftrightarrow \\ x \in D^t(a,a) \wedge -ab^2 \in D(a,-x) \overset{5.2.14(vii+x)}{\Leftrightarrow} x = a \end{aligned}$$

Then $a + ab^2 = \{a\}$. For the last property, we have by theorem 5.2.29(ii), we have that $d \in D^t(b^2, c^2) \Leftrightarrow h(d) \in D^t_{\mathbf{3}}(h(b^2), h(c^2))$ for every $h \in X_G$. Since $D^t(t^2, s^2)$ is unitary for every $s, t \in \mathbf{3}$, we have that $D^t(b^2, c^2)$ is unitary for every $b, c \in G$.

Hence, by definition 6.1.45 G is a real reduced multiring. □

Corollary 6.2.19. *There is a full and faithful functor $M : \mathcal{RS} \to \mathcal{MR}_{red}$.*

Proof. Let $R, S \in \mathcal{RS}$ and $f : R \to S$ a RS-morphism. Define $M(R)$ how the real reduced multiring as in theorem 6.2.18 and $M(f) = f$. Of course, $M(f)$ is a multiring morphism, because $c \in a + b \Rightarrow c \in D^t(a, b) \Rightarrow f(c) \in D^t(f(a), f(b)) \Rightarrow f(c) \in f(a) + f(b)$. This is suffice to prove that M is a functor. Full and faithfullyness are immediate. □

In order to associate a real semigroup to each real reduced multiring, we are going to set down some facts about multirings:

Proposition 6.2.20. *Let A be a real reduced multiring. Then we have the following:*

i - $x \in ax^2 + bx^2$ *if and only if* $x \in aA^2 + bA^2$;

ii - $x \in a + b$ *if and only if* $x \in ax^2 + bx^2$, $-a \in ba^2 - xa^2$ *and* $-b \in ab^2 - xb^2$;

iii - *If* $ax = bx$, $ay = by$ *and* $z \in xz^2 + yz^2$, *then* $az = bz$;

iv - *If* $x \in ax^2 + bx^2$, *then* $x^2 \in a^2x^2 + b^2x^2$.

Proof. Since A is a real reduced multiring, we have by the local-global principle for multirings 6.1.42 that $a \in b + c$ if and only if $\sigma(a) \in \sigma(b) + \sigma(c)$ for all $\sigma \in \mathrm{Sper}(A)$. So to prove these items we just need to do it in Q_2 which is trivial (it is just an amount of cases). □

Theorem 6.2.21. *Let A be a real reduced multiring. Then $(A, \cdot, 1, 0, -1, D)$ is a realsemigroup, where $d \in D(a, b) \Leftrightarrow d \in d^2a + d^2b$.*

Proof. Firstly, note that by the preceding proposition, $x \in D(a, b) \Leftrightarrow x \in aA^2 + bA^2$ and $D^t(a, b) = a + b$.

Now, we will check each axiom of definition 5.2.10:

RS0 - Is just commutativity of sum.

RS1 - It follows by item i of the preceding proposition.

RS2 - $a \in D(b, c) \Leftrightarrow a \in a^2b + a^2c \overset{d^3=d}{\Rightarrow} ad \in (ad)^2bd + (ad)^2cd \Rightarrow ad \in D(bd, cd)$.

RS3 - It is just associativity of sum.

RS4 - It follows by item i of the preceding proposition.

RS5 - It follows by item iii of the preceding proposition.

RS6 - It follows by the characterization of D^t.

RS7 - Since in a real reduced multiring we have $a + a = a$, if exist $c \in a - b$ with $-c \in a - b$, then $0 \in c - c \in a - b + a - b = a - b$ and then $a = b$.

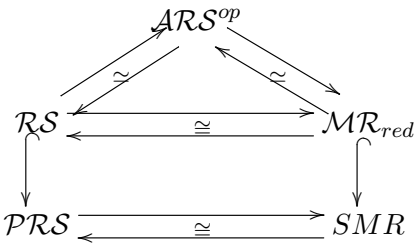
RS8 - It follows by item iv of the preceding proposition.

□

Corollary 6.2.22. *There exist an equivalence of categories between $\mathcal{RS}$ and $\mathcal{MR}_{red}$.*

Proof. Define the functor $S : \mathcal{MR}_{\text{red}} \to \mathcal{RS}$ as in corollary 6.2.19. The proof of $S \circ M \cong Id_{\mathcal{RS}}$ and $M \circ S \cong Id_{\mathcal{MR}_{\text{red}}}$ is mutatis mutandis of theorem 6.2.12. □

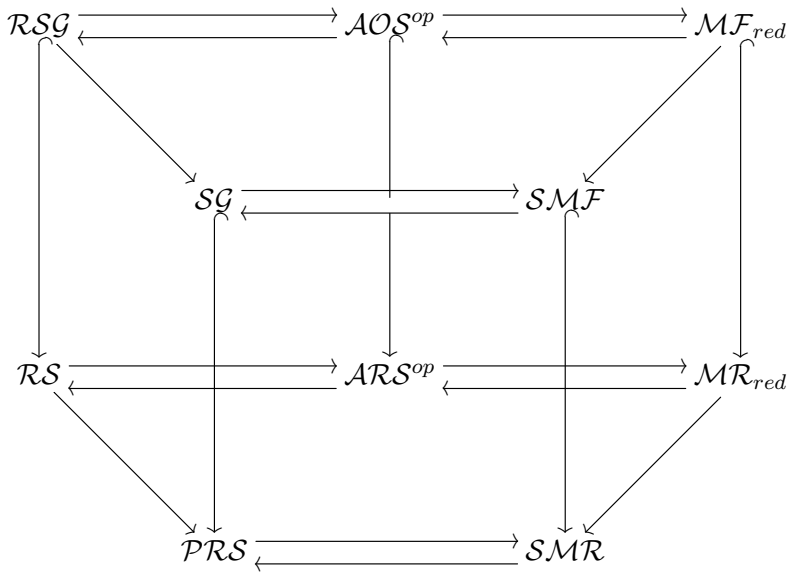
Of course, we can adapte the proof of theorem 6.2.18 to obtain a functor $M : \mathcal{PRS} \hookrightarrow \mathcal{MR}$. The image of this functor is a subcategory of $\mathcal{MR}$, that we will call *special multirings*, and denote by $\mathcal{SMR}$. Again, we can summarize the functors obtained by the following diagram:



Corollary 6.2.23. *Let $M : \mathcal{RS} \to \mathcal{MR}_{red}$ the functor defined in 6.2.18. Then M preserves products and directed limits.*

Proof. Follow directly by the definition of product and directed limits in $\mathcal{RS}$. □

Finally, we provide a diagram for a better visualization of the functors obtained:



6.3 Some final considerations

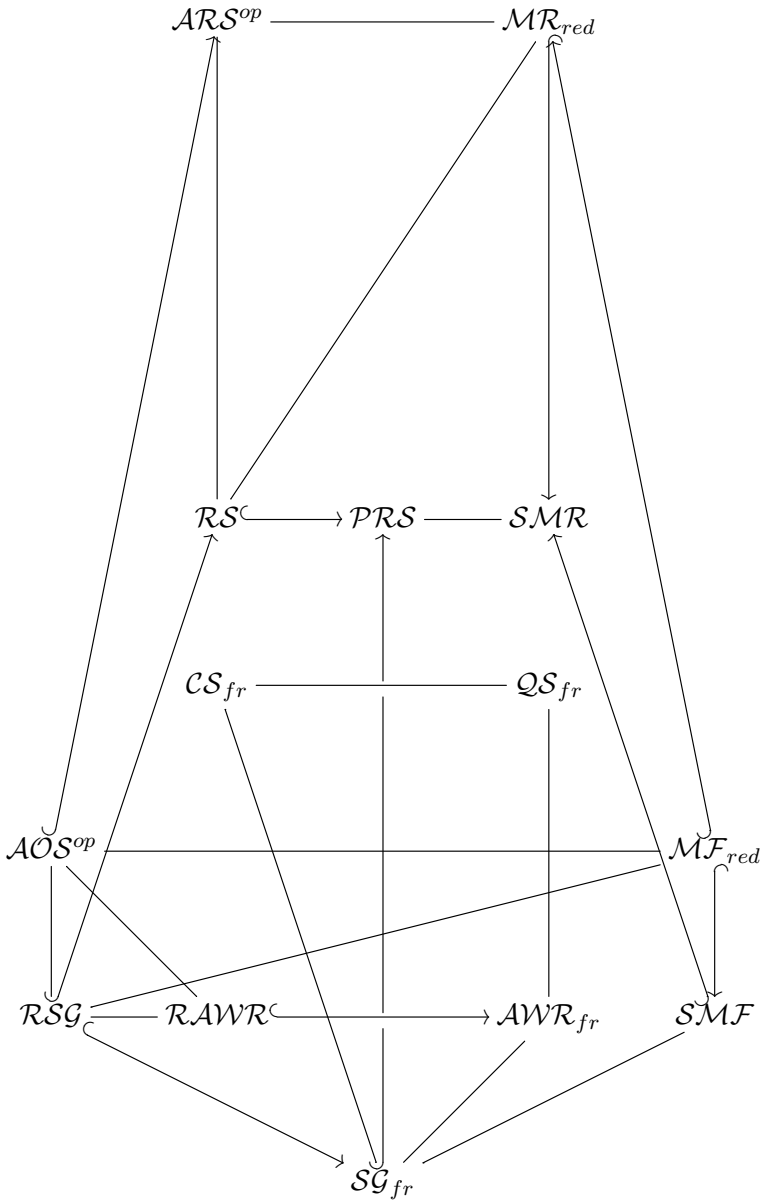
We hope that our task of

"Establish precisely what are the functorial connections between the abstract theories of quadratic forms as soon as to create a short and introductory path from the classic theory to the abstract ones"

has been successfully achieved. The algebraic theory of quadratic forms is a broad and deep subject of research, and the abstract theories of quadratic forms are teaching us an old an important lesson, that is

"If you have a difficult mathematical problem to deal with, it is better to try to abstract it as many different ways as you can, and "hear" the "point of view" that each of these abstractions would like to say to you."

Further, we hope that this work has aroused interest in the classical problems of quadratic form theory and its abstract theories, as well as in this new and promising theory of multirings and multifields. If this is not the case, at least we leave the complete functorial map of our "Chamber of The Secrets"[4]:



[4]Here, the arrows without a source and a target indicates equivalence or isomorphism of categories, and the subscript "fr" indicates a "formally real" notion that, if was not defined, then is the restriction of the equivalence or isomorphism functor of the entire categorie (like when we define the formally real Cordes Scheme).

Bibliography

[Cor75] Craig Cordes. Kaplansky's radical and quadratic forms over non-real fields. *Acta Arithmetica*, 28:253–261, 1975.

[Cor76] Craig Cordes. Quadratic forms over nonformally real fields with a finite number of quaternion algebras. *Pacific Journal of Mathematics*, 63(2):357–365, 1976.

[dL96] Arileide Lira de Lima. *Les groupes speciaux. Aspects algebriques et combinatoires de la theorie des espaces d'ordres abstraits.* PhD thesis, 1996.

[DM00] Maximo Dickmann and Francisco Miraglia. *Special groups: Boolean-theoretic methods in the theory of quadratic forms.* Number 689. American Mathematical Soc., 2000.

[DM15] Maximo Dickmann and Francisco Miraglia. *Faithfully quadratic rings*, volume 238. American Mathematical Society, 2015.

[DP04] Maximo Dickmann and A Petrovich. Real semigroups and abstract real spectra. i. *Contemporary Mathematics*, 344:99–120, 2004.

[DST19] Maximo Dickmann, Niels Schwartz, and Marcus Tressl. *Spectral spaces*, volume 35 of *New Mathematical Monographs.* Cambridge University Press, 2019.

[Efr06] Ido Efrat. *Valuations, orderings, and Milnor K-theory.* Number 124. American Mathematical Soc., 2006.

[End72] Otto Endler. *Valuation theory.* Springer, 1972.

[Hoc69] Melvin Hochster. Prime ideal structure in commutative rings. *Transactions of the American Mathematical Society*, 142:43–60, 1969.

[Jun18] Jaiung Jun. Algebraic geometry over hyperrings. *Advances in Mathematics*, 323:142–192, 2018.

[Knu91] Max-Albert Knus. *Quadratic and Hermitian forms over rings*, volume 294 of *Grundlehren der mathematischen Wissenschaften A Series of Comprehensive Studies in Mathematics.* Springer-Verlag, 1991.

[KSS88] M Kula, L Szczepanik, and Kazimierz Szymiczek. Quadratic form schemes and quaternionic schemes. *Fundamenta Mathematicae*, 3(130):181–190, 1988.

[Kul79] Mieczysaw Kula. Fields with prescribed quadratic form schemes. *Mathematische Zeitschrift*, 167(3):201–212, 1979.

[Lam83] Tsit-Yuen Lam. *Orderings, valuations and quadratic forms*, volume 52. American Mathematical Soc., 1983.

[Lam05] Tsit-Yuen Lam. *Introduction to quadratic forms over fields*, volume 67. American Mathematical Soc., 2005.

[Mar80] Murray Marshall. *Abstract Witt rings*. Kingston, Ont.: Queen's University, 1980.

[Mar96] Murray A Marshall. *Spaces of orderings and abstract real spectra*. Springer, 1996.

[Mar06] Murray Marshall. Real reduced multirings and multifields. *Journal of Pure and Applied Algebra*, 205(2):452–468, 2006.

[Mil70] John Milnor. Algebraic k-theory and quadratic forms. *Inventiones mathematicae*, 9(4):318–344, 1970.

[San15] Duílio Ferreira Santos. Elementos da teoria algébrica das formas quadráticas e de seus anéis graduados. Master's thesis, Universidade de São Paulo, 2015.

[Vir10] Oleg Viro. Hyperfields for tropical geometry i. hyperfields and dequantization. *arXiv preprint arXiv:1006.3034*, 2010.

Index