Multialgebraic structures and applications in abstract theories of quadratic forms and graded rings

Kaique Matias de Andrade Roberto

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

Área de Concentração: Matemática

Orientador: Prof. Dr. Hugo Luiz Mariano

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro da CAPES

Data da defesa: 09 de agosto de 2023

Multialgebraic structures and applications in abstract theories of quadratic forms and graded rings

Esta versão da tese contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa da versão original do trabalho, realizada em 09/08/2023. 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. Francisco Miraglia Neto - IME-USP
- Prof. Dr. Maximo Alejandro Dickmann - UP
- Prof. Dr. Alejandro Petrovich - UBA
- Prof. Dr. Oliver Lorscheid - IMPA

Agradecimentos

Estas notas constituem o ponto alto de 10 anos de trabalho duro. Em todo esse tempo, fui cercado pela companhia de pessoas maravilhosas, sem as quais esse trabalho não teria sido sequer imaginado.

Tive o privilégio de ter a companhia da minha amada esposa e companheira Amanda Freitas, que além de me incentivar a continuar demonstrando teoremas, é uma grande inspiração para mim. Além disso, toda a minha família e grandes amigos também me ajudaram durante essa jornada, principalmente o Daniel Reis, o Marcos Rafael e o Ricardo Murça, a Ana Luiza Tenório e o Hugo Rafael, que basicamente acompanharam todo o processo "multi-algébrico" desde a concepção. Também pude contar com companhia e inspiração da minha yalorixá Osunirê, minha mãe pequena Kolegi e pai pequeno Taogi e os meus mestres e amigos Leandro e Jota, sem os quais o meu ori não teria tido a paz e concentração necessárias para a escrita da tese e de tudo que a envolve.

Agradeço também àqueles que cuidaram de mim mas infelizmente não se encontram mais aqui: espero que estejam me assistindo do Orun.

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. Foram 10 anos aprendendo matemática contigo e espero que estas notas estejam à altura do trabalho que desenvolvemos juntos.

Agradeço à CAPES e OBMEP, pelo financiamento e suporte ao longo destes últimos 10 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.

Foi uma honra e uma grande alegria poder ter compartilhado todo esse tempo com vocês, alegria que espero ter transformado na matemática que seguem nas próximas 200 páginas.

Resumo

ROBERTO, K. M. A. **Estruturas multi-algébricas e aplicações em teorias abstratas de formas quadráticas e anéis graduados**. 2023. 214 f. Tese (Doutorado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2023.

O objetivo deste trabalho é iniciar a investigação de possíveis relações matemáticas que configurem um "novo quadro adjunto" entre grupos especiais, anéis graduados, 2-grupos e 2-grupos profinitos. Nós focamos na primeira parte deste programa, i.e. nas relações entre anéis graduados e grupos especiais. Em nossas investigações, a teoria dos multi anéis/hipercorpos desempenhou um papel central, e obtivemos um resultado interessante: uma ampla extensão (para todos os grupos/hipercorpos especiais) da validade do Arason-Pfister Hauptsatz ([7]) - uma resposta positiva para uma questão formulada por J. Milnor no clássico artigo de 1970 ([52]) - e aplicamos este resultado na obtenção de propriedades associadas aos anéis graduados provenientes de hipercorpos especiais ([30], [18]).

Palavras-chave: grupo especial, anéis graduados, 2-grupos profinitos, multi anéis, hipercorpos, formas quadráticas, Arason-Pfister hauptsatz.

Abstract

ROBERTO, K. M. A. **Multialgebraic structures and applications in abstract theories of quadratic forms and graded rings**. 2023. 214 f. Tese (Doutorado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2023.

The aim of this work is to initiate the investigation of the precise mathematical relationships so that possible configuring a “new adjoint” situation between special groups, graded rings, 2-groups and profinite 2-groups. We focused in the first part of this program, i,e, in the relations between graded rings and special groups. In our investigations, the theory of multirings/hyperrings played a central role, and we got an interesting result: we have obtained an wide extension (to all special hyperfields, or special groups) of the validity of the Arason-Pfister Hauptsatz ([7]) - a positive answer to a question posed by J. Milnor in a classical paper of 1970 ([52])- and applied that to obtain interesting properties of graded rings associated to special hyperfields ([30], [18]).

Keywords: special groups, graded rings, profinite 2-group, multirings, hyperfield, quadratic forms, Arason-Pfister hauptsatz.

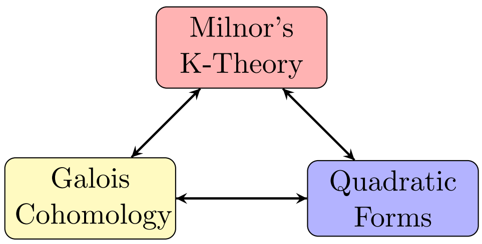
Contents

Introduction

It can be said that the Algebraic Theory of Quadratic Forms (ATQF) was founded in 1937 by E. Witt, with the introduction of the Witt ring concept of a given field, constructed from quadratic forms with coefficients in the field: given F, an arbitrary field of characteristic $\neq 2$, $W(F)$, the Witt Ring of F, classifies the quadratic forms on F that are regular and anisotropic. Moreover, this ring establishes a strong connection between quadratic forms and orderings in a field F: the set of orderings in F is in one-to-one correspondence with the set of minimal prime ideals of the Witt ring of F, and more, the set of orderings in F equipped with the Harrison's topology is a Boolean topological space and that by the bijection above, it is identified with a subspace of the Zariski spectrum of $W(F)$.

Further questions about Witt's ring structure $W(F)$ could only be answered about three decades after the original idea of Witt, through the introduction and analysis of the concept of Pfister form. The Pfister forms of degree $n \in \mathbb{N}$, in turn, are additive generators of the n-th power $I^n(F)$ of the fundamental ideal $I(F) \subseteq W(F)$ (the ideal determined by the anisotropic forms of even dimension).

In the early 1970s, J. Milnor, in his celebrated article [52], established deep functorial relationships, such as illustrated in the diagram below:



More specifically, Milnor determines a graded ring $k_*(F)$ (of reduced K-theory mod 2) associated to the field F, that interpolates, through morphisms of graded rings

$$h_*(F) : k_*(F) \longrightarrow H^*(F) \text{ and } s_*(F) : k_*(F) \longrightarrow W_*(F),$$

Where

$$W_*(F) := \bigoplus_{n \in \mathbb{N}} I^n(F)/I^{n+1}(F)$$

$$H^*(F) := \bigoplus_{n \in \mathbb{N}} H^n(Gal(F^s|F), \{\pm 1\})$$

are, respectively, the graded Witt ring of F and the graded cohomology ring of F (here, F^s denotes the separable closure of F).

In this context, two fundamental questions are posed by Milnor:

i - Is true that $\bigcap_{n\in\mathbb{N}} I^n(F) = \{0\}$?

ii - Are the morphisms $h_*(F), s_*(F)$ *isomorphisms* of graded rings, for all field F of characteristic not 2?

The question (i) was answered positively a few years later in a celebrated article by Arason and Pfister ([7]). Question (ii) resisted much longer until it was solved positively around the 2000s by V. Voevodsky and co-authors ([42]), results that earned to the first the Fields medal.

The absolute Galois group of F, $\mathrm{Gal}_F(F^s)$, detects the ordenability of F: F is formally real if and only if there is a non-trivial involution, i.e, an element $\sigma \in \mathrm{Gal}_F(F^s)$, $\sigma \neq 1$ such that $\sigma^2 = 1$. But the Galois group detects more: the ordering space $X_F := \mathrm{Sper}(F)$ is homeomorphic to the set

$$\{[g] : g \text{ is a non-trivial involution of } \mathrm{Gal}_F(F^s)\},$$

where $[g] := \{\sigma^{-1}g\sigma : \sigma \in \mathrm{Gal}_F(F^s)\}$.

We can see that, via the established functors, the Galois cohomology also describes orderings via the encoding of (graded) Witt rings. In fact, by Milnor's triangle, $W_*(F) \cong H^*(\mathrm{Gal}_F(F^s), \mathbb{Z})$ and, keeping in mind that also $W_*(F)$ determines $W(F)$, we get a connection between the classic Witt ring $W(F)$ and Galois cohomology. Moreover, since the space of orderings X_F is in natural bijection with $\mathrm{Hom}(W(F), \mathbb{Z})$, we obtain (again) a connection between orderings and Galois cohomology.

From the proof of Milnor's conjectures by Voevodski and the development of the theory of special groups - an abstract (first-order) theory of ATQF, introduced by M. Dickmann and F. Miraglia in the 1990s, – it was possible to demonstrate Conjectures on signatures put forward by M. Marshall and T. Lam in the mid-1970s ([27], [29]). We present below these two cases that exemplify the success of the application of instruments developed by the theory of the special groups:

Let G be a special group, $X_G = Hom_{SG}(G, \mathbb{Z}_2)$ the ordering space of G and $W(G)$ the Witt ring associated to G. Denote $I^n(G)$ by the n-th power of the fundamental ideal (the ideal of forms of even dimension) in $W(G)$ and $W_{tor}(G)$ denote the torsion subgroup of $W(G)$. Consider the following statements:

a - For all G-form ψ, if $sgn_\sigma(\psi) \equiv 0 \ mod\ 2^n$ for all $\sigma \in X_G$, then $\psi \in I(G)$.

b - For all G-form ψ, if $sgn_\sigma(\psi) \equiv 0 \ mod\ 2^n$ for all $\sigma \in X_G$, then $\psi \in I(G) + W_{tor}(G)$.

The **Marshall's signature Conjecture** ([MC]), originally stated in the (dual) context of abstract ordering spaces (see [48]), is that the statement **(a)** above is true for all **reduced** special group G. The **Lam's Conjecture** ([LC]), originally stated in the traditional context of formally real fields (see [43]), is that the statement **(b)** above is true for all **formally real** special group G. Note that both reverses of the above implications are true.

The fundamental stone for the solutions of Marshall's signature conjecture and Lam's conjecture for Pythagorean and formally real fields the introduction of the Boolean hull functor in SG-theory mainly through the definition of Horn-Tarski and Stiefel-Whitney invariants for isometry (see [28]). These encoding allows to rewrite [MC] in terms of information about the graded Witt ring and, through Voevodsky's results, switch these information in terms of the cohomology graded ring of a field, where the question is finally solved by the application of cohomological methods.

Entering in the "cohomology realm", in 1970's was established the first relations between quadratic forms and Galois cohomology, via the absolute Galois group $\mathrm{Gal}_F(F^s)$ ([52]). These relations was improved, first via the quadratic closure $F^q|F$ in the 1980's, and in the late 1990's via a certain quotient

$$\mathrm{Gal}_F(F^q) \twoheadrightarrow \mathrm{Gal}_F(F^{(3)})$$

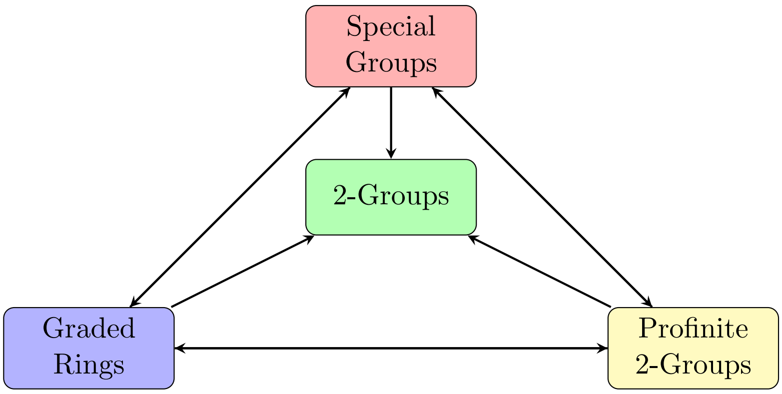
called the W-group of F (see [53]). Moreover, the induced arrow

$$H^*(Gal(F^s|F), \{\pm 1\}) \to H^*(Gal(F^{(3)}|F), \{\pm 1\})$$

is a monomorphism whose image is the subgraded ring of $H^*(Gal(F^{(3)}|F), \{\pm 1\})$ generated by cup products of level 1 members. However, only after 2010 the studies of this setting[1] have established that $F^{(3)}|F$ is the minimal extension that determines (and is determined by) $W(F)$.

All that was exposed above compose an amount of evidences so that we propose a new diagram

`new-intro`



Our proposal is to investigate the precise mathematical relationships so that the above diagram will be true, possible configuring a "new adjoint" situation for these theories, obviously with the intention of exploring the possible transport of information from this. It is important to point out that the current paradigm in abstract quadratic forms theories is that of equivalence (or duality) of categories, which is a relatively rigid connection. The context of adjunction allows more flexibility in attacking problems from one theory encoded in another.

In Chapter 1 we present the theory of multirings and multifields/hyperfields, closely to the perspective of Marshall's paper [47]. Roughly speaking, multirings are just "rings with a multivalued addition". In fact, many ideas of the ring theory can be imported. The main references are [47], [24], [23], [45] and [58], and we follow [47] closely. In fact, the main proofs concerning orderings over hyperfields are easier than the field case, and we got an Artin-Schreier Theory very similar to the field one (see for instance, Propositions 1.4.5 and 1.6.3). We also characterize real reduced hyperfields (Corollary 1.5.3) and real reduced multirings (Proposition 1.8.4), which are respectively dual to Marshall's abstract ordering spaces and abstract real spectra.

In Chapter 2 we connect the theory of Chapter 1 with the with the most significant theories of quadratic forms, via two main motivations: 1) to describe interesting pairs (A, T) where A is a (multi)ring and $T \subseteq A$ is a certain multiplicative subset in such a way to obtain models of abstract theories of quadratic forms (special groups and real semigroups) via natural quotients - Marshall's quotient construction; and 2) use this construction to motivate a "non reduced" expansion of the theory of real semigroups to deal the formally real case, isolating axioms over pairs involving multirings and a subset with some properties. The main results are Theorem 2.3.4, 2.3.7, 2.3.10 and 2.5.4, which characterize precisely the necessary conditions for a hyperfield/multiring come from a

[1] Carried out mainly by I. Minac and co-authors.

special group/real semigroup. Proposition 2.4.3 deals with a question posed by the authors of [37]. We also got a new and interesting Example of real semigroup (2.5.15): $A/_mT$ for $A = \mathcal{C}(X,\mathbb{R})$ and $T = A^2 \cap \mathrm{nzd}(A)$, where X is a T_6 topological space.

In Chapter 3 we introduce the theory of superrings. They are important in order to obtain the quadratic extension available for special groups. The concept of superring first appears in ([6]). There are many important advances and results in hyperring theory, and for instance, we recommend for example, the following papers: [3], [5], [6], [4], [49], [54], [51], [50]. Surprisingly we have obtained an interesting theory of matrices, linear systems, vector spaces and algebraic extensions available for a certain subclass of superfields. If R is a full superring, then $M_{m\times n}(R)$ and $R[X]$ are superrings (Theorem 3.2.6 and 3.4.2). We also obtained a kind of simple algebraic extension for a superfield F (Theorem 3.6.12), which culminate in the existence and unicity of a full algebraic extension of a superfield F (Theorems 3.7.3 and 3.7.4). If F is a linearly closed superfield (the system $Ax = 0$ always have a non trivial solution), then we have a well defined dimension theory for the vector spaces over F (Theorem 3.8.21). The main examples of linearly closed superfields are hyperbolic hyperfields (3.8.23) and simple full algebraic extensions over a linearly closed superfield (3.8.25). The linearly closed interpreted in the context of special groups leads to interesting Isotropic (Corollary 3.8.27) and Hyperbolic (Corollary 3.8.28) interpolations. We finish this Chapter with a quantifier elimination procedure for superfields (Theorem 3.9.3), which is a direct generalization of a result obtained in [19].

In Chapter 4 we we provide some new steps towards the development of tools of algebraic theory of quadratic forms in this multiring setting: we have defined and explored K-theory and graded rings in the context of hyperfields that, in particular, provides a generalization and unification of Milnor's K-theory ([52]) and special groups K-theory ([30]). We develop some properties of this generalized K-theory, that can be seen as a free inductive graded ring. The main results are Theorems 4.5.6 and its Corollaries, which provides interchanging formulas between the three K-theories considered here.

In Chapter 5 we deal with the category IGR. Theorem 4.5.6 gives a hint that the category of Igr is a good abstract environment for studying questions of "quadratic flavour". So a better understanding of Igr's is at least desirable and this is the main purpose of this Chapter. We develop the general properties valid for Igr's and the main results here are Theorem 5.5.4, providing an adjunction between the categories of pre-special groups and (a subcategory of) inductive graded rings. We also characterize the Special and Weak Marshall Conjecture in the context of inductive graded rings (Section 5.6).

In Chapter 6 we develop the theory of quadratic extensions for hyperfields/superfields, through the development of results concerning the superrings of polynomials, envisaging some applications to algebraic theory of quadratic forms and Real Algebraic Geometry. The main results here are the Arason-Pfister Hauptsatz for **all** special groups (Theorem 6.3.2) and its consequences.

The Igr's functors W_*, k_* were extended by M. Dickmann and F.Miraglia from the category of fields of characteristic $\neq 2$ to the category of special groups (equivalently, the category of special hyperfields). Another relevant Igr functor, the graded cohomology ring, $H^*(Gal(F^s|F), \{\pm 1\})$ remains defined only on the field setting. Chapter 7 constitutes an attempt to provide an Igr functor associated to a (Galois) cohomology theory for special groups, based on the work of J. Minac and M. Spira [53]: we will define - by "generator and relations", $Gal(G)$, the *Galois Group of an SG G*, and provide some properties of this construction, as the encoding of the orderings on G. However, since deeper results will depend of a description of $Gal(G)$ "from below", and it still unavailable a complete theory of algebraic extension of (super)hyperfields, we will not pursue a more complete development of this cohomology theory in this thesis, reserving it for a future research. The main results are Theorem 7.3.13 and 7.3.15, which recover for the abstract context the characterization of orderings in terms of the involutions in the Galois group of a field.

In Chapter 8 we finish the work indicating some possibilities of future research connected with this thesis.

Chapter 1

Multirings and Hyperfields

Here, we present the theory of multirings and multifields/hyperfields, closely to the perspective of Marshall's paper [47]. Roughly speaking, multirings are just "rings with a multivalued addition". In fact, many ideas of the ring theory can be imported. The main references are [47], [24], [23], [45] and [58], and we follow [47] closely.

In fact, the main proofs concerning orderings over hyperfields are easier than the field case, and we got an Artin-Schreier Theory very similar to the field one (see for instance, Propositions 1.4.5 and 1.6.3).

We also characterize real reduced hyperfields (Corollary 1.5.3) and real reduced multirings (Proposition 1.8.4), which are respectively dual to Marshall's abstract ordering spaces and abstract real spectra.

1.1 On Multialgebras

There are several Definitions of multialgebra on the literature, considering that each multialgebra application in a specific area of Mathematics (mainly Algebra and Logic) requires a particular adaptation. Here, we adapt the notion of multialgebra used in [10]; the identity theory here presented is close to the exposed in [55].

Definition 1.1.1. *A* ***multialgebraic signature*** *is a sequence of pairwise disjoint sets*

$$\Sigma = (\Sigma_n)_{n\in\mathbb{N}},$$

where $\Sigma_n = S_n \sqcup M_n$, which S_n is the set of strict multi-operation symbols and M_n is the set of multioperation symbols. In particular, $\Sigma_0 = S_0 \sqcup M_0$, F_0 is the set of symbols for constants and M_0 is the set of symbols for multi-constants. We also denote

$$\Sigma = ((S_n)_{n\geq 0}, (M_n)_{n\geq 0}).$$

Definition 1.1.2. *Let A be any set.*

i - A multi-operation of arity $n \in \mathbb{N}$ over a set A is a function

$$A^n \to \mathcal{P}^*(A) := \mathcal{P}(A) \setminus \{\emptyset\}.$$

ii - A multi-operation of arity $n \in \mathbb{N}$ over a set A, $A^n \to \mathcal{P}^*(A)$, is strict*, whenever it factors through the singleton function $s_A : A \rightarrowtail \mathcal{P}^*(A)$, $a \mapsto s_A(a) := \{a\}$. Thus it can be naturally identified with an ordinary n-ary operation $A^n \to A$.*

A 0-ary multi-operation (respectively *strict* multi-operation) on A can be identified with a non-empty subset of A (respectively a singleton subset of A).

Definition 1.1.3. *A* ***multialgebra*** *over a signature $\Sigma = ((S_n)_{n\geq 0}, (M_n)_{n\geq 0})$, is a set A endowed with a family of n-ary multioperations*

$$\sigma_n^A : A^n \to \mathcal{P}^*(A),\ \sigma_n \in S_n \sqcup M_n,\ n \in \mathbb{N},$$

such that: if $\sigma_n \in S_n$, then $\sigma_n^A : A^n \to \mathcal{P}^*(A)$ is a strict *n-ary multioperation.*

Remark 1.1.4.

i - Every algebraic signature $\Sigma = (F_n)_{n\in\mathbb{N}}$ is a multialgebraic signature where $M_n = \emptyset$, for all $n \in \mathbb{N}$. Each algebra

$$(A, ((A^n \xrightarrow{f^A} A)_{f\in F_n})_{n\in\mathbb{N}})$$

over the algebraic signature Σ can be naturally identified with a multi-algebra

$$(A, ((A^n \xrightarrow{f^A} A \overset{s_A}{\rightarrowtail} \mathcal{P}^*(A))_{f\in F_n})_{n\in\mathbb{N}})$$

over the same signature.

ii - Every multialgebraic signature $\Sigma = ((S_n)_{n\in\mathbb{N}}, (M_n)_{n\in\mathbb{N}})$ induces naturally a first-order language

$$L(\Sigma) = ((F_n)_{n\in\mathbb{N}}, (R_{n+1})_{n\in\mathbb{N}})$$

where $F_n := S_n$ is the set of n-ary operation symbols and $R_{n+1} := M_n$ is the set of (n+1)-ary relation symbols. In this way, multi-algebras

$$(A, ((A^n \xrightarrow{\sigma^A} \mathcal{P}^*(A))_{\sigma\in S_n\sqcup M_n})_{n\in\mathbb{N}})$$

over a multialgebraic signature $\Sigma = (S_n \sqcup M_n)_{n\in\mathbb{N}}$ can be naturally identified with the first-order structures over the language $L(\Sigma)$ that satisfies the $L(\Sigma)$-sentences:

$$\forall x_0 \cdots \forall x_{n-1} \exists x_n(\sigma_n(x_0, \cdots, x_{n-1}, x_n)),\ \textit{for each}\ \sigma_n \in R_{n+1} = M_n, n \in \mathbb{N}.$$

Now we focus our attention into a more syntactic aspect of this multi-algebras theory. We start with a (recursive) definition of multi-terms:

Definition 1.1.5. *A* **(multi-)term** *on a multialgebra A of signature*

$$\Sigma = ((S_n)_{n\geq 0}, (M_n)_{n\geq 0})$$

is defined recursively as:

i - Variables $x_i, i \in \mathbb{N}$ are terms.

ii - If $t_0, \cdots, t_{n-1}$ are terms and $\sigma \in S_n \sqcup M_n$, then $\sigma(t_0, \cdots, t_{n-1})$ is a term.

We will call a multi-term t **strict***, whenever it is composed only by combination of* **strict** *multi-operations and variables. The notion of* **occurrence** *of a variable in a term is as the usual. We will denote $var(t)$ as the (finite set of variables) that occurs in the term t.*

To define an interpretation for terms, we need a preliminary step. Given

$$\sigma \in S_n \sqcup M_n,$$

we "extend" $\sigma^A : A^n \to \mathcal{P}^*(A)$ to a n-ary operation in $\mathcal{P}^*(A)$,

$$\sigma^{\mathcal{P}^*(A)} : \mathcal{P}^*(A)^n \to \mathcal{P}^*(A),$$

by the rule:

$$\sigma^{\mathcal{P}^*(A)}(A_0, \cdots, A_{n-1}) := \bigcup_{a_0 \in A_0} \cdots \bigcup_{a_{n-1} \in A_{n-1}} \sigma^A(a_0, \cdots, a_{n-1}).$$

Definition 1.1.6. *The **interpretation of a term** t on a multialgebra A over a signature*

$$\Sigma = ((S_n)_{n \geq 0}, (M_n)_{n \geq 0})$$

is a function $t^A : A^{var(t)} \to \mathcal{P}^*(A)$ and is defined recursively as follows:

i - The interpretation of a variable x_i, $x_i^A : A^{\{x_i\}} \to \mathcal{P}^*(A)$ is essentially the singleton function of A:

$$x_i^A : A^{\{x_i\}} \cong A \rightarrowtail \mathcal{P}^*(A), \text{ is given by the rule } (\hat{a} : \{x_i\} \to A) \mapsto \{a\}.$$

ii - If $t = \sigma(t_0, \cdots, t_{n-1})$ is a term and $\sigma \in S_n \sqcup M_n$, denote $T = var(t)$ and $T_i = var(t_i)$. Then $T = \bigcup_{i<n} T_i$. Consider ${t_i}_T^A : A^T \to \mathcal{P}^*(A)$ the composition

$$A^T \overset{proj^T_{T_i}}{\twoheadrightarrow} A^{T_i} \overset{t_i^A}{\to} \mathcal{P}^*(A),$$

where $proj^T_{T_i}$ is the canonical projection induced by the inclusion $T_i \hookrightarrow T$. Then

$$t^A : A^T \to \mathcal{P}^*(A)$$

is the composition

$$A^T \overset{({t_i}_T^A)_{i<n}}{\longrightarrow} (\mathcal{P}^*(A))^n \overset{\sigma^{\mathcal{P}^*(A)}}{\longrightarrow} \mathcal{P}^*(A).$$

Definition 1.1.7. *Let A be a multialgebra A over a signature $\Sigma = ((S_n)_{n \geq 0}, (M_n)_{n \geq 0})$ and let t_1, t_2 be Σ-terms. We say that A realize that t_1 is* **contained in** t_2*, (notation: $A \models t_1 \sqsubseteq t_2$) whenever $t_1^A(\bar{a}) \subseteq t_2^A(\bar{a})$, for each tuple $\bar{a} : var(t_1) \cup var(t_2) \to A$.*

Apart from the notion of atomic formulas the definition of Σ-formulas for multi-algebraic theories is similar to the (recursive) definition of first-order $L(\Sigma)$-formulas:

Definition 1.1.8. *The formulas of Σ are defined as follows:*

i- Atomic formulas are the formulas of type $t \sqsubseteq t'$, where t, t' are terms.

ii- If ϕ, ψ are formulas, then $\neg\phi$ and $\phi \vee \psi, \phi \wedge \psi, \phi \to \psi, \phi \leftrightarrow \psi$ are formulas.

iii- If ϕ is a formula and x_i is a variable, then $\forall x_i \phi$, $\exists x_i \phi$ are formulas.

The notion of occurrence *(respectively free occurrence) of a variable in a formula is as the usual. We will denote $fv(\phi)$ as the (finite) set of variables that occurs free in the formula ϕ.*

We use $t_1 =_s t_2$ to abbreviate the formula $(t_1 \sqsubseteq t_2) \wedge (t_2 \sqsubseteq t_1)$: this means that t_1 and t_2 are "strongly equal terms".

Definition 1.1.9. *The definition of interpretation of formulas $\phi(\bar{x})$ where*

$$fv(\phi) \subseteq \bar{x} \subseteq \{x_i : i \in \mathbb{N}\}$$

under a valuation of variables $v : \bar{x} \to A$ (or we will denote simply by $v = \bar{a}$) is:

i- $A \models_v t(\bar{x}) \sqsubseteq t'(\bar{x})$ *iff* $t^A(\bar{a}) \subseteq t'^A(\bar{a})$

ii- The case of complex formulas (given by the connectives $\neg$, $\vee$, $\wedge$, $\to$, $\leftrightarrow$, and quantifiers $\forall, \exists$) is as satisfaction of first-order $L(\Sigma)$-formulas in $L(\Sigma)$-structure on a valuation v.

Remark 1.1.10.

i- The theory of multi-algebras entails that for each term t, and each strict *term t',*

$$t \sqsubseteq t' \text{ iff } t =_s t'.$$

ii- In [55] *contains a development of the identity theory for multialgebras, with another primitive notion: $t(\bar{x}) =_w t'(\bar{x})$; a Σ-multialgebra A satisfies the "weak identity" above iff there is some $\bar{a} \in A^{var(t)\cup var(t')}$ such that $t^A(\bar{a}) \cap t'^A(\bar{a}) \neq \emptyset$. This will not play any role in this work but is useful for applications of multi-algebraic semantics for complex logical systems (* [38]*).*

There are many ways of define morphism for multialgebras. Follow below our choice:

Definition 1.1.11. *Let A and B be multialgebras of signature $\Sigma = ((S_n)_{n\geq 0}, (M_n)_{n\geq 0})$ and $\varphi : A \to B$ be a function.*

*i - φ is a **partial morphism** if for every $n \geq 0$, every $\sigma \in S_n$ and every $a_1, ..., a_n \in A$, we have*

$$\varphi(\sigma^A(a_1, ..., a_n)) \subseteq \sigma^B(\varphi(a_1), ..., \varphi(a_n)).$$

*ii - φ is a **morphism** if for every $n \geq 0$, every $\sigma \in S_n \sqcup M_n$ and every $a_1, ..., a_n \in A$, we have*

$$\varphi(\sigma^A(a_1, ..., a_n)) \subseteq \sigma^B(\varphi(a_1), ..., \varphi(a_n)).$$

*iii - φ is a **strong morphism** if for every $n \geq 0$, every $\sigma \in S_n \sqcup M_n$ and every $a_1, ..., a_n \in A$, we have*

$$\varphi(\sigma^A(a_1, ..., a_n)) = \sigma^B(\varphi(a_1), ..., \varphi(a_n)).$$

`translation-rem`

Remark 1.1.12.

i - Let A, B be Σ-multialgebras. If B is a strict multilagebra *(i.e. $\sigma^B_n(\bar{b})$ is unitary subset of B, for each $\sigma \in \Sigma$ and each tuple $\bar{b}$ in B), then the morphisms $A \to B$ coincide with the strong morphisms $A \to B$.*

ii - There is a full and faithful concrete embedding of the category of ordinary algebraic structures over a signature Σ and homomorphisms into the category of Σ-multialgebras and (strong) morphisms: the image of this embedding is the class of strict multialgebras over Σ.

iii - The correspondence $\Sigma \mapsto L(\Sigma)$ induces a concrete *isomorphism between the category of Σ-multialgebras and the category of $L(\Sigma)$- first order structures satisfying suitable $\forall\exists$ axioms. It is ease to see that this correspondence induces a bijection between injective strong embedding of Σ-multialgebras and $L(\Sigma)$-monomorphisms of first-order structures.*

We finish this subsection with two illustrative examples of multialgebras derived from an algebraic structure and from a first-order structure.

Example 1.1.13. *Let $(R,+,\cdot,0,1)$ be a commutative ring with $1\neq 0$. Given $n\geq 1$, define an $(n+1)$-ary multioperation $*_n$ by the rule:*

$$d\in a_0 *_n a_1 *_n a_2 *_n \dots *_n a_n \Leftrightarrow \text{ there is some } t\in R \text{ such that}$$
$$d=a_0+a_1t+a_2t^2+\dots+a_nt^n.$$

*The idea here, is that $a_0 *_n a_1 *_n a_2 *_n \dots *_n a_n$ "analyze" the values taken in R by the polynomial $p(X)=a_0+a_1X+a_2X^2+\dots+a_nX^n\in R[X]$. $*_n$ will be called **The streching multialgebra of degree** n over R.*

`ordermulti`

Example 1.1.14. *Let $\mathcal{L}=\{0,1,+,\cdot,\leq\}$ the language of ordered fields. Consider $\mathbb{R}$ as an ordered field. We can look at the ordering relation as a multioperation of arity 1. In agreement with our notation, we have*

$$\leq(a):=\{x\in\mathbb{R}:a\leq x\}=[a,+\infty).$$

From now on, all multi-algebras considered in this work will contain only operations of arities $0,1,2$. They will have strict constants and strict unary operations; the binary operations maybe strict or multivalued.

1.2 Multigroups, Multirings and Multifields

Multigroups are a generalization of groups. We can think that a multigroup is a group with a multivalued operation:

`defn:multigroupI`

Definition 1.2.1. *A multigroup is a quadruple $(G,*,r,1)$, where G is a non-empty set, functions $*:G\times G\to\mathcal{P}(G)\setminus\{\emptyset\}$ and $r:G\to G$ 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 $x,y\in G$. The structure $(G,\cdot,1)$ is a **commutative multimonoid (with unity)** if satisfy M3 and M4 and the condition $a\in 1\cdot a$ for all $a\in G$.*

`mgmorph1`

Definition 1.2.2. *A **morphism** of multigroups is a function $f:G\to H$ between multigroups such that $f(1_G)=1_H$ and for all $a,b\in G$, $f(a*b)\subseteq f(a)*f(b)$. Of course, composition of morphisms is a morphism and the category of multigroups with their morphisms will be denoted by $MGrp$.*

There is another definition (due to Marshall in [47]) with a first order theoretic flavour.

defn:multigroupII

Definition 1.2.3 (Adapted from Definition 1.1 in [47]). *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 there exist* $p \in G$ *such that* $(u, v, p) \in \Pi$ *and* $(p, w, x) \in \Pi$ *then there exist* $q \in G$ *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 describes the same object, and that connection is established by the following Lemma:

Lemma:1.2

Lemma 1.2.4 (Lemma 1.3 of [47]). *For any multigroup* G *as in the second version 1.2.3, 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 there exist* $q \in G$ *such that* $(v, w, q) \in \Pi$ *and* $(u, q, x) \in \Pi$ *then there exist* $p \in G$ *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 - Since $i = i$, by II we have $(i, i, i) \in \Pi$. 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 $(\mathfrak{i}, x, y) \in \Pi$. Then

$$\begin{aligned}(\mathfrak{i}, x, y) \in \Pi &\overset{I}{\Rightarrow} (y, r(x), \mathfrak{i}) \in \Pi \overset{I}{\Rightarrow} (r(y), \mathfrak{i}, r(x)) \in \Pi \\ &\overset{I}{\Rightarrow} r(y) = r(x) \overset{(b)}{\Rightarrow} y = r(r(y)) = r(r(x)) = x.\end{aligned}$$

Conversely, suppose $x = y$. Then

$$\begin{aligned}x = y \Rightarrow r(x) = r(y) &\overset{II}{\Rightarrow} (r(y), \mathfrak{i}, r(x)) \in \Pi \\ &\overset{I+(b)}{\Rightarrow} (y, r(x), \mathfrak{i}) \in \Pi \overset{I}{\Rightarrow} (\mathfrak{i}, x, y) \in \Pi.\end{aligned}$$

e - Note that
$$(u,q,x)\in\Pi \overset{I}{\Rightarrow} (x,r(q),u)\in\Pi \overset{(c)}{\Rightarrow} (q,r(x),r(u))\in\Pi.$$
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 - Since $(b,r(b),\mathfrak{i})\in\Pi$ and $(a,\mathfrak{i},a)\in\Pi$, by (e), there exists $c\in G$ such that $(a,b,c)\in\Pi$ and $(c,r(b),a)\in\Pi$.

□

mgmorph2

Definition 1.2.5. *A* ***morphism*** *of multigroups (in the sense of Definition 1.2.3) is a function $f:G\to H$ between multigroups $(G,\Pi_G,r_G,\mathfrak{i}_G)$ and $(H,\Pi_H,r_H,\mathfrak{i}_H)$ such that $f(1_G)=f(1_H)$ and for all $a,b,c\in G$ if $(a,b,c)\in\Pi_G$ then $(f(a),f(b),f(c))\in\Pi_H$. Of course, composition of morphisms is a morphism and the category of multigroups with their morphisms will be denoted by $MGrp_{fol}$.* [1]

Theorem 1.2.6. *The categories $MGrp$ and $MGrp_{fol}$ are equivalent.*

Proof. Let $(G,*,r,1)$ be an object of $MGrp$. Define a multigroup $G_{fol}:=(G,\Pi_*,r,\mathfrak{i})$ taking $\mathfrak{i}=1$ and $\Pi_*=\{(a,b,c):c\in a*b\}$. The validity of axioms I,II, III (and IV) for G_{fol} are direct consequence of axioms i,ii, iii (and iv) for $(G,*,r,1)$, so G_{fol} is an object in $MGrp_{fol}$.

Conversely, let $(G,\Pi,r,\mathfrak{i})$ be an object in $MGrp_{fol}$. By 1.2.4(f), we have a well-defined function $*_\Pi:A\times A\to\mathcal{P}(A)\setminus\{\emptyset\}$, given by the rule
$$*_\Pi(a,b)=a*_\Pi b:=\{c\in G:(a,b,c)\in\Pi\}.$$
Let $G_M:=(G,*_\Pi,1)$ with $1=\mathfrak{i}$. Then, the validate of the axioms i,ii (and iv) for G_M 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 $q\in b*_\Pi c$. Since $(b,c,q)\in\Pi$ and $(a,q,x)\in\Pi$, by 1.2.4(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_M is an object in $MGrp$.

Using the above arguments, we have the equivalence of these categories witnessed by the functors $\mathcal{F}:MGrp\to MGrp_{fol}$ and $\mathcal{G}:MGrp_{fol}\to MGrp$ defined respectively on the objects by $\mathcal{F}(G)=G_{fol}$ and $\mathcal{G}(G)=G_M$; and on the morphisms $f\in MGrp(G,H)$ and $g:MGrp_{fol}(K,L)$ by $\mathcal{F}(f)=f$ and $\mathcal{G}(g)=g$. □

Now we deal with multirings.

defn:multiring

Definition 1.2.7 (Adapted from Definition 2.1 in [47])**.** *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:*

[1]Here the subscript "fol" is to indicate that we are thinking in the first order theory associated to multigroups.

i - $(R, +, -, 0)$ *is a commutative multigroup;*

ii - $(R, \cdot, 1)$ *is a monoid;*

iii - $a0 = 0$ *for all* $a \in R$*;*

iv - *If* $c \in a + b$*, then* $cd \in ad + bd$ *and* $dc \in da + db$*. Or equivalently,* $(a + b)d \subseteq ab + bd$ *and* $d(a + b) \subseteq da + db$*.*

v - *If the equalities holds, i.e,* $(a + b)d = ab + bd$ *and* $d(a + b) = da + db$*, we said that* R *is a* ***hyperring****.*

A multiring is commutative if $(R, \cdot, 1)$ *is a commutative monoid. A zero-divisor of a multiring* R *is a non-zero element* $a \in R$ *such that* $ab = 0$ *for another non-zero element* $b \in R$*. The multiring* 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.*

Remark 1.2.8. *It is straightforward to realize that every multifield* F *is in fact a hyperfield, i.e, for all* $a, b, d \in F$*,* $d(a + b) = da + db$*.*

ex:1.3

Example 1.2.9.

a - *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.*

b - *In the same way of item (a), every ring, domain and field is a multiring, multidomain and multifield respectively.*

c - $Q_2 = \{-1, 0, 1\}$[2] *is a multifield with the usual product and the multivalued sum defined by relations*

$$\begin{cases} 0 + x = x + 0 = x, \text{ for every } x \in Q_2 \\ 1 + 1 = 1, \ (-1) + (-1) = -1 \\ 1 + (-1) = (-1) + 1 = \{-1, 0, 1\} \end{cases}$$

d - *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 [41].*

Example 1.2.10 (Example 2.5 of [47])**.** *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 polynomial functions* $f : V \to \mathbb{R}$*. Define an equivalence relation* $\sim$ *on* A *by* $f \sim g$ *iff* $f(x)$ *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:*

$$\overline{x^2 + x^3} \in \overline{x}\overline{x} + \overline{x}\overline{1} \text{ but } \overline{x^2 + x^3} \notin \overline{x}(\overline{x} + \overline{1}),$$

and this not happen because $x^2 + x^3 > 0$ *and* $x(x + 1) < 0$ *for* x *near to* 0 *with* $x \neq 0$*.*

[2]According Marshall's notation in [47].

Example 1.2.11. *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 [58]. 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 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 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, $R_+ = \{x \in R : x \geq 0\}$.

`kaleid`

Example 1.2.12 (Kaleidoscope)**.** *Let $n \in \mathbb{N}$ and define $X_n = \{-n, ..., 0, ..., n\} \subseteq \mathbb{Z}$. We define the n-**kaleidoscope multiring** by $(X_n, +, \cdot, -, 0, 1)$, where $- : X_n \to X_n$ is restriction of the opposite map in$\mathbb{Z}$, $+ : X_n \times X_n \to \mathcal{P}(X_n) \setminus \{\emptyset\}$ is given by the rules:*

$$a+b = \begin{cases} \{a\}, & \text{if } b \neq -a \text{ and } |b| \leq |a| \\ \{b\}, & \text{if } b \neq -a \text{ and } |a| \leq |b| \\ \{-a, ..., 0, ..., a\} & \text{if } b = -a \end{cases},$$

and $\cdot : X_n \times X_n \to X_n$ is is given by the rules:

$$a \cdot b = \begin{cases} sgn(ab)\max\{|a|, |b|\} & \text{if } a, b \neq 0 \\ 0 & \text{if } a = 0 \text{ or } b = 0 \end{cases}.$$

. In this sense, $X_0 = \{0\}$ and $X_1 = \{-1, 0, 1\} = Q_2$. For X_2, we have the following "multioperation" table for the sum:

$+$	-2	-1	0	1	2
-2	$\{-2\}$	$\{-2\}$	$\{-2\}$	$\{-2\}$	$\{-2,-1,0,1,2\}$
-1	$\{-2\}$	$\{-1\}$	$\{-1\}$	$\{-1,0,1\}$	$\{2\}$
0	$\{-2\}$	$\{-1\}$	$\{0\}$	$\{1\}$	$\{2\}$
1	$\{-2\}$	$\{-1,0,1\}$	$\{1\}$	$\{1\}$	$\{2\}$
2	$\{-2,-1,0,1,2\}$	$\{2\}$	$\{2\}$	$\{2\}$	$\{2\}$

and the following operation table for the product:

$\cdot$	-2	-1	0	1	2
-2	2	2	0	-2	-2
-1	2	1	0	-1	-2
0	0	0	0	0	0
1	-2	-1	0	1	2
2	-2	-2	0	2	2

Clearly $(X_n, \cdot, 1)$ *is a commutative monoid and* $a \cdot 0 = 0$ *for all* $a \in X_n$.
Now, 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* $a, b \in X_n$.

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* $a + b = \{b\}$. *Hence* $d \in a + b$ *implies* $d = b$. *So* $b \in b - a = \{b\}$. *By symmetry, the same proof applies to the implication* $b \in d - a \Rightarrow d \in a + b$. *The case* $|b| = |a|$ *is immediate.*

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* $a \neq -b$, $b \neq -c$, *and* $|a| \leq |b| \leq |c|$,

$$(a + b) + c = a + (b + c) = \{c\}.$$

Similarly, $(a + b) + c = a + (b + c)$ *for the cases* $|a| \leq |c| \leq |b|$, $|b| \leq |a| \leq |c|$, $|b| \leq |c| \leq |a|$, $|c| \leq |a| \leq |b|$ *and* $|c| \leq |b| \leq |a|$ *(under the hypothesis* $a \neq -b$, $b \neq -c$*).*

Now let $a = -b$. *We want to prove that* $(a - a) + c = a + (-a + c)$. *If* $|a| \leq |c|$,

$$(a - a) + c = X_a + c = \{c\} \text{ and } a + (-a + c) = a + c = \{c\}.$$

If $|c| < |a|$, *then*

$$(a - a) + c = X_a + c = X_a \text{ and } a + (-a + c) = a - a = X_a$$

The case $b = -c$ *is analogous.*

iv - $d(a + b) \subseteq da + db$: *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.*

`H-multi`

Example 1.2.13 (H-multifield, Example 2.8 in [24])**.** *Let* $p \geq 1$ *be a prime integer and* $H_p := \{0, 1, ..., p - 1\} \subseteq \mathbb{N}$. *Now, define the binary multioperation and operation in* H_p *as follow:*

$$a + b = \begin{cases} H_p \text{ if } a = b,\ a, b \neq 0 \\ \{a, b\} \text{ if } a \neq b,\ a, b \neq 0 \\ \{a\} \text{ if } b = 0 \\ \{b\} \text{ if } a = 0 \end{cases}$$
$$a \cdot b = k \text{ where } 0 \leq k < p \text{ and } k \equiv ab \bmod p.$$

$(H_p, +, \cdot, -, 0, 1)$ *is a hyperfield such that for all* $a \in H_p$, $-a = a$. *In fact, these* H_p *is a kind of generalization of* K, *in the sense that* $H_2 = K$.

We have to treat sums with some care when we are working with multirings. In order to use the multivalued sum without danger, we define recursively for $n \geq 2$:

$$a_1 + ... + a_n := \bigcup_{d \in a_2 + ... + a_n} a_1 + d.$$

In particular, for a multiring A, with $a_1, ..., a_n \in A$ and $\sigma \in S_n$, we have

$$a_1 + a_2 + ... + a_n = a_{\sigma(1)} + a_{\sigma(2)} + ... + a_{\sigma(n)}.$$

We also use two conventions: if $Z, W \subseteq R$ and $x \in R$, $Z + W := \bigcup\{x + y : x \in Z, y \in W\}$ and $Z + x := Z + \{x\} = \bigcup\{z + x : z \in Z\}$. We work freely with the immediate consequences of these conventions. For example, from commutativity and associativity is immediate that for all $X, Y, Z \subseteq R$, $X + Y = Y + X$ and $(X + Y) + Z = Z + (X + Y)$. We return further to these conventions, in the general case of superfields (see for instance Lemma 3.1.5).

`Lemma:1.4`

Lemma 1.2.14. *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:

$$\begin{aligned}(ad + bd)d^{-1} \subseteq (ad)d^{-1} + (bd)d^{-1} = ad + bd \Rightarrow \\ ad + bd = [(ad + bd)d^{-1}]d \subseteq (a + b)d.\end{aligned}$$

□

Then every multifield is in fact a hyperfield, and we use "hyperfield" from now on since it is the prevailing terminology. Now we treat about morphism.

`defn:morphism`

Definition 1.2.15. *Let A and B multirings. A function $f : A \to B$ 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 - $f(1) = 1$.

The category of multirings with their morphisms will be denoted by $MRing$.

For multirings, there are types of morphisms that can be considered. Let $f : A \to B$ a multiring morphism.

- f is a **strong morphism** if for all $a, b, c \in A$, if $f(c) \in f(a) + f(b)$, then there exist $a', b', c' \in A$ with $f(a') = f(a), f(b') = f(b), f(c') = f(c)$ such that $c' \in a' + b'$.
- f is an **ideal morphism** if for all $a, b, c \in A$, if $f(c) \in f(a) + f(b)$, then exists $c' \in A$ with $f(c') = f(c)$ such that $c' \in a + b$. In other words, $f(a + b) = (f(a) + f(b)) \cap \mathrm{Im}(f)$.
- We say that f is a **full morphism** if it is a strong morphism for all $a, b \in A$ and all $d \in B$,

$$d \in f(a) + f(b) \Rightarrow \text{ exists } c \in a + b \text{ such that } d = f(c).$$

In other words, $f(a + b) = f(a) + f(b)$.

- We say that f is a **strong embedding** if f is injective and it is a strong morphism. In this case, A is a **submultiring** of B if $A \subseteq B$ and the canonical inclusion $\iota : A \hookrightarrow B$ is a strong embedding.

- We say that f is a **full embedding** if it is a strong embedding and a full morphism[3].

The different notions of morphisms are related by the following:

$$\text{Full Morphism} \Rightarrow \text{Ideal Morphism} \Rightarrow \text{Strong Morphism}$$

$$\text{Full Embedding} \Rightarrow \text{Strong Embedding} \Leftrightarrow \text{Ideal Embedding}$$

The category of hyperfields (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:

ex:2.1

Example 1.2.16.

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 1.2.9(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 $Kerf = \{0\}$. Also $\mathbb{R}/Kerf$ 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 1.2.9(b)) is not a multiring morphism.*

1.3 Commutative Multialgebra

In the sequel, we extend some terminology of commutative algebra from multirings and hyperfields that could appear throughout this text. Of course, we are not intend to exhaust the theme and for a more detailed exposition, we recommend H. Ribeiro's ph.D Thesis, [23] (in portuguese) or [24].

[3] There is no consensus on the definition "submultiring": here we do adopted one of intermediary strength that coincides with the notion of substructure in relational structures; in [47], submultiring means an inclusion of multirings that is strong *and* full.

defn:ideal

Definition 1.3.1 (Definition 2.11 of [24]). *An* ***ideal of a multiring*** *A is a non-empty subset of A such that $\mathfrak{a}+\mathfrak{a}\subseteq\mathfrak{a}$ and $A\mathfrak{a}=\mathfrak{a}$. 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 for all ideals $\mathfrak{a}$ with $\mathfrak{m}\subseteq\mathfrak{a}\subseteq A\Rightarrow$, then $\mathfrak{a}=\mathfrak{m}$ or $\mathfrak{a}=A$. We will denote $Spec(A)=\{\mathfrak{p}\subseteq A:\mathfrak{p}$ is a prime ideal$\}$.*

If $\mathfrak{a}$ is an ideal of A, note that $0\in\mathfrak{a}$ and $-\mathfrak{a}\subseteq\mathfrak{a}$. With the notion of ideal, we define some new multirings structures with the language of commutative algebra in mind:

terminology

Definition 1.3.2 (Definition 2.12 of [24]).

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 (component wise) way.*

b - *Let $\mathfrak{a}\subseteq A$ be an ideal. Elements of $A/\mathfrak{a}$ are cosets $\overline{a}=a+\mathfrak{a}$, $a\in A$. More explicitly,*

$$a\equiv b \ mod\ I \text{ if and only if } b\in\overline{a}, \text{ if and only if } (b-a)\cap\mathfrak{a}\neq\emptyset.$$

This is the multialgebra analogous of the usual congruence relation in commutative algebra. 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 multiplication on $A/\mathfrak{a}$ is defined by $\overline{a}\overline{b}=\overline{ab}$. Note that if $\overline{c}\in\overline{a}+\overline{b}$, then exists $c'\in a+b$ such that $\overline{c'}=\overline{c}$. The natural arrow $\pi:A\to A/\mathfrak{a}$ is a strong morphism and as in the ring case it is easily proved that given another multiring morphism $f:A\to B$ with $f(\mathfrak{a})=\{0\}$, there is a unique morphism $\overline{f}:A/\mathfrak{a}\to B$ such that $f=\overline{f}\circ\pi$.

c - *Let S be a multiplicative set in A. Elements of $S^{-1}A$ have the form a/s, $a\in A$, $s\in S$, $a/s=b/t$ if and only if $atu=bsu$ 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 $c/v\in a/s+b/t$ if and only if $cstv\in atuv+bsuv$ for some $v\in S$. The natural arrow $\rho\colon A\hookrightarrow S^{-1}A$ is a strong morphism and given a multirng morphism $f\colon A\to B$ with $f(S)\subseteq B^{\times}$, then exists a unique morphism $\overline{f}\colon S^{-1}A\to B$ such that $f=\overline{f}\circ\rho$.*

d - *If D is a multidomain, we define the multifield of fractions $ff(D):=(D\setminus\{0\})^{-1}D$.*

Let X be a subset of a multiring A. We define the **ideal generated by** X by

$$\langle X\rangle:=\bigcap\{\mathfrak{a}\subseteq A:X\subseteq\mathfrak{a},\mathfrak{a}\ \text{ is an ideal}\}.$$

If $X\neq\emptyset$, we have that $\langle X\rangle=\bigcup\{\lambda_1x_1+\cdots+\lambda_nx_n\colon n\geq 1,\lambda_i\in A,x_i\in X,\ \text{for all } i=1,\dots,n\}$. In particular

$$\langle a\rangle=\sum Aa:=\left\{\sum_{j=1}^{n}\lambda_ja:\lambda_1,...,\lambda_n\in A,\ n\geq 1.\right\}.$$

If A is a hyperring then $\sum Aa=Aa$.

lem:iso

Proposition 1.3.3 (Proposition 2.13 of [24]). *Let A and B be multirings and $\varphi:A\to B$ a surjective morphism. Consider $\overline{\varphi}:A/Ker(\varphi)\to B$ the induced morphism. Then the following are equivalent:*

i- φ is a strong morphism and if $\varphi(a)=\varphi(a')$ for $a,a'\in A$, then $(a-a')\cap ker(\varphi)\neq\emptyset$.

ii- φ is an ideal morphism.

iii- $\overline{\varphi}$ *is an isomorphism.*

Proof. $i) \Rightarrow ii)$: Assume that $\varphi(a) \in \varphi(b)+\varphi(c)$. Since φ is a strong morphism, exists $a', b', c' \in A$ with $\varphi(a') = \varphi(a), \varphi(b') = \varphi(b), \varphi(c') = \varphi(c)$ such that $a' \in b'+c'$. By hypothesis, exists $b' \in b+i$ and $c' \in c+j$ such that $i, j \in \ker(\varphi)$. Then $a' \in b'+c' \subseteq (b+c)+(i+j)$ and so exists $x \in i+j \subseteq \ker(\varphi)$ such that $a' \in b+c+x$. Thus exist $a'' \in a'-x$ with $a'' \in b+c$ and note that $\varphi(a'') = \varphi(a') = \varphi(a)$.

$ii) \Rightarrow iii)$: Let $a, b \in A$ such that $\varphi(a) = \overline{\varphi}(\overline{a}) = \overline{\varphi}(\overline{b}) = \varphi(b)$. By hypothesis exist $x \in a-b$ such that $x \in \ker(\varphi)$ and so $\overline{a} = \overline{b}$ in $A/\ker(\varphi)$, proving the injectivity of $\overline{\varphi}$. Since φ is a strong morphism, if $\overline{\varphi}(\overline{a}) \in \overline{\varphi}(\overline{b}) + \overline{\varphi}(\overline{c})$, then exists $a', b', c' \in A$ with $\varphi(a') = \varphi(a), \varphi(b') = \varphi(b), \varphi(c') = \varphi(c)$ such that $a' \in b'+c'$. By hypothesis, it is easy to see that $\overline{a'} = \overline{a}, \overline{b'} = \overline{b}, \overline{c'} = \overline{c}$ and so $\overline{a} \in \overline{b}+\overline{c}$ in $A/\ker(\varphi)$. Thus $\overline{\varphi}$ is an isomorphism.

$iii) \Rightarrow i)$: Assume that $\varphi(a) = \varphi(a')$ for $a, a' \in A$. Then $\overline{\varphi}(\overline{a}) = \overline{\varphi}(\overline{a}')$ and hence $\overline{a} = \overline{a'}$, which means that $(a-a') \cap \ker(\varphi) \neq \emptyset$. Therefore $0 = \varphi(0) \in \varphi(a) - \varphi(a')$, and by hypothesis there exist $i \in a-a'$ such that $\varphi(i) = \varphi(0) = 0$. On the other hand, we have $\varphi = \overline{\varphi} \circ \pi$, where $\pi\colon A \to A/\ker(\varphi)$. Then φ is a composition of strong morphisms and so φ is strong itself. □

teo:iso

Theorem 1.3.4 (Isomorphism Theorem, 2.14 of [24])**.** *Let A and B be multirings and $\varphi : A \to B$ an ideal morphism. Then $Im(\varphi)$ is a multiring (contained in B) with the structure induced by the domain A, and the induced morphism $\overline{\varphi} : A/Ker(\varphi) \to Im(\varphi)$ is an isomorphism.*

Proof. By the previous Proposition, it is enough to prove that $\mathrm{Im}(\varphi)$ is a multiring and this is accomplished by proving the associativity property for $\mathrm{Im}(\varphi)$. Assume that $\varphi(x) \in \varphi(p)+\varphi(w)$ with $\varphi(p) \in \varphi(u)+\varphi(v)$. Since φ is an ideal morphism, exists $x' \in p+w$ and $p' \in u+v$ such that $\varphi(x') = \varphi(x)$ and $\varphi(p') = \varphi(p)$. Then, by the same argument as the previous Lemma, it should exist $i \in \mathrm{Ker}(\varphi)$ such that $p \in i+p'$. Then $p \in i+(u+v) \subseteq (i+u)+v$ and thus exist $u' \in i+u$ such that $p \in u'+v$. Then exist $q \in v+w$ with $x \in u'+q$. Thus $\varphi(x) \in \varphi(u')+\varphi(q) = \varphi(u)+\varphi(q)$ and $\varphi(q) \in \varphi(v)+\varphi(w)$. □

Lemma:1.1

Lemma 1.3.5 (Lemma 2.16 of [24])**.** *Let A be a multiring. Then:*

a - *an ideal $\mathfrak{p}$ of A is prime if and only if $A/\mathfrak{p}$ is a multidomain.*

b - *An ideal $\mathfrak{m}$ is maximal if and only if for all $a \neq 0$ in $A/\mathfrak{m}$, exists $t_1, \ldots, t_n$ such that*

$$1 \in at_1 + \cdots + at_n.$$

In particular, maximal ideals are prime and if A is a hyperring, an ideal $\mathfrak{m}$ is maximal if and only if $A/\mathfrak{m}$ is a multifield.

Proof.

a - The same of the ring case.

b - $\Rightarrow$: Let $\overline{a} \in A/\mathfrak{m}$ non-zero, that is, $a \notin \mathfrak{m}$. Since m is maximal, the ideal generated by $\mathfrak{m} \cup \{a\}$, namely

$$I = \bigcup \{m + at_1 + \cdots + at_n \colon n \geq 1 \text{ and } t_i \in A\},$$

is improper. Then exists $m \in \mathfrak{m}$ and $t_1, \cdots, t_n \in A$ such that $1 \in m + at_1 + \cdots + at_n$ and so $\overline{1} \in \overline{a}\overline{t_1} + \cdots + \overline{a}\overline{t_n}$.

$\Leftarrow$: Let $a \notin \mathfrak{m}$. By the property valid in $A/\mathfrak{m}$, exists $m \in \mathfrak{m}$ and $t_1, \cdots, t_n \in A$ such that $1 \in m + at_1 + \cdots + at_n$ and so the ideal generated by $\mathfrak{m} \cup \{a\}$ is improper. Then $\mathfrak{m}$ is maximal.

□

Proposition 1.3.6 (Proposition 2.17 of [24]).

a - *Let A be a multiring, $I \subseteq A$ an ideal and $S \subseteq A$ be a multiplicative subset of A. Then $(S/I)^{-1}A/I \cong S^{-1}A/S^{-1}I$.*

b - *Let $\{A_i\}_{i\in I}$ be a family of multirings and $\mathfrak{a}_i \subseteq A_i$ be an ideal of A_i for every $i \in I$. Then*

$$\prod_{i\in I} A_i/\mathfrak{a}_i \cong \prod_{i\in I} A_i/\prod_{i\in I}\mathfrak{a}_i.$$

Proof. For the item (a), consider the morphism $f : S^{-1}A \to (S/I)^{-1}A/I$ given by $f(a/s) = \overline{a}/\overline{s}$ and apply the Theorem 1.3.4. For the item (b), the same strategy holds with the morphism $g : \prod_{i\in I} A_i \to \prod_{i\in I} A_i/\prod_{i\in I}\mathfrak{a}_i$ given by $g(a_i)_{i\in I} = (\overline{a}_i)_{i\in I}$. □

Now, we present the main construction related to quadratic forms, that we baptize "Marshall's quotient". This kind of quotient appears naturally in the context of abstract theories of quadratic forms, as we will have the opportunity to see later in the text.

defn:strangeloc

Definition 1.3.7 (Example 2.6 of [47]). *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 $A/_mS = \{\overline{a} : a \in A\}$. Defining $-\overline{a} = \overline{-a}$, $\overline{a}\overline{b} = \overline{ab}$ and*

$$\overline{a} + \overline{b} = \{\overline{c} : cv \in as + bt, \text{ for some } s, t, v \in S\},$$

*we have that $(A/_mS, +, \cdot, -, \overline{0}, \overline{1})$ is a multiring, called **the Marshall's quotient** of A by S.*

Let S be a non-empty subset of a multiring A. We define the **ideal generated by** S by $\langle S\rangle := \bigcap\{\mathfrak{a} \subseteq A \text{ ideal} : S \subseteq \mathfrak{a}\}$. If $S = \{a_1, ..., a_n\}$, we have 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 is a hyperring, then $\sum Aa = Aa$.

Proposition 1.3.8 (Proposition 2.19 of [24]). *Let A, B be a multiring and $S \subseteq A$ a multiplicative subset of A. Then for every morphism $f : A \to B$ such that $f[S] = \{1\}$, there exist a unique morphism $\tilde{f} : A/_mS \to B$ such that the following diagram commute:*

$$\begin{tikzcd} A \arrow[r, "\pi"] \arrow[dr, "f"'] & A/_mS \arrow[d, "!\tilde{f}"] \\ & B \end{tikzcd}$$

where $\pi : A \to A/_mS$ is the canonical projection $\pi(a) = \overline{a}$.

Proposition 1.3.9 (Proposition 2.20 of [24]). *Let A be a multiring, $I \subseteq A$ an ideal and $S \subseteq A$ a multiplicative subset such that $I \subseteq S$. Define $S/I = \{\overline{s} : s \in S\}$ (modulo I). Then*

$$(A/I)/_m(S/I) \cong A/_mS.$$

Proof. Define $\Phi : A/I \to A/_mS$ given by $\Phi(\overline{a}^I) = \overline{a}^S$ and use the previous Proposition. □

Proposition 1.3.10 (Proposition 2.21 of [24]). *Let A be a multiring and $P, S \subseteq A$ multiplicative subsets of A such that $P \subseteq S$. Then*

$$A/_m S \cong P^{-1}A/_m P^{-1}S.$$

1.4 Ordering Structures and Artin-Schreier Theorem

`defn:mfordering`

Definition 1.4.1 (Page 8 of [47]). *Let F be a hyperfield. 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 hyperfield F, denoted $Sper(F)$, is defined to be the set of all orderings of F.*

`defn:mfpreordering`

Definition 1.4.2 (Page 8 of [47]). *A preordering of a hyperfield 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 hyperfield 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 $-1 \notin T$.*

`lem:3.2marshall`

Lemma 1.4.3 (Lemma 3.2 of [47]). *Suppose F is a hyperfield 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 $a = (a/u)u \in T$. □

`lem:3.3marshall`

Lemma 1.4.4 (Lemma 3.3 of [47]).

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 hyperfield 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 denote by X_T the set of all orderings of F with $T \subseteq F$.

`prop:3.4marshall`

Proposition 1.4.5 (Generalized Artin-Schreier Theorem (Proposition 3.4 of [47])). *Let F be an hyperfield 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 1.4.4). By the Zorn's Lemma, there exists a maximal and proper preordering P such that $T - aT \subseteq P$. By 1.4.4, P is an ordering, and $-a \in P$, so $a \notin P$. $\square$

1.5 Real Reduced hyperfields

Consider the hyperfield Q_2. $\{0,1\}$ is an ordering on Q_2. For any ordering P on a hyperfield F, $Q_P(F) = F/mP \cong Q_2$ by a unique isomorphism. Orderings of a hyperfield F correspond bijectively to a multiring homomorphism $\sigma : F \to Q_2$ via $P = \sigma^{-1}(\{0,1\})$.

prop:4.1marshall

Proposition 1.5.1 (Proposition 4.1 of [47]). *For a real hyperfield 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)$\Leftrightarrow$(b) Is just the general fact that if $\sigma : F \to K$ is a morphism of real hyperfields, then $\sigma\left(\sum F^2\right) \subseteq \sum K^2$ and that $\sum Q_{red}(F)^2 = \{0,1\}$.

(a)$\Rightarrow$(c) $Q_{red}(F)$ already satisfy $a^3 = a$ for all a and $1+1 = \{1\}$.

(c)$\Rightarrow$(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 $\sum F^2 = F^2 = \{0,1\}$. $\square$

defn:mfrealreduced

Definition 1.5.2. *A hyperfield F is said to be real reduced if satisfies the equivalent conditions of Proposition 1.5.1.*

A morphism of real reduced hyperfield is just a morphism of hyperfields. The category of real reduced hyperfields will be denoted by $\mathcal{MF}_{red}$.

cor:4.2marshall

Corollary 1.5.3 (Corollary 4.2 of [47]). *A hyperfield 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. ($\Rightarrow$) is already done. For ($\Leftarrow$), by Proposition 1.5.1 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. $\square$

For any proper preordering T of a real reduced hyperfield F, $Q_T(F)$ is a real reduced hyperfield. In particular, $Q_{red}(F)$ is a real reduced hyperfield. If $p : F_1 \to F_2$ is a multiring homomorphism of real hyperfields, 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 hyperfields onto the subcategory of real reduced hyperfields.

lem:4.3marshall

Proposition 1.5.4 (Lemma 4.3 of [47]). *Let F be a real reduced hyperfield, $T = \sum F^2$. For any $a, b \in \dot{F}$,*

$$(a+b)^* = (Ta+Tb)^* = \{c \in \dot{F} : \forall\, \sigma \in Sper(F),\ \sigma(c) = \sigma(a),\ or\ \sigma(c) = \sigma(b)\}.$$

Proof. Since F is a real reduced hyperfield, $T = \{0, 1\}$, 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 remains 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 1.4.5, $c/a \in T + T(b/a)$. Multiplying by a, this yields $c \in Ta + Tb$ as required. □

Real reduced hyperfields have a natural representation in terms of functions:

cor:4.4marshall

Theorem 1.5.5 (Local-Global principle, Corollary 4.4 of [47]). *For any real reduced hyperfield F, the natural embedding $F \hookrightarrow Q_2^{Sper(F)}$ is a strong embedding.*

Proof. Let F be a real reduced hyperfield and $T = \sum F^2 = \{0, 1\}$. By Proposition 1.4.5,

$$\{0, 1\} = \bigcap_{P\in X_T} P,$$

or 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 remains 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 1.5.4. □

In particular, for any real reduced hyperfield, $\mathrm{Sper}(F)$ separate points of F and $c \in a + b \subseteq F$ if and only if, for every $\sigma : F \to Q_2$, $\sigma(c) \in \sigma(a) + \sigma(b)$.

1.6 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.

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 *semi real* 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 $T \subseteq M$).

prop:5.2marshall

Proposition 1.6.1 (Proposition 5.2 of [47]). *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 $a\left(\sum aT\right) \subseteq T$, this yields $-a^2 \in M + t_1a - a^2$ and $-a^2 \in M - t_2a$, for some $t_1, t_2 \in T$. Then $-t_1a \in a^2 + M \subseteq M$, and $t_2a \in a^2 + M \subseteq M$, so $t_1t_2a \in \mathfrak{p}$. 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 $A = M \cup -M$. □

cor:5.3marshall

Corollary 1.6.2 (Corollary 5.3 of [47]). *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 1.6.1 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 $\sigma \in X_T$.

prop:5.4marshall

Proposition 1.6.3 (Proposition 5.4 of [47]). *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* $-d^{2k} \in T + \sum A^2c$ *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 $T + \sum A^2c$ and the T'-module $T' + \sum B^2c$. If $-S \cap (T + \sum A^2c) = \emptyset$, then $-1 \notin T' + \sum B^2c$, so there is a T'-module M in B containing $T' + \sum B^2c$ and maximal subject to $-1 \notin M$. By Proposition 1.6.1, $\mathfrak{p} := M \cap -M$ 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 hyperfield $F := ff(A/\mathfrak{p})$. 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 1.4.5, 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 $-st = s^2c \in \sum B^2c \subseteq M$, 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 $-d^{2k} \in T + \sum A^2c$, 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 $\sigma \in X_T$. □

cor:5.5marshall

Corollary 1.6.4 (Corollary 5.5 of [47]).

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 1.6.3 as follows: (a) take $c = 0$, $d = a$. (b) Take $c = -a$, $d = 1$. (c) Take $c = -a$, $d = a$. (d) Take $c = -bc$, $d = a$. □

1.7 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.

prop:6.1marshall

Proposition 1.7.1 (Proposition 6.1 of [47]). *For a prime ideal $\mathfrak{p}$ in a multiring A, the following are equivalent:*

a - $\mathfrak{p}$ is real.

b - The residue hyperfield $ff(A/\mathfrak{p})$ 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 1.4.4, $ff(A/\mathfrak{p})$ 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 $\sum A^2$. □

defn:multirealradical

Definition 1.7.2. *The real radical of an ideal $\mathfrak{a}$ in A is*

$$\sqrt[R]{\mathfrak{a}} := \left\{ a \in A : \exists\, b_i \in A \text{ and } k \geq 0 \text{ such that } \left(a^{2k} + \sum b_i^2\right) \cap \mathfrak{a} \neq \emptyset \right\}.$$

prop:6.2marshall

Proposition 1.7.3 (Proposition 6.2 of [47]). *$\sqrt[R]{\mathfrak{a}}$ 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 1.6.4(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 1.6.4(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 $a \in \sqrt[R]{\mathfrak{a}}$. □

prop:6.3marshall

Proposition 1.7.4 (Proposition 6.3 of [47]). *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 1.7.3. 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 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 $a \notin \mathfrak{q}$. □

defn:multiringreal

Definition 1.7.5. *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.

1.8 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:

defn:multivalue

Definition 1.8.1. *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 $\overline{b} \in D(\phi)$.

lem:7.1marshall

Lemma 1.8.2 (Lemma 7.1 of [47])**.**

i - $D(\overline{a}) = \{\overline{b}^2\overline{a} : b \in A\} = \{\overline{t}\overline{a} : t \in A,\ \overline{t} \geq 0\} =$
$\{\overline{b} :$ *for each* $\sigma \in X_T$ *either* $\overline{b}(\sigma) = 0$ *or* $\overline{a}(\sigma)\overline{b}(\sigma) > 0\}$.

ii - $D(\overline{a}, \overline{b}) = \{\overline{c} :$ *for each* $\sigma \in X_T$, *either* $\overline{c}(\sigma) = 0$ *or* $\overline{a}(\sigma)\overline{c}(\sigma) > 0$ *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 $\sigma \in X_T$, $\overline{c}(\sigma) = 0$ or 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 1.6.4(b),

$$-1\in T'-\sum T'a'-\sum A'^2b'.$$

Multiplying by c^{2m+1}, m sufficiently large, $-c^{2m+1}\in Tc-\sum Ta-\sum Tb$. This yields

$$c_1\in\left(\sum Ta+\sum Tb\right)\cap(c^{2m+1}+Tc).$$

It follows that $\overline{c}=\overline{c}_1\in D(\overline{a},\overline{b})$.

iii - This follows 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).

□

lem:7.2marshall

Lemma 1.8.3 (Lemma 7.2 of [47])**.** *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 1.8.2(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 $\overline{0}$.

prop:7.3marshall

Proposition 1.8.4 (Local-Global principle, Proposition 7.3 of [47])**.** *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 1.8.3, 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 1.8.3, $\overline{c} \in \overline{a}+\overline{b}$ 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 1.8.2(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:

cor:7.4marshall

Corollary 1.8.5 (Corollary 7.4 of [47]). *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 1.8.2 and (ii) is direct consequence of 1.8.3. □

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.

prop:7.5marshall

Proposition 1.8.6 (Proposition 7.5 of [47]). *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 $-c^{2k} \in A^2 - \sum A^2 ab$. Since $c^3 = c$, $c^{2k} = c^2$. Thus, there exists $d \in \sum A^2 ab$ with $d \in c^2 + A^2$. Hence

$$ac \in a(a^2+b^2) \subseteq a^3+ab^2 = a+ab^2 = a,$$

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 $ab = abd \in \sum e_i^2a^2b^2 \subseteq A^2$. This implies $ab \in A^2$, so $ab = a^2b^2$. Thus, $a^2 = a^2d \in \sum e_i^2a^3b = \sum e_i^2ab = \sum e_i^2a^2b^2$ and, similarly, $b^2 \in \sum e_i^2a^2b^2$. Since $\sum e_i^2a^2b^2$ 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. □

defn:mrrealreduced

Definition 1.8.7. *A multiring satisfying* $-1 \notin \sum A^2$ *and the equivalent conditions of Proposition 1.8.6 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* $\mathcal{MR}_{red}$.

cor:7.6marshall

Corollary 1.8.8 (Corollary 7.6 of [47])**.** *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 1.8.6 to conclude that A is a real reduced multiring. The converse is immediate. □

Chapter 2

Hyperfields, Special Groups and Quadratic Forms

There are many of abstract theories of quadratic forms. The first ones (abstract Witt rings, quaternionic structures and Cordes schemes [46]) have appeared in the late 70s, by the hands of M. Marshall and C. M. Cordes, with the following central target: analyze the existence (or not) of fields with certain properties relating to quadratic forms. In the decade of 80's, appears the Marshall's abstract space of orderings (AOS) [48]: they are important because generalize both theory of orderings on fields and the reduced theory of quadratic forms. But only in the early 90's that arise a (finitary) first-order theory that generalizes the reduced and non-reduced theory of quadratic forms simultaneously. This theory is the special groups of F. Miraglia and M. Dickmann [28]. At that moment, the focus was to look at generalizations for the theory of quadratic forms with invertibles coefficients (fields, von Neumman rings, semi-local rings..., in general, rings with a good amount of invertibles). In the mid 90's, Marshall generalizes the abstract ordering spaces to rings, and called his new theory by "abstract real spectra" (ARS), in a first attempt to develop a theory of quadratic forms over (general) coefficients on rings. The ring-theoretic case is much more difficult to deal than the field one, the isometry is not well behaved and an algebraic counterpart of the abstract real spectra just appears in years 2000, with the real semigroups (RS) of Dickmann and Petrovich.

Following the work of professors F. Miraglia and M. Dickmann, through a fruitful and successful partnership between IME-USP and IMJ-PRG (Paris 6,7), which began in the 1990s, the three authors of this paper continue to expand the boundaries of abstract theories of quadratic forms, carrying forward the ideas of Dickmann-Miraglia's works, making the IME-USP a center for the development of such theories.

All those abstract theories constitute categories that are equivalent, or dually equivalent to full subcategories of each other. Also, each one has a particular motivation and advantage. In particular, some of them are categories of first-order theories and the corresponding language homomorphisms, thus allowing the application of model-theoretical notions and methods in this subject of algebra.

In [28], [32] and [33] are considered special groups and real semigroups. The former treats simultaneously reduced and non-reduced theories but focuses on rings with a good amount of invertible coefficients to quadratic forms. The latter has the advantage of potentially consider general coefficients of a ring, but only addresses the reduced case. Both are first-order theory, thus they allow the use of model theoretic methods.

M. Marshall in [47] introduced an approach to (reduced) theory of quadratic forms trough the concept of multiring: this seems more intuitive for an algebraist, encompassing some techniques of ordinary commutative algebra, encodes copies of special groups and real semigroups (see [24]), but still allows the use of model-theoretic tools.

In this Chapter we study the relations between special groups, real semigroups and multivalued structures. The main results are Theorem 2.3.4, 2.3.7, 2.3.10 and 2.5.4, which characterize precisely the necessary conditions for a hyperfield/multiring come from a special group/real semigroup. Proposition 2.4.3 deals with a question posed by the authors of [37]. We also got a new and interesting Example of real semigroup (2.5.15): $A/_mT$ for $A = \mathcal{C}(X,\mathbb{R})$ and $T = A^2 \cap \mathrm{nzd}(A)$, where X is a T_6 topological space.

2.1 Special Groups

extrel

Definition 2.1.1 (Extension of a Relation). *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 $n \geq 1$, as follows:*

i - $\equiv_1$ *is the diagonal relation* $\Delta_A \subseteq A \times A$

ii - $\equiv_2 = \equiv$.

iii - if $n \geq 3$, $\langle a_1,...,a_n\rangle \equiv_n \langle b_1,...,b_n\rangle$ *if and only there are* $x, y, z_3, ..., z_n \in A$ *such that*

$$\begin{aligned}&\langle a_1, x\rangle \equiv \langle b_1, y\rangle\\&\langle a_2,...,a_n\rangle \equiv_{n-1} \langle x, z_3,...,z_n\rangle \text{ and}\\&\langle b_2,...,b_n\rangle \equiv_{n-1} \langle y, z_3,...,z_n\rangle\end{aligned}$$

Whenever clear from the context, we frequently abuse notation and indicate the aforedescribed extension $\equiv$ by the same symbol.

defn:sg

Definition 2.1.2 (Special Group, 1.2 of [28]). *A* ***special group*** *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 (as in 2.1.1) is a transitive relation.*

A group of exponent 2, with a distinguished element -1, satisfying the axioms SG0-SG3 and SG5 is called a **proto special group**; a **pre special group** is a proto special group that also satisfies SG4. Thus a **special group** is a pre-special group that satisfies SG6 (or, equivalently, for each $n \geq 1$, $\equiv_n$ is an equivalence relation on G^n.)

A n-**form** (or form of dimension $n \geq 1$) is an n-tuple of elements of a pre-special group G. An element $b \in G$ is **represented** on G by the form $\varphi = \langle a_1, ..., a_n\rangle$, in symbols $b \in D_G(\varphi)$, if there exists $b_2, ..., b_n \in G$ such that $\langle b, b_2, ..., b_n\rangle \equiv \varphi$.

A pre-special group (or special group) $(G, -1, \equiv)$ is:
- **formally real** if $-1 \notin \bigcup_{n\in\mathbb{N}} D_G(n\langle 1\rangle)$;
- **reduced** if it is formally real and, for each $a \in G$, $a \in D_G(\langle 1, 1\rangle)$ iff $a = 1$.

Now, some examples:

ex2.2

Example 2.1.3 (The trivial special relation, 1.9 of [28])**.** *Let G be a group of exponent 2 and take -1 as any element of G different of 1. For $a, b, c, d \in G$, define $\langle a, b\rangle \equiv_t \langle c, d\rangle$ if and only if $ab = cd$. Then $G_t = (G, \equiv_t, -1)$ is a special group ([28]). In particular $2 = \{-1, 1\}$ is a reduced special group.*

ex2.3

Example 2.1.4 (Special group of a field, Theorem 1.32 of [28])**.** *For F be a field, denote $\dot{F} = F\backslash\{0\}$, $\dot{F}^2 = \{x^2 : x \in \dot{F}\}$ and $\Sigma\dot{F}^2 = \{\sum_{i\in I} x_i^2 : I$ is finite and $x_i \in \dot{F}^2\}$. Let $G(F) = \dot{F}/\dot{F}^2$. In the case of F is be formally real, we have $\Sigma\dot{F}^2$ is a subgroup of $\dot{F}$, then we take $G_{red}(F) = \dot{F}/\Sigma\dot{F}^2$. Note that $G(F)$ and $G_{red}(F)$ are groups of exponent 2. In [28] they prove that $G(F)$ and $G_{red}(F)$ are special groups with the special relation given by usual notion of isometry (see for instance, [43]), and $G_{red}(F)$ is always reduced.*

defnmorph

Definition 2.1.5 (1.1 of [28])**.** *A map $(G, \equiv_G, -1) \xrightarrow{f} (H, \equiv_H, -1)$ between pre-special groups is a **morphism of pre-special groups or PSG-morphism** if $f : G \to H$ is a homomorphism of groups, $f(-1) = -1$ and for all $a, b, c, d \in G$*

$$\langle a, b\rangle \equiv_G \langle c, d\rangle \Rightarrow \langle f(a), f(b)\rangle \equiv_H \langle f(c), f(d)\rangle$$

*A **morphism of special groups or SG-morphism** is a pSG-morphism between the correspondents pre-special groups. f will be an isomorphism if is bijective and f, f^{-1} are PSG-morphisms.*

It can be verified that a special group G is formally real iff it admits some SG-morphism $f : G \to 2$.

The category of special groups (respectively reduced special groups) and theirs morphisms will be denoted by SG (respectively RSG). Now, we will analyze the connections between the SG and MF. For this, we need more results about special groups and their characterization. For this, we use the results proved in Lira's thesis [22]. Consider these axioms concerns about a group of exponent 2 with a distinguished element:

SG 7 $\forall a\, \forall a'\, \forall x\, \forall t\, \forall t'\, \forall y[(a, a') \equiv (x, t) \wedge (t, t') \equiv (1, y)]$
$\Rightarrow \exists a''\, \exists s\, \exists s'[(a, a'') \equiv (y, s) \wedge (s, s') \equiv (1, x)]$.

An equivalent statement for SG7 is

$$\bigcup_{t\in D_G(1,y)} D_G(x, t) = \bigcup_{s\in D_G(1,x)} D_G(y, s)$$

for all $x, y \in G$.

SG 8 For all forms $f_1, ..., f_n$ of dimension 3 and for all $a, a_2, a_3, b_2, b_3 \in G$,

$$\langle a, a_2, a_3\rangle \equiv f_1 \equiv ... \equiv f_n \equiv \langle a, b_2, b_3\rangle \Rightarrow \langle a_2, a_3\rangle \equiv \langle b_2, b_3\rangle.$$

SG 9 $\forall a \forall b \forall c \forall d[\langle a,b,ab\rangle \equiv \langle c,d,cd\rangle \Rightarrow \langle a,b,ab\rangle \equiv \langle d,c,cd\rangle]$

sg6moreasy

Proposition 2.1.6 (A. de Lima, [22]). *Let $(G,-1,\equiv)$ be a pre-special group. The following are equivalent:*

i - $G \models SG6$

ii - $G \models SG7 \wedge SG8$

iii - $G \models SG9$

1.23chico

Theorem 2.1.7. *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 $b_1, b_2, b_3 \in G$,

$$\varphi \equiv \langle b_1,b_2,b_3\rangle \text{ implies } \varphi \equiv \langle b_2,b_1,b_3\rangle.$$

1.24chico

Corollary 2.1.8. *Let $(G,\equiv,-1)$ be a pre-special group, 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 $a,b,c,x,y \in G$

$$\varphi \equiv \langle a,b,c\rangle \text{ and } \langle a,b\rangle \equiv \langle x,y\rangle \Rightarrow \varphi \equiv \langle x,y,c\rangle.$$

2.3chico

Definition 2.1.9 (2.3 of [28]). *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.

2.4chico

Lemma 2.1.10 (2.4 of [28]). *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, $D_G(\varphi) \subseteq \Delta$.

2.2 Special Hyperfields

`sg.to.mf`

Proposition 2.2.1. *Let $(G, \equiv, -1)$ be a special group and $M(G) := G \cup \{0\}$ where $0 := \{G\}$. Then $(M(G), +, -, \cdot, 0, 1)$ with operations*

- $a \cdot b = \begin{cases} 0 \textit{ if } a = 0 \textit{ or } b = 0 \\ a \cdot b \textit{ otherwise} \end{cases}$
- $-(a) = (-1) \cdot a$
- $a + b = \begin{cases} \{b\} \textit{ if } a = 0 \\ \{a\} \textit{ if } b = 0 \\ M(G) \textit{ if } a = -b, \textit{ and } a \neq 0 \\ D_G(a, b) \textit{ otherwise} \end{cases}$

is a hyperfield.

Proof. Firstly, note that $+$ is well-defined. Then, we verify the conditions of Definition 1.2.7:

i - For this, we check the conditions of definition 1.2.1.

a - $d \in a + 0 = \{a\}$ imply $d = a$, and then $a \in d + (-0)$ 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 an immediate 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 $a \neq -b$. Since $D_G(a, b) = D_G(b, a)$, we have $a + b = b + a$ proving the commutativity. 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 $a = -c$.

$$(a + b) + (-a) = \bigcup \{g + (-a) : g \in a + b\} = M(G)\,(\mathrm{I})$$

because $a \in a+b$, and

$$a+(b+(-a)) = \bigcup\{a+h : h \in b+(-a)\} = M(G)\,(\mathrm{II})$$

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

$$(a+(-a))+c = \bigcup\{g+c : g \in M(G)\} = M(G)\,(\mathrm{III})$$

and

$$a+((-a)+c) = \bigcup\{a+h : h \in (-a)+c\} = M(G)\,(\mathrm{IV})$$

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 $a \neq -c$.

$$(a+b)+c = c+(a+b) = \bigcup\{c+g : g \in a+b\} = \bigcup_{g \in D_G(a,b)} D_G(c,g)\,(\mathrm{V})$$

and

$$a+(b+c) = \bigcup\{h+a : h \in b+c\} = \bigcup_{h \in D_G(b,c)} D_G(h,a)\,(\mathrm{VI})$$

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 $(G,\cdot,1)$ being 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 $a,b,g \in M(G)$.

□

cor:equiv1

Corollary 2.2.2. *The correspondence $G \mapsto M(G)$ defines a full and faithful functor*

$$M : SG \to MF.$$

Proof. Let $f : G \to H$ be a SG-morphism. We 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 $M(f)(ab) = M(f)(a)M(f)(b)$. Since $d \in D_G(a,b)$ implies $f(d) \in D_H(f(a),f(b))$ we have

$$d \in a+b \text{ imply } M(f)(d) \in M(f)(a)+M(f)(b) \text{ for all } a,b \in M(G),$$

so $M(f)$ is a multiring morphism. Now, let $f : G \to H$ and $g : H \to K$ be SG-morphisms. Since $M(f\circ g)\restriction_G = f\circ g = M(f)\restriction_G \circ M(g)\restriction_G$ 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 $M : SG \to MF$ 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 $M(G) \setminus \{0\} = G$. □

prop:missues

Proposition 2.2.3. *Let G be an SG and $M(G)$ as above. Then:*

i - $a^2 = 1$ *for all* $a \in M(G) \setminus \{0\}$*;*

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*

$$\begin{cases} ax = cy \\ a = xz \\ d = yz \end{cases} \quad \textit{and} \begin{cases} a \in c + y \\ b \in x + z \\ c \in y + z \end{cases}$$

then there exists $t, v, w \in \dot{M}(G)$ *such that*

$$\begin{cases} bt = cv \\ b = tw \\ c = vw \end{cases} \quad \textit{and} \begin{cases} b \in c + v \\ a \in t + w \\ d \in v + w \end{cases}$$

Proof.

i - Is just the fact of G be a group of exponent 2.

ii - Follow immediately.

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 1, we get

$$\langle xy, xya\rangle \equiv \langle y, ya\rangle \equiv \langle 1, a\rangle$$

and then $xy \in D_G(1, a) = 1 + a \equiv_G$.

iv - Follow from 3-transitivity.

□

defn:special.mf

Definition 2.2.4. *A hyperfield F satisfying the properties i-iv of Proposition 2.2.3 will be called a special hyperfield (SMF). Note that, if G is a SG, then $M(G)$ is a SMF.*

mf.to.special

Theorem 2.2.5. *If F is a special hyperfield the $(F \setminus \{0\}, \equiv, -1)$ is a special group where*

$$\langle a, b\rangle \equiv \langle c, d\rangle \textit{ iff } ab = cd \textit{ and } a \in c + d$$

Proof. By (i), we have that $(F \setminus \{0\}, 1)$ is a group of exponent 2. Now, we check each axiom of Definition 2.1.2:

SG0 - By (ii) $1 \in 1+ab$, so $ab \in 1+ab$ and $a \in b+a$. Since $ab = ab$, then $\langle a,b\rangle \equiv \langle a,b\rangle$, i.e, the relation $\equiv$ 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 hyperfield, $ab = ba$. 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 $a \in c+d$.

eq:1
$$ab = cd \Rightarrow -abbc = -bccd \Rightarrow -ac = -bd \tag{2.1}$$

eq:2
$$a \in c+d \Rightarrow ad \in 1+cd = 1+ab \Rightarrow d \in a+b \Rightarrow a \in -b+d \tag{2.2}$$

so by 2.1 and 2.2 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 2.1.8. $\langle a,b,ab\rangle \equiv \langle c,d,cd\rangle \Rightarrow$ there exists $x,y,t \in F\setminus\{0\}$ 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 $t,v,w \in F\setminus\{0\}$ 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 $\langle b,a,ab\rangle \equiv \langle c,d,cd\rangle$.

□

cor:equiv2

Corollary 2.2.6. *There is a functor $S : SMF \to SG$.*

Proof. In the objects of SMF, we define $S(F) = F\setminus\{0\}$ since the special group as stated in Theorem 2.2.5. Now, let $\sigma : F \to K$ be a SMF-morphism. Define $S(\sigma) = \sigma|_{F\setminus\{0\}}$. 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 $d \in F\setminus\{0\}$ 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. □

teo:sgsmfequiv

Theorem 2.2.7. *There exist an equivalence of categories between SG and SMF.*

Proof. By the Corollaries 2.2.2 and 2.2.6, we have functors $M : SG \to SMF$ and $S : SMF \to SG$. We will proof that $M \circ S \cong Id_{SMF}$ and $S \circ M \cong Id_{SG}$.

i - $M \circ S \cong Id_{SMF}$. Let F be a SMF. How $S(F) = F \setminus \{0\}$ 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 $S(\sigma) = \sigma|_{F\setminus\{0\}}$ and $M(S(\sigma))$ is defined with the extension $S(\sigma)(0) = 0$. Therefore $M(S(\sigma)) = \sigma$ and $M \circ S \cong Id_{SMF}$.

ii - $S \circ M \cong Id_{SG}$. 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 $S \circ M \cong Id_{SG}$, finalizing the proof.

□

psgpsmfhell

Theorem 2.2.8. *Let G be a pre-special group and consider $(M(G), +, -, 0, 1)$, with operations defined by*

- $a \cdot b = \begin{cases} 0 \textit{ if } a = 0 \textit{ or } b = 0 \\ a \cdot b \textit{ otherwise} \end{cases}$
- $-(a) = (-1) \cdot a$
- $a + b = \begin{cases} \{b\} \textit{ if } a = 0 \\ \{a\} \textit{ if } b = 0 \\ M(G) \textit{ if } a = -b, \textit{ and } a \neq 0 \\ D_G(a, b) \textit{ otherwise} \end{cases}$

Then $M(G)$ is a pre-special multifield. Conversely, if F is a pre-special multifield then $(\dot{F}, \equiv_F, -1)$ is a pre-special group, where

$$\langle a, b\rangle \equiv_F \langle c, d\rangle \textit{ iff } ab = cd \textit{ and } a \in c + d.$$

To prove it we will need a result from [28].

1.21chico

Lemma 2.2.9 (Lemma 1.21 of [28])**.** *Let $(G, \equiv, -1)$ be a pre-special group. Let a, b, c, x, y be elements of G and φ, ψ be forms over G. Assume that $\langle a, b\rangle \equiv \langle x, y\rangle$. Then*

i - If $\varphi \equiv \langle a, b\rangle$ then $\varphi \equiv \langle x, y\rangle$.

ii - For all $\sigma \in S_3$, $\langle a, b, c\rangle \equiv \langle x, y, c\rangle^\sigma$, where

$$\langle x, y, c\rangle^\sigma := \langle \sigma(e_1), \sigma(e_2), \sigma(e_3)\rangle \textit{ with } e_1 = x,\ e_2 = y,\ e_3 = c.$$

Proof of Theorem 2.2.8. Let F be a pre-special hyperfield. The argument to proof that $(\dot{F}, \cdot, 1, \equiv)$ is a pre-special group is the same of the proof of Theorem 3.18 in [24].

Now let $(G, \cdot, 1, \equiv)$ be a pre-special group an $M(G)$ as above. Firstly, note that by SG2 and the fact that $\equiv$ is an equivalence relation we have $a - a = 1 - 1 = M(G)$ for all $a \in G$. Moreover if $x, y \in 1 + a = D_G(1, a)$ with $a \neq -1$, we have $\langle x, xa\rangle \equiv \langle 1, a\rangle$ and $\langle y, ya\rangle \equiv \langle 1, a\rangle$. Using SG5 (and the fact that $\equiv$ is an equivalence relation) we get that $\langle 1, a\rangle \equiv \langle x, xa\rangle$ imply

$$\langle (xy)1, (xy)a\rangle \equiv \langle (xy)x, (xy)xa\rangle \equiv \langle y, ya\rangle \equiv \langle 1, a\rangle,$$

proving that $xy \in D_G(1,a) = 1+a$.

Therefore, once we verify the conditions of Definition 1.2.7 we get that $(M(G),+,\cdot,0,1)$ is a pre-special hyperfield.

The verification of the conditions in Definition 1.2.7 is quite straightforward except perhaps by associativity, which we will prove here. We want to show that for all $a,b,c \in M(G)$,

$$(a+b)+c = a+(b+c).$$

If $0 \in \{a,b,c\}$ we are done. Now let $0 \notin \{a,b,c\}$. We prove that

$$a+(b+c) = D_G(a,b,c).$$

In fact, if $x \in a+(b+c)$ then $x \in a+y$ for some $y \in b+c$. Then we have $v,w \in G$ with

$$\langle x,v\rangle \equiv \langle a,y\rangle \text{ and } \langle y,w\rangle \equiv \langle b,c\rangle.$$

These isometries imply that $\langle x,v,w\rangle \equiv \langle a,b,c\rangle$ and then $x \in D_G(a,b,c)$. Conversely, let $x \in D_G(a,b,c)$. Then

$$\langle x,z_2,z_3\rangle \equiv \langle a,b,c\rangle$$

for some $z_2,z_3 \in G$, and hence, there are $t_1,t_2,t_3 \in G$ with

$$\langle x,t_1\rangle \equiv \langle a,t_2\rangle,\ \langle z_2,z_3\rangle \equiv \langle t_1,t_3\rangle \text{ and } \langle b,c\rangle \equiv \langle t_2,t_3\rangle.$$

Therefore $x \in a+t_2$ with $t_2 \in b+c$, so $x \in a+(b+c)$. In particular, if $\langle a,b,c\rangle \equiv \langle x,y,z\rangle$, then

$$a+(b+c) = x+(y+z).$$

Since $a,b \in \langle a,b\rangle$ and $\langle a,b\rangle \equiv \langle b,c\rangle$, using Lemma 2.2.9 we have

$$\langle a,b,c\rangle \equiv \langle c,a,b\rangle \Rightarrow a+(b+c) = c+(a+b) = (a+b)+c.$$

Then, $(M(G),+,-,\cdot,0,1)$ is a pre-special hyperfield. □

2.3 A Special Group associated to domains via Marshall quotient

Let F be a field. There is an almost canonical way to associate a special group to F (described in Example 2.1.4): consider $G_F := \dot{F}/\dot{F}^2$ with the isometry given by the usual isometry provide by the algebraic theory of quadratic forms. As we have already seen, G_F is the multiplicative group of units of a special hyperfield, and in this sense,

$$M_F = G_F \cup \{0\} \cong F/_m\dot{F}^2.$$

In other words, we put in correspondence special groups and special hyperfields just adding (or erasing) a zero element.

One of the main purposes of this work is extend the above situation, $M_A \cong A/_mT$, where A is a commutative ring with unit and M_A is a *formally* real semigroup. This section deals with the case where A is a domain, i.e, rings without zero divisors. Of course, we fatally need to impose some conditions to our structures:

Definition 2.3.1. *An* ***hyperbolic multiring*** *is a multiring R such that $1-1=R$.*

Note that if R is hyperbolic and $a \in R^\times$, then $R = a - a$. For a ring R (i.e, the sum is univalorated), *R never is hyperbolic*, since $1 - 1 = \{0\}$. However, this is not a problem, since the inclusion functor $Ring_2 \hookrightarrow MRing_2$ is not the most natural to be considered in the quadratic forms context. Considering the special group of a field $G(F) = \dot{F}/\dot{F}^2$ and its special hyperfield associated, $M(G(F)) = G(F) \cup \{0\}$, we get that $M(G(F))$ is hyperbolic. Hence, the desired functor to keep in mind is $M \circ G : Fields_2 \to SMF$.

Let R be a ring without zero divisors. The main goal of this section is to describe conditions for a subset $T \subseteq R \setminus \{0\}$ of R in such a way that $R/_mT$ is a special hyperfield and therefore, (essentially) a special group. Of course, here is an abuse of notation: when we say that "$R/_mT$ is a special group" we mean that "the induced structure in $(R/_mT) \setminus \{0\}$ provides a special group strucuture".

We we seek for inspiration in the analogous conditions for the field case (see for instance, Definition 1.28 of [28], and in particular, the "completing squares" Lemma 1.29). After months of hard work, we obtained the following Definition:

Definition 2.3.2. *A* ***Dickmann-Miraglia multiring (or DM-multiring for short)*** [1] *is a pair (R, T) such that R is a multiring, $T \subseteq R$ is a multiplicative subset of $R \setminus \{0\}$, and (R, T) satisfy the following properties:*

DM0 *$R/_mT$ is hyperbolic.*

DM1 *If $\overline{a} \neq 0$ in $R/_mT$, then $\overline{a}^2 = \overline{1}$ in $R/_mT$. In other words, for all $a \in R \setminus \{0\}$, there are $r, s \in T$ such that $ar = s$.*

DM2 *For all $a \in R$, $(\overline{1} - \overline{a})(\overline{1} - \overline{a}) \subseteq (\overline{1} - \overline{a})$ in $R/_mT$.*

DM3 *For all $a, b, x, y, z \in R \setminus \{0\}$, if*

$$\begin{cases} \overline{a} \in \overline{x} + \overline{b} \\ \overline{b} \in \overline{y} + \overline{z} \end{cases} \quad \text{in } R/_mT,$$

then exist $\overline{v} \in \overline{x} + \overline{z}$ such that $\overline{a} \in \overline{y} + \overline{v}$ and $\overline{vb} \in \overline{xy} + \overline{az}$ in $R/_mT$.

If R is a ring, we just say that (R, T) is a DM-ring, or R is a DM-ring. A Dickmann-Miraglia hyperfield (or DM-hyperfield) F is a hyperfield such that $(F, \{1\})$ is a DM-multiring (satisfy DM0-DM3). In other words, F is a DM-hyperfield if F is hyperbolic and for all $a, b, v, x, y, z \in F^*$,

i - $a^2 = 1$.

ii - $(1 - a)(1 - a) \subseteq (1 - a)$.

iii - *If* $\begin{cases} a \in x + b \\ b \in y + z \end{cases}$ *then exist $v \in x + z$ such that $a \in y + v$ and $vb \in xy + az$.*

Remark 2.3.3. *These Axioms above deserves some explanation:*

i - Since R is a domain and $0 \notin T$, $\overline{a} = \overline{0}$ in $R/_mT$ iff $a = 0$.

ii - DM1 entails that $R/_mT$ is a hyperfield.

[1]The name "Dickmann-Miraglia" is given in honor to professors Maximo Dickmann and Francisco Miraglia, the creators of the special group theory.

iii - In DM2, the expression $(1-a)(1-a)$ *means* ***multiplication of sets****, i.e,*

$$(1-a)(1-a) := \{x \cdot y : x, y \in 1-a\}.$$

iv - Looking at the expression in DM3, from

$$\begin{cases} \overline{v} \in \overline{x} + \overline{z} \\ \overline{b} \in \overline{y} + \overline{z} \\ \overline{a} \in \overline{x} + \overline{b} \end{cases} \quad in\ R/_mT,$$

and the properties of multiring, we obtain

$$\overline{vb} \in \overline{xy} + (\overline{xz} + \overline{yz} + \overline{z}^2) \supseteq \overline{xy} + \overline{z}(\overline{x} + \overline{y} + \overline{z}) \ in\ R/_mT$$

and

$$\overline{a} \in \overline{x} + \overline{b} \subseteq \overline{x} + \overline{y} + \overline{z} \ in\ R/_mT.$$

Hence, we can interpret the condition $\overline{vb} \in \overline{xy} + \overline{az}$ *in* $R/_mT$ *as a way of "controlling" the product* $\overline{vb}$ *to "not escape so much" under the set* $\overline{x} + \overline{y} + \overline{z}$*. In the field case (when we can "change"* $\in$ *by* $=$*), under the Marshall's quotient the condition M3 is not necessary (see Theorem 1.32 of [28]).*

v - In DM3, if $0 \in \{a, b, x, y, z\}$ *the axiom is trivially valid.*

teopmf

Theorem 2.3.4. *Let* (R, T) *be a DM-multiring and denote* $Sm(R,T) = (R/_mT)$*. Then* $Sm(R)$ *is a special hyperfield (thus* $Sm(R,T)^\times$ *is a special group).*

Remember that a special hyperfield is a hyperfield F satisfying:

SMF1 $a^2 = 1$ for all $a \in \dot{F}$;

SMF2 $1 \in 1 + a$ for all $a \in F$;

SMF3 $1 + a$ is closed by multiplication for all $a \in \dot{F}$;

SMF4 For all $a, b, c \in \dot{F}$,

$$\text{If } \exists\, p \in \dot{F} \text{ such that } \begin{cases} a & \in c + cp \\ b & \in p + ap \\ d & \in p + cp. \end{cases} \text{ then } \exists\, l \in \dot{F} \text{ such that } \begin{cases} a & \in d + dl \\ b & \in l + al \\ c & \in l + dl. \end{cases}$$

Proof of Theorem 2.3.4. The properties [SMF1]-[SMF3] are imediately consequence of the axioms of sum in a multiring and [M0]-[M2] in the Definition of DM-multirings. Then, we shall prove [SMF 4]: we will rewrite de argument of Theorem 1.32 in [28]. In order to do this, we use the language of special groups. If we prove that $R/_mT$ is a special group, then we prove that it is a special hyperfield (since [SMF 4] is precisely the translation of the axiom [SG9] for special groups to the language of hyperfields).

Here, the special relation in $R/_mT$ is defined by the rule

$$\langle \overline{a}, \overline{b} \rangle \equiv \langle \overline{c}, \overline{d} \rangle \Leftrightarrow [\overline{ab} = \overline{cd} \text{ and } \overline{a} \in \overline{c} + \overline{d}] \ (\text{ in } R/_mT).$$

Translating this to a condition with coefficients in R, we have

$$\langle \overline{a}, \overline{b}\rangle \equiv \langle \overline{c}, \overline{d}\rangle \Leftrightarrow [abv = cdw \text{ and } ar \in cs + dt] \text{ for some } r, s, t, v, w \in R.$$

Using [SMF1]-[SMF3] and the multirings properties we obtain the validity of [SG0-SG5] (for more details, see Theorem 3.18 of [24]).

Hence by 2.1.6 we only need to deal with [SG9] (see condition (5) in Theorem 1.23 of [28]), and it is enough to show that

$$\langle \overline{a}, \overline{b}, \overline{c}\rangle \equiv \langle \overline{x}, \overline{y}, \overline{z}\rangle \text{ implies } \langle \overline{a}, \overline{b}, \overline{c}\rangle \equiv \langle \overline{y}, \overline{x}, \overline{z}\rangle.$$

Suppose $\langle \overline{a}, \overline{b}, \overline{c}\rangle \equiv \langle \overline{x}, \overline{y}, \overline{z}\rangle$. Then, there exist α, β, γ such that

$$\langle \overline{a}, \overline{\alpha}\rangle \equiv \langle \overline{x}, \overline{\beta}\rangle,\ \langle \overline{b}, \overline{c}\rangle \equiv \langle \overline{\alpha}, \overline{\gamma}\rangle \text{ and } \langle \overline{y}, \overline{z}\rangle \equiv \langle \overline{\beta}, \overline{\gamma}\rangle. \tag{2.3}$$

Then, there exists $p_a, q_a, r_a, p_\beta, q_\beta, r_\beta \in T$ such that

$$ap_a \in xq_a + \beta r_a. \tag{2.4}$$

$$\beta p_\beta \in yq_\beta + zr_\beta. \tag{2.5}$$

Therefore $\overline{a} \in \overline{x} + \overline{b}$ and $\overline{b} \in \overline{y} + \overline{z}$. Applying [DM3], exists

$$\overline{v} \in \overline{x} + \overline{z}, \tag{2.6}$$

such that

$$\overline{a} \in \overline{y} + \overline{v}. \tag{2.7}$$

We discuss two cases.

Case I: $v = 0$. Then, from equation 2.7, we have $\overline{a} = \overline{y}$. Consequently, the third isometry in equation 2.3 can be written as $\langle \overline{a}, \overline{z}\rangle \equiv \langle \overline{\beta}, \overline{\gamma}\rangle$. This isometry, the first one in equation 2.3 and [SG4] yield

$$\langle \overline{x}, -\overline{\alpha}\rangle \equiv \langle \overline{a}, -\overline{\beta}\rangle \equiv \langle -\overline{z}, \overline{\gamma}\rangle,$$

and so $\langle \overline{x}, -\overline{\alpha}\rangle \equiv \langle -\overline{z}, \overline{\gamma}\rangle$. Another application of [SG4] yields $\langle \overline{x}, \overline{z}\rangle \equiv \langle \overline{\alpha}, \overline{\gamma}\rangle$, which together with the second isometry in equation 2.3, gives $\langle \overline{x}, \overline{z}\rangle \equiv \langle \overline{b}, \overline{c}\rangle$. Then, we have

$$\langle \overline{a}, \overline{x}\rangle \equiv \langle \overline{a}, \overline{x}\rangle,\ \langle \overline{b}, \overline{c}\rangle \equiv \langle \overline{x}, \overline{z}\rangle, \text{ and } \langle \overline{x}, \overline{z}\rangle \equiv \langle \overline{x}, \overline{z}\rangle,$$

which shows that $\langle \overline{a}, \overline{b}, \overline{c}\rangle \equiv \langle \overline{a}, \overline{x}, \overline{z}\rangle$, as required.

Case II: $v \neq 0$. Equation 2.7 implies $\overline{a} \in \overline{y} + \overline{v}$, while equation 2.6 yields $\overline{v} \in \overline{x} + \overline{z}$. Therefore,

$$\langle \overline{a}, \overline{vay}\rangle \equiv \langle \overline{y}, \overline{v}\rangle \text{ and } \langle \overline{v}, \overline{vxz}\rangle \equiv \langle \overline{x}, \overline{z}\rangle.$$

These isometries imply that, in order to prove that $\langle \overline{a}, \overline{b}, \overline{c}\rangle \equiv \langle \overline{y}, \overline{x}, \overline{z}\rangle$, it is enough to verify that $\langle \overline{vay}, \overline{vxz}\rangle \equiv \langle \overline{b}, \overline{c}\rangle$. From the isometries in equation 2.3 we get $\overline{\alpha} = \overline{ax\beta}$, $\overline{\gamma} = \overline{yz\beta}$ and $\langle \overline{b}, \overline{c}\rangle \equiv \langle \overline{\alpha}, \overline{\gamma}\rangle$. Then, we have $\langle \overline{b}, \overline{c}\rangle \equiv \langle \overline{ax\beta}, \overline{z\beta}\rangle$.

Hence, what is needed is equivalent to $\langle \overline{ax\beta}, \overline{z\beta}\rangle \equiv \langle \overline{vay}, \overline{vxz}\rangle$. Since the discriminants are the same, it is enough to prove $\overline{ax\beta} \in \overline{vay} + \overline{vxz}$.

$$\overline{ax\beta} \in \overline{vay} + \overline{vxz} \Leftrightarrow \overline{ax\beta axv} \in \overline{vayaxv} + \overline{vxzaxv} \Leftrightarrow \overline{v\beta} \in \overline{xy} + \overline{az}.$$

then, it is enough verify that $\overline{v\beta} \in \overline{xy} + \overline{az}$. Moreover, axiom [DM3], already gave to us that $\overline{v}\overline{\beta} \in \overline{xy} + \overline{az}$, which finalize the verification of [SG6].

□

Example 2.3.5. *Let X_n be the kaleidoscope multiring (as defined in 1.2.12). Of course, if $n \geq 2$, X_n is never a DM-hyperfield. However, considering $T = X_n^2 \setminus \{0\}$, since $X_n^2 = \{0, 1, 2, ..., n\}$ we get*

$$K := X_n/_mT \cong X_1 = \{-1, 0, 1\}.$$

Since X_1 is a special hyperfield, (X_n, T) is a DM-multiring.

Example 2.3.6. *Let p be a prime integer and consider the H_p as defined in 1.2.13 and $T = \sum H_p^2 \setminus \{0\}$. Then (H_p, T) is a DM-hyperfield since $H_p/_mT$ is a real reduced hyperfield.*

The above Theorem says that our DM-hyperfields are compatible with the special group structure obtained using Theorem 1.32 of [28].

sgf

Theorem 2.3.7. *Let A be a domain with $2 \neq 0$. Consider $T \subseteq A$ be a proper preordering or $T = A^2$ and denote $T^* = T \setminus \{0\}$. Then $A/_mT^*$ is a special hyperfield, and therefore $G_T(A) := (A/_mT^*) \setminus \{0\}$ is a special group with representation given by*

$$D_{G_A}(\overline{a}, \overline{b}) = \overline{a} + \overline{b} = \{\overline{c} : cr = as + bt \text{ for some } r, s, t \in T^*\}.$$

Moreover, $G_T(A)$ is reduced if and only if T is a proper preordering.

Proof. By Theorem 2.3.4, we only need to proof that $A/_mT^*$ is a DM-hyperfield. First of all, note that

$$\text{For all } a, b \in A^*,\ \overline{a}, \overline{b} \in \overline{a} + \overline{b}. \tag{2.8}$$

lemsgf

If $a = \pm b$ is immediate (for example, $a(5a)^2 = a(4a)^2 + a(3a)^2$ or $a(3a)^2 = a(5a)^2 - a(4a)^2$, in the case where $3, 5 \neq 0$). If $a \neq \pm b$, then

$$a(a + b)^2 = a(a - b)^2 + b(2a)^2$$

and $a^2 + b^2, (a - b)^2, 2a^2 \in T^*$. Hence $\overline{a} \in \overline{a} + \overline{b}$. Similarly we conclude $\overline{b} \in \overline{a} + \overline{b}$.

Now, we verify the axioms [DM0]-[DM3].

DM0 Of course, $\overline{0} \in \overline{1} - \overline{1}$. If $a \neq 0$, and $a \neq \pm 1$, then

$$4a = (a + 1)^2 - (a - 1)^2,$$

and hence $\overline{a} \in \overline{1} - \overline{1}$. If $a = 1$ or $a = -1$, then

$$9 = 5^2 - 4^2 \text{ and } -9 = 4^2 - 5^2$$

testimony that $\overline{1}, -\overline{1} \in \overline{1} - \overline{1}$. Therefore $A/_mT^*$ is hyperbolic.

DM1 Let $\overline{a} \neq 0$ in $A/_mT$. Then $a^2 \in T$, hence $\overline{a}^2 = \overline{1}$.

DM2 Suppose without loss of generality that $a \in A^*$, $a \notin T$ (and hence $\overline{a} \notin \{-\overline{1}, \overline{0}, \overline{1}\}$). Now, let $\overline{\alpha}, \overline{\beta} \in \overline{1} + \overline{a}$, with $\alpha x = r + as$, $\beta y = t + aw$, for some $x, y, r, s, t, w \in T^*$. Then

$$(r + as)(t + aw) = (rt + a^2 sw) + (st + rw)a.$$

If T is a preordering, then $rt + a^2 sw \in T^*$ and $st + rw \in T^*$. If $T = A^2$, then $r = r_1^2$, $s = s_1^2$, $t = t_1^2$, $w = w_1^2$ for some $r_1, s_1, t_1, w_1 \in A^*$. Therefore

$$\begin{aligned}(r + as)(t + aw) &= (rt + a^2 sw) + (st + rw)a \\ &= a^2 sw + rt - 2r_1 s_1 t_1 w_1 a + 2r_1 s_1 t_1 w_1 a + (st + rw)a \\ &= (a^2 sw - 2r_1 s_1 t_1 w_1 a + rt) + (st + 2r_1 s_1 t_1 w_1 + rw)a \\ &= (a^2 s_1^2 w_1^2 - 2r_1 s_1 t_1 w_1 a + r_1^2 t_1^2) + (s_1^2 t_1^2 + 2r_1 s_1 t_1 w_1 + r_1^2 w_1^2)a \\ &= (as_1 w_1 - r_1 t_1)^2 + (s_1 t_1 + r_1 w_1)^2 a.\end{aligned}$$

If $(as_1 w_1 - r_1 t_1)^2 = (s_1 t_1 + r_1 w_1)^2 = 0$ we have $\overline{r + at} = \overline{0}$ or $\overline{s + aw} = \overline{0}$, and hence $r = -at$ or $s = -aw$, and both cases imply $-\overline{a} = \overline{1}$. If $(as_1 w_1 - r_1 t_1)^2, (s_1 t_1 + r_1 w_1)^2 \neq 0$ then $(as_1 w_1 - r_1 t_1)^2, (s_1 t_1 + r_1 w_1)^2 \in T^*$ and we are done. If $(as_1 w_1 - r_1 t_1)^2 = 0$, using 2.8

$$(r + as)(t + aw) = (s_1 t_1 + r_1 w_1)^2 a \Rightarrow \overline{\alpha}\overline{\beta} = \overline{a} \in 1 + \overline{a}.$$

If $(s_1 t_1 + r_1 w_1)^2 = 0$, using 2.8

$$(r + as)(t + aw) = (as_1 w_1 - r_1 t_1)^2 \Rightarrow \overline{\alpha}\overline{\beta} = \overline{1} \in 1 + \overline{a},$$

completing the proof.

DM3 Let

$$\begin{cases} \overline{a} \in \overline{x} + \overline{b} \\ \overline{b} \in \overline{y} + \overline{z} \end{cases} \quad \text{in } A/_m T,$$

with $\overline{a}, \overline{b}, \overline{x}, \overline{y}, \overline{z} \neq \overline{0}$. Then, there exists $p_a, q_a, r_a, p_b, q_b, r_b \in T$ such that

$$ap_a = xq_a + br_a. \tag{2.9}$$

$$bp_b = yq_b + zr_b. \tag{2.10}$$

Therefore

$$ap_a p_b = xp_b q_a + bp_b r_a = xp_b q_a + (yq_b + zr_b)r_a = xp_b q_a + yq_b r_a + zr_a r_b.$$

Now, consider

$$v = xp_b q_a + zr_a r_b. \tag{2.11}$$

Note that $\overline{v} \in \overline{x} + \overline{z}$ and

$$ap_a p_b = yq_b r_a + v, \tag{2.12}$$

with $\overline{a} \in \overline{y} + \overline{v}$. In order to complete the proof, we only need to verify that $\overline{vb} \in \overline{xy} + \overline{az}$. In fact,

$$\begin{aligned}
vbp_b &= (xp_bq_a + zr_ar_b)(yq_b + zr_b) \\
&= xyp_bq_aq_b + xzp_bq_ar_b + yzq_br_ar_b + z^2r_ar_b^2 \\
&= xyp_bq_aq_b + z(xp_bq_ar_b + yq_br_ar_b + zr_ar_b^2) \\
&= xyp_bq_aq_b + z(xp_bq_ar_b + (yq_b + zr_b)r_ar_b) \\
&= xyp_bq_aq_b + z(xp_bq_ar_b + bp_br_ar_b) \\
&= xyp_bq_aq_b + (xq_a + br_a)zp_br_b \\
&= xyp_bq_aq_b + ap_azp_br_b \\
&= xyp_bq_aq_b + azp_ap_br_b,
\end{aligned}$$

and hence, $\overline{vb} \in \overline{xy} + \overline{az}$.

□

Corollary 2.3.8. *Let D be a domain with $2 \neq 0$ and consider the polynomial ring $D[x_1, ..., x_n]$. Let $T \subseteq D[x_1, ..., x_n]$ be a preordering or $T = (D[x_1, ..., x_n])^2$. Then $D[x_1, ..., x_n]/_mT^*$ is a special group.*

Theorem 2.3.9. *Let F be a hyperfield satisfying DM0-DM2. Then F satisfy DM3 if and only if satisfy SMF4. In other words, F is a DM-hyperfield if and only if is a special hyperfield.*

Proof. After Theorem 2.3.4, we only need to prove that if F is a special hyperfield then F satisfy DM3. Let $a \in x + b$ and $b \in y + z$. Then by definition, $a \in x + y + z$, and then, there exist some $v \in x + z$ such that $a \in y + v$. We need to prove that $vb \in xy + az$. We discuss two cases.

Case I: $v = 0$. Then $a = y$ and $z = -x$. Moreover

$$0 = vb \in ax - ax = xy + az.$$

Case II: $v \neq 0$. Here we consider the special group structure in F^*. Moreover, for all $a, b \in F^*$, $a, b \in a + b$. Considering $a \in x + b$ and $b \in y + z$, we get the above isometries

$$\langle byz, x\rangle \equiv \langle x, byz\rangle,\ \langle axb, a\rangle \equiv \langle x, b\rangle \text{ and } \langle y, z\rangle \equiv \langle byz, b\rangle.$$

Then by definition $\langle byz, axb, a\rangle \equiv \langle x, y, z\rangle$.

Moreover, considering $a \in y + v$ and $v \in x + z$, we get the above isometries

$$\langle vxz, y\rangle \equiv \langle y, vxz\rangle,\ \langle ayv, a\rangle \equiv \langle y, v\rangle \text{ and } \langle x, z\rangle \equiv \langle vxz, v\rangle.$$

Then by definition $\langle vxz, ayv, a\rangle \equiv \langle y, x, z\rangle$. Since F^* is a special group, $\langle x, y, z\rangle \equiv \langle y, x, z\rangle$ and the isometry relation is 3-transitive. Then

$$\langle byz, axb, a\rangle \equiv \langle x, y, z\rangle \equiv \langle y, x, z\rangle \equiv \langle vxz, ayv, a\rangle,$$

and hence, $\langle byz, axb, a\rangle \equiv \langle vxz, ayv, a\rangle$. Using Witt's Cancellation, $\langle byz, axb\rangle \equiv \langle vxz, ayv\rangle$. Then,

$$vxz \in byz + axb \Rightarrow vbxz \in yz + ax \Rightarrow vb \in xy + az,$$

completing the proof.

□
hkh

Theorem 2.3.10. *Let $(G, \equiv, 1, -1)$ be a pre-special group. Are equivalent:*

1. *G is special, i.e, satisfy (for example) SG6.*
2. *$M(G)$ (the hyperfield associated to G) satisfy DM3.*
3. *G satisfy the following condition for all $a, b, x, y, z \in G$:*

$$\text{If } a \in D_G(x, b) \text{ and } b \in D_G(y, z) \text{ then there exist } v \in D_G(x, z)$$
$$\text{such that } a \in D_G(y, v) \text{ and } vb \in D_G(xy, az).$$

2.4 DM-multirings and Quadratically presentable fields

Let (R, T) be a DM-multiring and $G(R, T) := (R/_mT) \setminus \{0\}$. Since $G(R, T)$ is a special group, we can provide a theory of quadratic forms for R inherited from $G(R, T)$: Let $\equiv$ be the isometry relation on $G(R, T)^2$ given by $\langle a, b\rangle \equiv \langle c, d\rangle$ iff $ab = cd$ in $G(R, T)$ and $a \in c + d \setminus \{0\}$. We extend $\equiv$ to a binary relation $\equiv_n$ on $G(R, T)^n$, 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 $\langle b_2, ..., b_n\rangle \equiv_{n-1} \langle y, z_3, ..., z_n\rangle$.

Since $G(R, T)$ is a special group, $\equiv_n$ is transitive for all $n \geq 2$ (in fact, this is the content of axiom SG6). Whenever clear from the context, we frequently abuse notation and indicate the aforedescribed extension $\equiv$ by the same symbol.

A **form** φ on $G(R, T)$ is an n-tuple $\langle a_1, ..., a_n\rangle$ of elements of $G(R, T)$; 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 $G(R, T)$, define

a - The **set of elements represented by** φ as

$$D_{G(R,T)}(\varphi) := \{b \in G(R, T) : \exists\, z_2, ..., z_n \in G(R, T) \text{ such that } \varphi \equiv \langle b, z_2, ..., z_n\rangle\}.$$

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 $a \in G(R, T)$, $\langle a\rangle \otimes \varphi$ is written $a\varphi$.

A form φ on $G(R, T)$ is **isotropic** if there is a form ψ over $G(R, T)$ such that $\varphi \equiv \langle 1, -1\rangle \oplus \psi$; otherwise it is said to be **anisotropic**. We say that φ is **universal** if $D_{G(R,T)}(\varphi) = G(R, T)$.

In this sense, **Witt Ring** $W(R, T)$ of (R, T) is defined as the Witt ring $W(G(R, T))$ of $G(R, T)$. We can go further, and define a **form** $\varphi = \langle a_1, ..., a_n\rangle$ on (R, T) by considering the form $\overline{\varphi} := \langle \overline{a_1}, ..., \overline{a_n}\rangle$ on $G(R, T)$ and so on.

Moreover, this quadratic form theory inherited from $G(R, T)$ is compatible with the more general Witt rings described by P. Gladik and K. Worytkiewicz in [37]:

Definition 2.4.1 (Presentable monoid, group, ring [37]). *Let $(A, \leq, 0)$ be a pointed poset (i.e, a poset with a distinguished element $0 \in A$).*

a - $(A, \leq, 0, +)$ is a ***presentable monoid*** *if the distinguished element 0 is supercompact and $+ : M \times M \to M$ is a suprema-preserving binary operation such that for all $a, b, c \in M$*

- *(a) $a + (b + c) = (a + b) + c$;*
- *(b) $a + 0 = 0 + a = a$;*
- *(c) $a + b = b + a$.*

b - $(A, \leq, 0, +, -)$ is a ***presentable group*** *if $(A, \leq, 0, +)$ is a presentable monoid and $- : G \to G$ is a suprema preserving involutive homomorphism (called* ***inversion****) such that $s \leq t+u$ imply $t \leq s + (-u)$ for all $s, t, u \in \mathcal{S}_G$ (here $\mathcal{S}_G$ denote the set of G's minimal elements).*

c - $(A, \leq, 0, 1, +, -, \cdot)$ is a ***presentable ring*** *if $(A, \leq, 0, +, -)$ is a presentable group, $(A, 1, \cdot)$ is a commutative monoid such that the element 1 is supercompact, $\cdot$ is compatible with $\leq$ and $-$ (i.e, $a \leq b$ imply $a \cdot c \leq b \cdot c$ and $a \cdot (-b) = -(a \cdot b)$ for all $a, b, c \in A$), $\cdot$ is distributive with respect to $+$, $0 \cdot a = 0$ for all $a \in R$ and $\cdot$ satisfy*

$$\mathcal{S}_{a \cdot b} = \{s \cdot t : s \in \mathcal{S}_a,\ t \in \mathcal{S}_b\}.$$

Here $\mathcal{S}_a :=\downarrow a \cap \mathcal{S}_A$ for all $a \in A$, i.e, $\mathcal{S}_a$ is the set of all minimal elements below $a \in A$.

d - $(A, \leq, 0, 1, +, -, \cdot)$ is a ***presentable field*** *if is a presentable ring such that every non-zero element is invertible.*

Now we recall the concept of quadratically presentable fields (in the sense of Definitions 5.1, 5.5 and 5.7 of [37]). A presentable field $(A, \leq, 0, 1, +, -, \cdot)$ is **pre-quadratically presentable** whenever

i - $a \leq a + b$ for all $a \in \mathcal{S}_A^*$, $b \in \mathcal{S}_A$;

ii - $a \leq 1 + b$ and $a \leq 1 + c$ imply $a \leq 1 - bc$ for all $a, b, c \in \mathcal{S}_A$;

iii - $a^2 = 1$ for all $a \in \mathcal{S}_A \setminus \{0\}$.

A **form** on a pre-quadratically presentable field A is an n-tuple $\langle a_1, ..., a_n\rangle$ of elements of $\mathcal{S}_A^*$. The relation $\cong$ of **isometry** of forms of the same dimension is given by induction: (i) $\langle a\rangle \cong \langle b\rangle$ iff $a = b$; (ii) $\langle a_1, a_2\rangle \cong \langle b_1, b_2\rangle$ iff $a_1a_2 = b_1b_2$ and $b_1 \leq a_1 + a_2$; (iii) finally, for $n \geq 3$

$$\langle a_1, ..., a_n\rangle \cong \langle b_1, ..., b_n\rangle \text{ iff there exists } x, y, c_3, ..., c_n \in \mathcal{S}_A^* \text{ such that } \langle a_1, x\rangle \cong \langle b_1, y\rangle$$
$$\langle a_2, ..., a_n\rangle \cong \langle x, c_3, ..., c_n\rangle,\ \langle a_b, ..., b_n\rangle \cong \langle y, c_3, ..., c_n\rangle.$$

A pre-quadratically presentable field is **quadratically presentable** whenever the isometry relation defined above is an equivalence relation on the set of all forms of the same dimension.

Let (R, T) be a DM-multiring. Let $K := R/_mT$ and consider $\mathcal{P}^*(K)$, the pierced powerset of the set K (that is, its set of nonempty subsets). Then $(\mathcal{P}^*(K), \subseteq, \{0\}, \{1\}, +, -, \cdot)$ is a presentable field ([37], Example 4.5), where the operations in $\mathcal{P}^*(K)$ are defined for $A, B \in \mathcal{P}^*(K)$ by

$$-A := \bigcup_{a \in A}\{-a\},\ \ A + B := \bigcup_{a \in A,\, b \in B} a + b \text{ and } A \cdot B := \bigcup_{a \in A,\, b \in B} \{a \cdot b\}.$$

Following 5.18 [37], we obtain:

gladkiadapted

Theorem 2.4.2. *Let (R,T) be a DM-multiring. Let $K := R/_mT$ and $(\mathcal{P}^*(K), \subseteq, \{0\}, \{1\}, +, -, \cdot)$ be the induced presentable field. Then:*

1. *$\mathcal{P}^*(K)$ is a quadratically presentable field.*

2. *$W(\mathcal{P}^*(K)) \cong W(K) = W(R,T)$, where $W(\mathcal{P}^*(K))$ is the Witt ring defined in 5.13[37].*

Proof. (1) This follows, essentially, from the same argument of 2.3.4, since K is a special hyperfield.

(2) Just repeat the arguments used in 7.1, 7.2 and 7.3 of [37].

For the readers comfortable with theory of special groups, the proof of this Theorem is just a translation of axiom SG6. □

In 7.4 of [37] is asked:
"It is an open question when the resulting pre-quadratically presentable field is quadratically presentable."

We finish this section arguing that such question is, in principle, non void. More precisely:

qgladik

Proposition 2.4.3. *There exists a pre-quadratically presentable field that is not quadratically presentable.*

Proof. We show that $pQPF$ is a cocomplete category but QPF is not a cocomplete category.

- In 5.18 of [37] are established equivalences of categories:
  quadratically presentable fields (QPF) $\leftrightsquigarrow$ special groups (SG);
  pre-quadratically presentable fields ($pQPF$) $\leftrightsquigarrow$ pre-special groups (pSG).

- $pQPF$ ($\simeq pSG$) is a cocomplete category. According the Definition of pre-special group (Definition 1.2 in [28]), it is axiomatized by a universal Horn Theory (Definition 5.10 in [1]) thus it is a limit theory (Definition 5.7 in [1]). By Theorem 5.9 in [1], pSG is a finitely locally presentable category, (Definition 1.9 in [1]), thus it is a cocomplete category.

- QPF ($\simeq SG$) is not a cocomplete category.

  * Consider RSG the full subcategory of SG of all reduced special groups, i.e. a special group G such that for each $a \in G$, $\langle a, a\rangle \equiv \langle 1, 1\rangle$ iff $a = 1$. This is a slightly variation on the notion of reduced special group (Definition 1.2 in [28]) since we not exclude the case where $G = \{1\}$ (equivalently, we not impose $-1 \neq 1$). Following the proofs of the results in Chapter 10, Section 3, in [28], the category RSG of all reduced special groups (including the trivial special group $\{1\}$)) misses some binary coproducts, thus is not cocomplete (see for instance, Proposition 10.11 of [28]).

  * The full subcategory $\iota : RSG \hookrightarrow SG$ is reflexive, i.e. it has a left adjoint $S : SG \to RSG$, $G \in Obj(SG) \mapsto G/Sat(G) \in Obj(RSG)$, where the unity of adjunction is $(G \overset{q_G}{\twoheadrightarrow} S(G) := G/Sat(G))_{G\in Obj(SG)}$. This follows from a combination of results in [28]: Remark (iii) just below Definition 2.7; Remark 2.16 and Proposition 2.21.

  * Let $\Gamma : \mathcal{I} \to RSG$ be a small diagram that does not have a colimit in RSG. Suppose that $\iota \circ \Gamma : \mathcal{I} \to SG$ has a colimit $(\gamma_i : \Gamma(i) \to G_\infty)_{i\in obj(\mathcal{I})}$ in SG. Then it is easy to check that $(q_{G_\infty} \circ \gamma_i : \Gamma(i) \to S(G_\infty))_{i\in Obj(\mathcal{I})}$ satisfies the universal property of being the colimit of $\Gamma : \mathcal{I} \to RSG$ in RSG, a contradiction.

□

2.5 Quadratic Multirings and (Formally) Real Semigroup associated to Semi real rings via Marshall quotient

Paraphrasing M. Marshall, "when we change fields for rings, we are in deep water" ([48])! For example, let R be a generic commutative ring and $T \subseteq R$ be a multiplicative set containing 1. From now on, we denote

$$zd(R) := \{a \in R : a \text{ is a zero divisor}\}$$
$$nzd(R) := R \setminus zd(R) = \{a \in R : a \text{ is not a zero divisor}\}.$$

If $a, b \in T \setminus \{0\}$ with $ab = 0$ (i.e, a, b are zero-divisors), then $R/_mT^* \cong \{0\}$: in fact for all $x \in R$, $x(ab) = 0 \cdot 1$ with $ab, 1 \in T$, and hence $\overline{x} = \overline{0}$. Even in the case $T \subseteq nzd(R)$, if $a \in zd(R)$, say $ab = 0$ for some $b \in zd(R)$ then $\overline{a}\overline{b} = \overline{0}$, so $(\overline{ab})^2 = 0 \neq \overline{1}$, and in particular, $R/_mT$ is not a hyperfield.

Then, *if $zd(R) \neq \emptyset$, $R/_mT^*$ will never be a special group, since will never be a hyperfield.* Because this, we seek for conditions for a pair (R, T) with R a ring and $T \subseteq nzd(R)$ multiplicative provide a (formally) real semigroup structure in $R/_mT$.

In this context we christen the following Definition:

qring

Definition 2.5.1. *Let R be a multiring and $T \subseteq nzd(R)$ be a multiplicative subset containing 1. We say that (R, T) is a **quadratic pair** if*

Q1 *$R/_mT$ is semi real.*

Q2 *If $a \in R$ and $a^2 \notin zd(R)$, then $a^2 \in T$.*

Q3 *For all $a \in R$, then $\overline{a}^3 = \overline{a}$ in $R/_mT$.*

Q4 *For all $a, b \in R$, there exists $r, s, t \in T$ such that $ar \in a^3s + a^2bt$.*

Let's look closely to the axioms in Definition 2.5.1. In this sense, Q1 is a kind of generalization of the semireal condition and Q2 is a weakness of $A^2 \subseteq T$. The following Theorem is immediate:

qringteo

Theorem 2.5.2. *Let (R, T) be a quadratic pair and define for all $a, b, c \in R$ the following relations:*

$$\overline{c} \in D^t(\overline{a}, \overline{b}) \text{ if and only if } \overline{c} \in \overline{a} + \overline{b}$$
$$\overline{c} \in D(\overline{a}, \overline{b}) \text{ if and only if } \overline{c} \in D^t(\overline{c}^2 a, \overline{c}^2 b).$$

Then $(R/_mT, D, D^t)$ is a formally real semigroup. Conversely, if (G, D, D^t) is a formally real semigroup such that a^2 is a zero divisor or $a^2 = 1$. Define

$$c \in a + b \text{ if and only if } c \in D^t(a, b).$$

Then $(G, \{1\})$ is a quadratic pair.

Proof. Let (R, T) be a quadratic pair. Axiom RS7b is consequence of Q1 and axiom RS1 is consequence of Q4. The other axioms of formally realsemigroup are consequence of basic properties of multiring and so on.

Conversely, if (G, D, D^t) is a formally real semigroup such that a^2 is a zero divisor or $a^2 = 1$, we automatically have Q2. Q1 is consequence of RS7b, Q3 is consequence of G be a ternary semigroup and Q4 is consequence of RS1. The fact of $(G, +, \cdot, 0, 1)$ be a multiring is consequence of the another axioms of formally realsemigroup (and ternary semigroup). □

Now is time to deal with the real semigroup case. We define the following:

Definition 2.5.3. *A* ***Dickmann-Petrovich multiring (or DP-multiring for short)***[2] *is a quadratic pair* (R,T) *satisfy the following properties:*

DP1 $1+T\subseteq T$.

DP2 *For all* $a\in R$*, exist* $t\in T$ *such that* $1+a^2t\in T$.

DP3 *For all* $a,b\in R$*,* $\overline{a}^2+\overline{b}^2$ *is a singleton set in* $R/_mT$.

teopmr

Theorem 2.5.4. *Let* (R,T) *be a DP-ring and denote* $Rs(R)=(R/_mT)$*. Then* $Rs(R)$ *is a real reduced multiring (thus it is a real semigroup).*

Proof. Since $T\subseteq nzd(R)$, $\overline{1}\neq\overline{0}$ in $Rs(R)$. Moreover, by (Q4) we get $\overline{a^3}=\overline{a}$ in $Rs(R)$.

Note that since T is multiplicative, [Q0] and [DP1] imply $T\cdot T=T$ and

$$T+T=T+T\cdot T=T\cdot(1+T)\subseteq T\cdot T=T,$$

then we have that $T+T\subseteq T$ which imply that $\overline{a}+\overline{a}=\{\overline{a}\}$ for all $\overline{a}\in Rs(R)$.

From (DP2) we get $\overline{1}+\overline{b}^2=\{\overline{1}\}$ for all $b\in R$, which imply $\overline{a}+\overline{ab^2}=\{\overline{a}\}$ for all $a,b\in R$. Finally, [DP3] says that $\overline{a}^2+\overline{b}^2$ is a singleton set in $R/_mT$, completing the proof that $R/_mT$ is a real semigroup. □

Example 2.5.5. *Let* (R,T) *be a DM-multiring. Then* (R,T) *is also a quadratic pair.*

Example 2.5.6. *Let* (R,T) *be a DM-ring such that* $T+T\subseteq T$*. Then* (R,T) *is also a DP-ring.*

With Definition 2.5.1 and Theorem 2.5.2, we generalize the real reduced multirings:

quadraticring

Definition 2.5.7. *A multiring* A *is said to be* ***quadratic*** *if satisfy the following properties:*

QM0 $-1\notin\sum A^2$.

QM1 *for all* $a\in A$*,* $a\in 1-1$.

QM2 *for all* $a\in A$*,* $a^3=a$.

QM3 *for all* $a,b\in A$*,* $a\in a+a^2b$.

Example 2.5.8. *Let* p *be a prime integer and consider* H_p *as in 1.2.13. Since* $a^2=1$ *and* $a=-a$ *for all* $a\in H_p$ *and* $a+a=H_p$ *for all* $a\neq 0$*, we have that* H_p *is not a quadratic multiring.*

But H_p *satisfy QM1, QM2 and QM3. Then, consider the product multiring* $R=X_1\times H_p$*, where* $X_1=\{-1,0,1\}$*. Since* X_1 *is a DM-hyperfield (and hence a DP-multiring) and the operations and multioperation in* R *is defined coordinatewise, we have that* R *satisfy QM1, QM2 and QM3. Since* $(a,b)\in R^2$ *if and only if* $a\in\{0,1\}$ *and* $b\in H_p$*, we have* $-1_R=(-1,1)\notin R^2$*. Hence* R *is a quadratic multiring.*

Example 2.5.9 (Constructions)**.**

[2] The name “Dickmann-Petrovich” is given in honor to professors Max Dickmann and Alejandro Petrovich, who are the creators of realsemigroup theory.

i - *(Products) Let $\{R_i\}_{i\in I}$ be a class of quadratic multiring and let $R=\prod_{i\in I}R_i$. Since the operations and multioperation in R is defined coordinatewise, we have that R is a quadratic multiring. More generally, suppose that R_i satisfy QM1, QM2 and QM3 for all $i\in I$. If there is an index $i_0\in I$ such that R_{i_0} is a quadratic multiring, then R is a quadratic multiring.*

ii - *(Directed Colimits) If $(I,\leq)$ is an upward directed poset and $(f_{ij}:R_i\to R_j)_{i\leq j}$ is a diagram of quadratic multirings, then $colim_{i\in I}R_i$ is a quadratic multiring. More generally, if $(f_{ij}:R_i\to R_j)_{i\leq j}$ is an upward directed diagram of multirings such that $\{i\in I: R_i$ is a quadratic multiring$\}$ is a cofinal subset of I, then $colim_{i\in I}R_i$ is a quadratic multiring.*

iii - *(Reduced Products and Ultraproducts) The class of quadratic multirings can be axiomatized by certain kind of first-order formulas (in a convenient relational language) that shows that this subclass of the class of multirings is closed under reduced products (and ultraproducts, in particular). This result can be achieved more directly by the description of reduced product of a family of (quadratic) multirings, modulo some filter on the index set, as the directed colimit of products of the members of the family indexed by some member of the filter: $\prod_{i\in I}R_i/\mathcal{F}\cong colim_{J\in\mathcal{F}}\prod_{i\in J}R_i$.*

`sgqring`

Example 2.5.10 (Special Groups). *Let G be a special group, and consider $F=M(G):=G\cup\{0\}$ its special hyperfield associated. Of course, F satisfy conditions QM1-QM3 in 2.5.7. F satisfy DM0 iff F is formally real, i.e, if $-1\notin\sum F^2$, which occurs iff G is formally real, i.e,*

$$-1\notin D_G(n\otimes\langle 1\rangle)\text{ for all }n\geq 1.$$

Example 2.5.11. *Let A be a von Neumann regular semi-real ring such that $2\in A^\times$. Then $A/_mA^{\times 2}$ is a quadratic multiring. In fact, first observe that*

*i) If F is a field with $2\in F^\times$, then $F/_mF^{\times 2}$ is a multiring that satisfies **QM1-QM3** as indicate Examples 2.1.4 and 2.5.10. This means that F satisfies the following Horn-geometric sentences:*

- $\forall a\exists x,y,x',y'(xx'=yy'=1\wedge a=x^2-y^2)$.
- $\forall a\exists x,y,x',y'(xx'=yy'=1\wedge a^3x^2=ay^2)$.
- $\forall a,b\exists x,y,z,x',y',z'(xx'=yy'=zz'=1\wedge ax^2=ay^2+a^2bz^2)$.

ii) The Proposition 5.6 of [31] shows that the von Neumann regular ring A is the ring of global sections over a Boolean space where the sheaf has fields with 2 invertible as stalks.

Thus, the Proposition 3.2-(d), [31], applied to the sheaf of item ii) above implies that formulas of item i) are valid in A. Therefore $A/_mA^{\times 2}$ is a quadratic multiring.

Example 2.5.12 (Faithfully Quadratic Rings). *Now, we relate our DM-multirings, DP-multirings and quadratic multirings with faithfully quadratic rings as presented in [32]: let A be a semi-real ring with $2\in\dot{A}$, T be a preordering of A or $T=A^2$. A **T-subgroup** of A is a multiplicative subset S of $\dot{A}$ containing $\{-1\}\cup\dot{T}$. For $a,b\in S$, denote*

$$D^v_{S,T}(a,b):=\{c\in S:c=as+bt\text{ for some }s,t\in T\}.$$
$$D^t_{S,T}(a,b):=\{c\in S:c=as+bt\text{ for some }s,t\in\dot{T}\}.$$

*The triple (A,T,S) is **faithfully quadratic** if (among other things) satisfy $D^v_{S,T}(a,b)=D^t_{S,T}(a,b)$ for all $a,b\in S$ (see for instance, Definition 3.1 in [32]). Denote*

$$a^T=b^T\text{ iff }ab\in\dot{T}\text{ iff }b=at\text{ for some }t,$$

and consider $G_T(S) = \{a^T : a \in S\}$. *Define the binary isometry* $\equiv_T^S$ *by*

$$\langle a^T, b^T\rangle \equiv \langle c^T, d^T\rangle \text{ iff } a^T b^T = c^T d^T \text{ and } D^v_{S,T}(a,b) = D^v_{S,T}(c,d).$$

In general, $(G_T(S), \equiv_T^S, -1^T)$ *is a proto-special group. If* (A,T,S) *is faithfully quadratic, then Dickmann and Miraglia showed (see Theorem 3.5[32]) that* $G_T(S)$ *is a special group.*

Now, consider (A,T,S) *and let* $R = A/_m(T \cap nzd(A))$. *Then* $D^t_{S,T}(a,b) \subseteq \overline{a} + \overline{b}$ *for all* $a, b \in A$. *Moreover, if* $A^2 \subseteq nzd(A)$, *or more generally, if* (A,T) *is a quadratic ring, then* R *is a quadratic multiring containing the proto special group* $G_T(S)$. *This is particularly useful given that* (A,T,S) *is not necessarily faithfully quadratic.*

Definition 2.5.13. *Let* (X,τ) *be a topological space. The topology* τ *is called perfectly normal if it is normal and every closed set is* G_δ*-set. The topology* τ *is called* T_6 *if it is Hausdorff and perfectly normal.*

Example 2.5.14.

- *A* T_1 *topological space* X *is perfectly normal if, and only if, for every closed set* F *exists a continuous function* $f\colon X \to \mathbb{R}$ *such that* $F = f^{-1}(0)$ *(Theorem 1.5.19 of [35]).*
- *Every metric space is* T_6 *(Corollary 4.1.13 of [35]).*

`contf`

Example 2.5.15 (The ring of continuous functions)**.** *Let* X *be* T_6 *topological space and consider* $A = C(X,\mathbb{R})$, *the ring of continuous functions* $f : X \to \mathbb{R}$. *Let* $T = A^2 \cap nzd(A)$. *In the following, is proved that* $C(X,\mathbb{R})/_mT$ *is a real reduced multiring (in particular, a quadratic multiring). Before that, consider the remarks:*

- *Since* X *is perfectly normal, given a open set* $U \subseteq X$ *there is a continuous function* $g\colon X \to \mathbb{R}$ *such that* $g\big|_U$ *is strictly positive and* $Z(g) = U^c$.
- $f \in C(X,\mathbb{R})$ *is zero divisor if, and only if,* $Z(f)$ *has non-empty interior. In fact, if* $U \subseteq Z(f)$ *is non-empty interior, then exists* $g \in C(X,\mathbb{R})$ *such that* $Z(g) = U^c$*; thus* g *is a non-zero function and* $fg = 0$. *Reciprocally, if* $Z(f)$ *has empty interior and* $g \in C(X,\mathbb{R})$ *satisfies* $fg = 0$, *then* $Z(f)^c$ *is open and dense while* $Z(f)^c \subseteq Z(g)$. *Since* g *is continuous,* $g = 0$ *and so* f *is non-zero divisor.*
- *By the preceding item,*

$$T = \{f \in C(X,\mathbb{R})\colon f \text{ is non-negative and } Z(f) \text{ has empty interior}\}.$$

Before proceeding with the proof, a notation: given $h \in C(X,\mathbb{R})$, *denote by* $p_h \in C(X,\mathbb{R})$ *any function satisfying:*

- $Z(p_h)$ *has empty interior (i.e.* p_h *is a non-zero divisor).*
- p_h *is non-negative over* $Z(h)$.
- *For all* $x \notin Z(h)$, $p_h(x) = h(x)$.

A possible construction is to consider a positive function $p \in C(X,\mathbb{R})$ *with* $Z(p) = (int(Z(h)))^c$ *and set* $p_h := h + p$.

Claim. *Let* $f, g \in C(X,\mathbb{R})$ *be two functions and* $D \subseteq X$ *a dense subset such that for all* $x \in D$, $sgn(f(x)) = sgn(g(x))$. *Then* $\overline{f} = \overline{g}$ *in* $C(X,\mathbb{R})/_mT$.

Proof. Assume that for all $x \in D$, $\operatorname{sgn}(f(x)) = \operatorname{sgn}(g(x))$. Then for all $x \in D$ we have $f(x) \cdot p_{|g|}(x) = g(x) \cdot p_{|f|}(x)$ $(*)$. Since D is a dense subset of X, the equality $(*)$ is true for all real number. Thus, since $p_{|f|}, p_{|g|} \in T$, we have $\overline{f} = \overline{g}$ in $A/_m T$. $\square$

To finalize this Example, we have to prove the axioms of real reduced multiring:

- *Since* $0 \notin T$, *we have* $\overline{1} \neq \overline{0}$ *in* $A/_m T$.
- *For all* $x \in \mathbb{R}$, *we have* $sgn(f^3(x)) = sgn(f(x))$. *Thus by the above claim* $\overline{f}^3 = \overline{f}$ *in* $A/_m T$.
- *Let* $f, g \in A$ *and* $\overline{h} \in \overline{f} + \overline{f}\overline{g}^2$ *in* $A/_m T$. *Then exists* $s_1, s_2, s_3 \in T$ *such that* $hs_1 = fs_2 + fg^2 s_3$. *Thus, for all* $x \in Z(s_1)^c \cap Z(s_2)^c \cap Z(s_3)^c$, *we have*

  . *if* $f(x) = 0$, *then* $h(x) = 0$;
  . *if* $f(x) > 0$, *then* $h(x) > 0$;
  . *if* $f(x) < 0$, *then* $h(x) < 0$.

  Since $Z(s_1)^c \cap Z(s_2)^c \cap Z(s_3)^c$ *is a dense subset, by above claim,* $\overline{h} = \overline{f}$.
- *Let* $f, g \in A$ *and* $\overline{h_1}, \overline{h_2} \in \overline{f} + \overline{g}$ *in* $A/_m T$. *By an argument similar of the preceding item, the signals of* h_1, h_2 *are equal in dense subset and thus* $\overline{h_1} = \overline{h_2}$.

Chapter 3

From Multirings to Superrings

The concept of superring first appears in ([6]). The very first advantage of considering superrings instead of hyperrings is the possibility of built a theory of polynomials and matrices, available for hyperrings but only closed by constructions in superrings. There are many important advances and results in superring theory, and for instance, we recommend for example, the following papers: [3], [5], [6], [4], [49], [54], [51], [50].

Surprisingly we have obtained an interesting theory of matrices, linear systems, vector spaces and algebraic extensions available for a certain subclass of superfields. If R is a full superring, then $M_{m\times n}(R)$ and $R[X]$ are superrings (Theorem 3.2.6 and 3.4.2). We also obtained a kind of simple algebraic extension for a superfield F (Theorem 3.6.12), which culminate in the existence and unicity of a full algebraic extension of a superfield F (Theorems 3.7.3 and 3.7.4). If F is a linearly closed superfield (the system $Ax = 0$ always have a non trivial solution), then we have a well defined dimension theory for the vector spaces over F (Theorem 3.8.21). The main examples of linearly closed superfields are hyperbolic hyperfields (3.8.23) and simple full algebraic extensions over a linearly closed superfield (3.8.25). The linearly closed interpreted in the context of special groups leads to interesting Isotropic (Corollary 3.8.27) and Hyperbolic (Corollary 3.8.28) interpolations.

We finish this Chapter with a quantifier elimination procedure for superfields (Theorem 3.9.3), which is a direct generalization of a result obtained in [19].

3.1 Superrings, Superfields

`superring`

Definition 3.1.1 (Definition 5 in [6]). *An associative superring is a structure* $(S, +, \cdot, -, 0, 1)$ *such that:*

i - $(S, +, -, 0)$ *is a commutative multigroup.*

ii - $(S, \cdot, 1)$ *is a multimonoid.*

iii - 0 *is an absorbing element:* $a \cdot 0 = \{0\} = 0 \cdot a$, *for all* $a \in S$.

iv - *The weak/semi distributive law holds: if* $d \in c.(a + b)$ *and* $e \in (a + b)c$ *then* $d \in ca + cb$ *and* $e \in ac + bc$, *for all* $a, b, c, d, e \in S$.

v - *The rule of signals holds:* $-(ab) = (-a)b = a(-b)$, *for all* $a, b \in S$.

A superdomain is a non-trivial superring without zero-divisors in this new context, i.e. whenever

$$0 \in a \cdot b \text{ iff } a = 0 \text{ or } b = 0$$

A quasi-superfield is a non-trivial superring such that every nonzero element is invertible in this new context[1]*, i.e. whenever*

$$\text{For all } a \neq 0 \text{ exists } b \text{ such that } 1 \in a \cdot b.$$

A superfield is a quasi-superfield which is also a superdomain. A superring is full if for all $a, b, c, d \in S$*,* $d \in c \cdot (a + b)$ *iff* $d \in ca + cb$*.*

A superring, superdomain or superfield is commutative (associative) if $(S, \cdot, 1)$ *is respectively commutative (associative).*

From now on, all superrings will be commutative (with exceptions sinalized).

Example 3.1.2. *Every multiring can be seen as a superring, in the very same fashion of 1.2.9(a). Our main example of superring is the superring of multipolynomials* $R[X]$ *over a multiring* R*. The construction will be presented in short in Section 3.4. For more details, see [15], [6] or [11].*

Now we treat about morphisms.

Definition 3.1.3. *Let* A *and* B *superrings. A map* $f : A \to B$ *is a* ***morphism*** *if for all* $a, b, c \in A$*:*

i - $f(0) = 0$*;*

ii - $f(1) = 1$*;*

iii - $f(-a) = -f(a)$*;*

iv - $c \in a + b \Rightarrow f(c) \in f(a) + f(b)$*;*

v - $c \in a \cdot b \Rightarrow f(c) \in f(a) \cdot f(b)$*.*

A morphism f *is* ***a full morphism*** *if for all* $a, b \in A$*,*

$$f(a + b) = f(a) + f(b) \text{ and } f(a \cdot b) = f(a) + f(b).$$

From now on, we use the following conventions: Let $(R, +, \cdot, -, 0, 1)$ be a superring, $p \in \mathbb{N}$ and consider a p-tuple $\vec{a} = (a_0, a_1, ..., a_{p-1})$. We define the finite sum by:

$$x \in \sum_{i<0} a_i \text{ iff } x = 0,$$
$$x \in \sum_{i<p} a_i \text{ iff } x \in y + a_{p-1} \text{ for some } y \in \sum_{i<p-1} a_i, \text{if } p \geq 1.$$

and the finite product by:

$$x \in \prod_{i<0} a_i \text{ iff } x = 1,$$
$$x \in \prod_{i<p} a_i \text{ iff } x \in y \cdot a_{p-1} \text{ for some } y \in \prod_{i<p-1} a_i, \text{if } p \geq 1.$$

Thus, if $(\vec{a}_0, \vec{a}_1, ..., \vec{a}_{p-1})$ is a p-tuple of tuples $\vec{a}_i = (a_{i0}, a_{i1}, ..., a_{im_i})$, then we have the finite

[1]For a quasi-superfield F, we **are not imposing** that $(S \setminus \{0\}, \cdot, 1)$ will be a commutative multigroup, i.e, that if $d \in a \cdot b$ then $b^{-1} \in a \cdot d^{-1}$.

sum of finite products:

$$x \in \sum_{i<0} \prod_{j<m_i} a_{ij} \text{ iff } x = 0,$$

$$x \in \sum_{i<p} \prod_{j<m_i} a_{ij} \text{ iff } x \in y + z \text{ for some } y \in \sum_{i<p-1} \prod_{j<m_i} a_{ij} \text{ and } z \in \prod_{j<m_{p-1}} a_{p-1,j}, \text{if } p \geq 1.$$

Remark 3.1.4. *Note that, in this sense, we have (for example) that*

$$\prod_{j=1}^{4} a_j = ((a_1 a_2) a_3) a_4.$$

lembasic1

Lemma 3.1.5 (Basic Facts)**.** *Let A be a superring.*

a - *For all $n \in \mathbb{N}$ and all $a_1, ..., a_n \in A$, the sum $a_1 + ... + a_n$ does not depends on the order of the entries, and if is A is associative, the product $a_1 \cdot ... \cdot a_n$ also does not depends on the order of the entries.*

b - *If A is a full superdomain, then $ax = ay$ for some $a \neq 0$ imply $x = y$.*

c - *If A is full, then for all $d, a_1, ..., a_n \in A$*

$$d(a_1 + ... + a_n) = da_1 + ... + da_n.$$

d - *Suppose A is a full superdomain and let $a \in A \setminus \{0\}$. If $1 \in (a \cdot b) \cap (a \cdot c)$ then $b = c$.*

e - *(Newton's Binom Formula) For $n \geq 1$ and $X \subseteq A$ denote*

$$nX := \sum_{i=1}^{n} X.$$

Then for $A, B \subseteq A$,

$$(A + B)^n \subseteq \sum_{j=0}^{n} \binom{n}{j} A^j B^{n-j}.$$

Proof.

a - It is an immediate consequence of associativity and induction.

b - Let $ax = ay$ for some $a \neq 0$. Then $ax - ay = ay - ay$. Since A is full, $a(x - y) = ay - ay$, and then,

$$0 \in ay - ay = a(x - y).$$

Moreover, $0 \in az$ for some $z \in x - y$. Since A is a superdomain and $a \neq 0$, $z = 0$. Then $0 \in x - y$, which imply $x = y$.

c - By induction, we only need to proof the case $n = 2$. Let $a, b, c, d \in A$. We already know that $d(a + b + c) \subseteq da + db + dc$. Now consider $x \in da + db + dc$. Then $x \in e + dc$ for some $e \in da + db = d(a + b)$. Then $e \in de'$ with $e' \in a + b$ and $x \in e + dc \subseteq de' + dc = d(e' + c)$. Hence

$$x \in d(e' + c) \subseteq d(a + b + c).$$

d - Let $1 \in (a \cdot b) \cap (a \cdot c)$. Then

$$0 \in 1 - 1 \subseteq (a \cdot b) - (a \cdot c) = a \cdot (b - c).$$

Since $0 \in a \cdot (b - c)$ and $a \neq 0$ we have $0 \in b - c$, which imply $b = c$.

e - By induction is enough to prove the case $n = 2$. We have

$$\begin{aligned}(A+B)^2 &:= (A+B)(A+B) \subseteq A(A+B) + B(A+B) \subseteq A^2 + AB + BA + B^2 \\ &= A^2 + AB + AB + B^2 = A^2 + 2AB + B^2 := \sum_{j=0}^{2} \binom{n}{j} A^j B^{n-j}.\end{aligned}$$

$\square$

factstrong2

Lemma 3.1.6 (Facts about full morphisms of superrings). *Let $f : A \to B$ be a full morphism of superrings. Then*

a - For all $a_1, ..., a_n \in A$,

$$f(a_1 + ... + a_n) = f(a_1) + ... + f(a_n).$$

b - For all $a_1, ..., a_n, b_1, ..., b_n \in A$,

$$f[(a_1 + b_1)(a_2 + b_2)...(a_n + b_n)] = (f(a_1) + f(b_1))(f(a_2) + f(b_2))...(f(a_n) + f(b_n)).$$

c - For all $c_1, ..., c_n, d_1, ..., d_n \in A$,

$$f(c_1 d_1 + c_2 d_2 + ... + c_n d_n) = f(c_1)f(d_1) + f(c_2)f(d_2) + ... + f(c_n)f(d_n).$$

d - For all $a_0, ..., a_n, \alpha \in A$,

$$f(a_0 + a_1\alpha + ... + a_n\alpha^n) = f(a_0) + f(a_1)f(\alpha) + ... + f(a_n)f(\alpha)^n.$$

Here we always interpret $ab^n := a(b^n)$, unless stated contrary.

e - Let A_1, A_2, A_3 be superrings with injective morphisms (embeddings) $i_{12} : A_1 \to A_2$, $i_{13} : A_1 \to A_3$ and $i_{23} : A_2 \to A_3$.

$$\begin{tikzcd} A_1 \arrow[r, "i_{12}"] \arrow[dr, "i_{13}"'] & A_2 \arrow[d, "i_{23}"] \\ & A_3 \end{tikzcd}$$

Suppose that $i_{13} = i_{23} \circ i_{12}$ is a full embedding. If i_{23} is a full embedding then i_{12} is a full embedding.

char

Definition 3.1.7.

*i - The **characteristic** of a superring is the smaller integer $n \geq 1$ such that*

$$0 \in \sum_{i<n} 1,$$

otherwise the characteristic is zero. For full superdomains, this is equivalent to say that n is the smaller integer such that

$$\text{For all } a,\ 0 \in \sum_{i<n} a.$$

ii - *An* ***ideal*** *of a superring A is a non-empty subset $\mathfrak{a}$ of A such that $\mathfrak{a}+\mathfrak{a} \subseteq \mathfrak{a}$ and $A\mathfrak{a} \subseteq \mathfrak{a}$. We denote*

$$\mathfrak{I}(A) = \{I \subseteq A : I \text{ is an ideal}\}.$$

iii - *Let S be a subset of a superring 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

$$\langle a_1, ..., a_n \rangle = \sum Aa_1 + ... + \sum Aa_n, \text{ where } \sum Aa = \bigcup_{n\geq 1} \{\underbrace{Aa + ... + Aa}_{n \text{ times}}\}.$$

Note that if A is a full superring, then $\sum Aa = Aa$.

iv - *An ideal $\mathfrak{p}$ of A is said to be* ***prime*** *if $1 \notin \mathfrak{p}$ and $ab \subseteq \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. We denote*

$$Spec(A) = \{\mathfrak{p} \subseteq A : \mathfrak{p} \text{ is a prime ideal}\}.$$

v - *An ideal $\mathfrak{p}$ of A is said to be* ***strongly prime*** *if $1 \notin \mathfrak{p}$ and $ab \cap \mathfrak{p} \neq \emptyset \Rightarrow a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. We denote*

$$Spec_s(A) = \{\mathfrak{p} \subseteq A : \mathfrak{p} \text{ is a strongly prime ideal}\}.$$

Note that every strongly prime ideal is prime.

vi - *An ideal $\mathfrak{m}$ is maximal if it is proper and for all ideals $\mathfrak{a}$ with $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A$ then $\mathfrak{a} = \mathfrak{m}$ or $\mathfrak{a} = A$.*

vii - *For an ideal $I \subseteq A$, we define operations in the quotient $A/I = \{x+I : x \in A\} = \{\overline{x} : x \in A\}$, by the rules*

$$\overline{x} + \overline{y} = \{\overline{z} : z \in x + y\}$$
$$\overline{x} \cdot \overline{y} = \{\overline{z} : z \in xy\}$$

for all $\overline{x}, \overline{y} \in A/I$.

Remark 3.1.8.

a - *If A is a multiring, then every prime ideal is strongly prime. We do not know if this is the case for general superrings.*

b - *If A is a multiring, then every maximal ideal is prime (Proposition 1.7 of [23]). For a general superring A, we do not know if a maximal ideal is prime.*

c - *In his Ph.D Thesis [23], H. Ribeiro deals with elements* weakly invertible *on a multiring A. This could be an alternative in dealing with the above questions.*

With all conventions and notations above, we obtain the following Lemma, which recover for superrings some properties holding for rings (and multirings).

lem1

Lemma 3.1.9. *Let A be an associative superring and I an ideal.*

i - $I = A$ if and only if $1 \in I$.

ii - A/I is a superring. Moreover, if A is full then A/I is also full.

iii - I is strongly prime if and only if A/I is a superdomain.

If A is full, then

iv - $I = A$ if and only if $1 \in I$, which occurs if and only if $A^* \cap I \neq \emptyset$ (in other words, if and only if I contains an invertible element).

v - A is a superfield if and only if $\mathfrak{I}(A) = \{0, A\}$.

vi - I is maximal if and only if A/I is a superfield.

Proposition 3.1.10. *Let A be an associative superring and I an ideal.*

i - If I is a maximal ideal, then it is prime.

ii - The ideal I is prime if, and only if, A/I is quasi-superdomain[2].

iii - (Prime Ideal Theorem) Let $S \subseteq A$ be a multiplicative set ($1 \in S$ and $S \cdot S \subseteq S$). Suppose that $S \cap I = \emptyset$. Then there is a prime ideal p such that $I \subseteq p$ and $S \cap p = \emptyset$.

Proof.

i - Let $a, b \in A$ with $ab \subseteq I$. Assume that $a \notin I$ and consider the ideal $J = I + (a)$. Then there are $x \in I, t_1, \ldots, t_n \in A$ such that $1 \in x + at_1 + \cdots + at_n$. Thus $b \in bx + bat_1 + \cdots + bat_n \subseteq I$.

ii - If I is prime and $\overline{a} \cdot \overline{b} = \{\overline{0}\}$ in A/I, then $a \cdot b \subseteq I$. Therefore, by primality, $a \in I$ or $b \in I$. Thus $\overline{a} = 0$ or $\overline{b} = 0$ in A/I. Reciprocally, assume A/I a quasi-superdomain and let $a, b \in A$ with $ab \subseteq I$. Then $\overline{a} \cdot \overline{b} = \{\overline{0}\}$ and by hypothesis follows $a \in I$ or $b \in I$, as desired.

iii - Consider the partial order $\mathcal{X} = \{J \subseteq A\colon J \text{ is an ideal and } S \cap J = \emptyset\}$ ordered by inclusion. Since the directed union of ideals is again an ideal, we have by Zorn's Lemma that $\mathcal{X}$ has a maximal element p. Suppose that p is not prime, that it, there is $a, b \in$ with $ab \subseteq p$ and $a, b \notin p$. Now notice that $J_a = p + (a)$ and $J_b = p + (b)$ are ideals that proper extend p. Hence, by maximality, there are $s, v \in S, x, y \in p, t_1, \ldots, t_n, w_1, \ldots, w_k \in A$ with

$$s \in x + at_1 + \cdots + at_n$$
$$v \in y + bw_1 + \cdots + bw_k.$$

These equations implies that

$$sv \subseteq xy + xbw_1 + \cdots + xbw_k + yat_1 + \cdots + yat_n + \sum_{i,j} abt_i w_j \subseteq S \cap p,$$

a contradiction. Then p is prime.

□

[2] A superring B is called quasi-superdomain if given $a, b \in B$ with $ab = \{0\}$, then $a = 0$ or $b = 0$

3.2 Matrices and determinants over commutative superrings

Definition 3.2.1. *Let m, n be positive integers. A $m \times n$ **matrix** over a commutative superring R is a double sequence A of elements of F, distributed in m rows and n columns. The set of $m \times n$ matrices is denoted by $M_{m\times n}(R)$. When $m = n$, we denote $n \times n$ matrices by $M_n(R)$.*

A matrix $A \in M_{m\times n}(R)$ is represented simply by $A = (a_{ij})$ (with m and n subscript if necessary) or by a table as below:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

For $A, B \in M_{n\times m}(R)$ and $\lambda \in R$ with $A = (a_{ij})$ and $B = (b_{ij})$ we define $-A = (-a_{ij})$ and (multi) operations

$$A + B := \{(d_{ij}) : d_{ij} \in a_{ij} + b_{ij} \text{ for all } i, j\} \neq \emptyset$$

and

$$\lambda A = \{(d_{ij}) : d_{ij} \in \lambda a_{ij} \text{ for all } i, j\}.$$

If $A \in M_{n\times m}(R)$ with $A = (a_{ij})$ and $B \in M_{m\times p}(R)$ with $B = (a_{ij})$, we define

$$A \cdot B = AB \subseteq M_{n\times p}(R)$$

by

$$AB = \{(d_{ij}) : d_{ij} \in \sum_{k=1}^{n} a_{ik}b_{kj} = a_{i1}b_{1j} + a_{i2}b_{2j} + ... + a_{in}b_{nk} \text{ for all } i, j\} \neq \emptyset.$$

We denote $0 = (0_{ij}) \in M_{m\times n}(R)$ and $1 = (\delta_{ij})_{ij} \in M_n(R)$ the usual zero and identity matrices respectively.

We say that $A \in M_n(R)$ is **invertible** iff there exist $B \in M_n(R)$ with $1 \in AB$ and $1 \in BA$.

Of course, we adopt freely the usual simplified notation from commutative algebra. For example for $A = (a_{ij})$ and $B = (b_{ij})$ we simply write

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \dots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \dots & a_{2n}+b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \dots & a_{mn}+b_{mn} \end{pmatrix}$$

with the analogous simplifications for λA and AB.

Example 3.2.2. *Consider $X_2 = \{-2, -1, 0, 1, 2\}$ as in Example 1.2.12 and matrices $A, B, C \in M_2(X_2)$ given by*

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \text{ and } C = \begin{pmatrix} 2 & 0 \\ -1 & 2 \end{pmatrix}.$$

With our notations we have

$$A+B=\begin{pmatrix}1-1 & 1+1\\ 0+0 & 1-1\end{pmatrix}=$$
$$\left\{\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix},\begin{pmatrix}-1 & 1\\ 0 & 0\end{pmatrix},\begin{pmatrix}-1 & 1\\ 0 & 1\end{pmatrix},\begin{pmatrix}0 & 1\\ 0 & -1\end{pmatrix},\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix},\begin{pmatrix}0 & 1\\ 0 & 1\end{pmatrix},\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix},\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix},\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right\}$$

$$A\cdot B=\begin{pmatrix}1\cdot(-1)+1\cdot 0 & 1\cdot 1+1\cdot(-1)\\ 0\cdot(-1)+1\cdot(0) & 0\cdot 1+1\cdot(-1)\end{pmatrix}=\begin{pmatrix}-1 & 1-1\\ 0 & -1\end{pmatrix}=$$
$$\left\{\begin{pmatrix}-1 & -1\\ 0 & -1\end{pmatrix},\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}\right\}$$

$$A\cdot C=\begin{pmatrix}1\cdot 2+1\cdot(-1) & 1\cdot 0+1\cdot 2\\ 0\cdot 2+1\cdot(-1) & 0\cdot 0+1\cdot 2\end{pmatrix}=\begin{pmatrix}2-1 & 2\\ -1 & 2\end{pmatrix}=\left\{\begin{pmatrix}2 & 2\\ -1 & 2\end{pmatrix}\right\}.$$

Here we will "export" the usual terminology of diagonal, triangular, block and elementary matrices available for fields to superfields.

With these, using the fact that $(R,+,-,0)$ is a commutative multigroup we immediately have the following Theorem.

`matrix1`

Theorem 3.2.3. *Let R be a superring. Then $(M_{m\times n}(R),+,-,0)$ is a commutative multigroup.*

For a general associative superring R, the matrix product in $M_n(R)$ is not associative in general (and of course, $M_n(R)$ is not an associative superring in general).

Example 3.2.4. *Let $R=X_2$ as in Example 1.2.12. Of course, R is not full because, for example,*

$$2(1-1)=\{-2,0,2\} \text{ and } 2-2=R.$$

Now, consider the matrices

$$A=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix},\ B=\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix} \text{ and } C=\begin{pmatrix}2 & 0\\ -1 & 2\end{pmatrix}.$$

In fact we have

$$\begin{aligned}(AB)C&=\left[\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}\right]\begin{pmatrix}2 & 0\\ -1 & 2\end{pmatrix}\\ &=\begin{pmatrix}-1 & 1-1\\ 0 & -1\end{pmatrix}\begin{pmatrix}2 & 0\\ -1 & 2\end{pmatrix}=\begin{pmatrix}-2-(1-1) & 2(1-1)\\ 1 & -2\end{pmatrix}\end{aligned}$$

and

$$\begin{aligned}A(BC)&=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\left[\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}\begin{pmatrix}2 & 0\\ -1 & 2\end{pmatrix}\right]\\ &=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}-2-1 & 2\\ 1 & -2\end{pmatrix}=\begin{pmatrix}(-2-1)+1 & 2-2\\ 1 & -2\end{pmatrix}.\end{aligned}$$

Then we have $(AB)C\neq A(BC)$.

Despite the fact that $M_n(R)$ is not an associative superring in general, it is a structure of interest (as we will see, for example, in Theorem 3.6.12) and in the following Lemma we collect the properties holding for the product in the general case.

`matrix2`

Lemma 3.2.5. *Let R be a superring and A, B, C matrices in $M_n(R)$. Then:*

a - $A \cdot 0 = 0 \cdot A = \{0\}$.

b - If $m = n$, then $A \cdot 1 = 1 \cdot A = \{A\}$.

c - If $A(B + C) \subseteq AB + AC$, with equality if R is full.

d - $(B + C)A \subseteq BA + CA$, with equality if R is full.

e - If R is associative and full, then $(AB)C = A(BC)$.

Firstly, let us explicit the notation for AB: we write

$$AB = \begin{pmatrix} D_{11} & D_{12} & \dots & D_{1n} \\ D_{21} & D_{22} & \dots & D_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ D_{m1} & D_{m2} & \dots & D_{mn} \end{pmatrix}$$

or $AB = (D_{ij})$ where for all i, j, D_{ij} is the set

$$D_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = a_{i1}b_{1j} + a_{i2}b_{2j} + ... + a_{in}b_{nk} \text{ (of course, this is an equality of sets).}$$

Alternatively, we can proceed more directly, simply writing

$$AB = \begin{pmatrix} \sum_{k=1}^{n} a_{1k}b_{k1} & \sum_{k=1}^{n} a_{1k}b_{k2} & \dots & \sum_{k=1}^{n} a_{1k}b_{kn} \\ \sum_{k=1}^{n} a_{2k}b_{k1} & \sum_{k=1}^{n} a_{2k}b_{k2} & \dots & \sum_{k=1}^{n} a_{2k}b_{kn} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^{n} a_{mk}b_{k1} & \sum_{k=1}^{n} a_{mk}b_{k2} & \dots & \sum_{k=1}^{n} a_{mk}b_{kn} \end{pmatrix}$$

Now we proceed with the proof of the Lemma.

Proof of Lemma 3.2.5. The argument here is in fact very similar to those one used in linear algebra over fields.

a - Let $A \cdot 0 = (D_{ij})$ (as explained above). For all i, j we have

$$D_{ij} = \sum_k a_{ik}0_{kj} = \sum_k a_{ik} \cdot 0 = \sum_k 0 = 0.$$

Then $A \cdot 0 = \{0\}$. The same reasoning provide $0 \cdot A = \{0\}$.

b - Let $A \cdot 1 = (D_{i,j})$. Since $1 = (\delta_{i,j})$ with $\delta_{i,j} \in \{0, 1\}$ and $\delta_{i,j} = 1$ iff $i = j$, we have

$$D_{i,j} = \sum_k a_{i,k}\delta_{k,j} = a_{i,j} \cdot 1 = \{a_{i,j}\}.$$

Thus, $A \cdot 1 = \{A\}$. Similarly, $1 \cdot A = \{A\}$.

c -

$$\begin{aligned}
A(B+C) &= (a_{i,j})_{i,j} \cdot (b_{i,j}+c_{i,j})_{i,j} \\
&= \left(\sum_k a_{i,k}(b_{k,j}+c_{k,j})\right)_{i,j} \\
&\subseteq \left(\sum_k a_{i,k}b_{k,j}+a_{i,k}c_{k,j}\right)_{i,j} \\
&= \left(\sum_k a_{i,k}b_{k,j}\right)_{i,j} + \left(\sum_k a_{i,k}c_{k,j}\right)_{i,j} = AB+AC.
\end{aligned}$$

When R is full, it is immediate from above that $A(B+C)=AB+AC$.

d - Similar argument as above.

e - Assume that R is associative and full. Then

$$\begin{aligned}
(AB)C &= \left[(a_{i,j})_{i,j} \cdot (b_{i,j})_{i,j}\right] \cdot (c_{i,j})_{i,j} \\
&= \left(\sum_k a_{i,k}b_{k,j}\right)_{i,j} \cdot (c_{i,j})_{i,j} \\
&= \left(\sum_l \left(\sum_k a_{i,k}b_{k,l}\right) \cdot c_{l,j}\right)_{i,j} \\
&= \left(\sum_l \sum_k a_{i,k}b_{k,l}c_{l,j}\right)_{i,j} \\
&= \left(\sum_k a_{i,k} \cdot \left(\sum_l b_{k,l}c_{l,j}\right)\right)_{i,j} \\
&= (a_{i,j}) \cdot \left(\sum_l b_{i,l}c_{l,j}\right)_{i,j} = A(BC).
\end{aligned}$$

□

In fact, with Theorem 3.2.3 and Lemma 3.2.5 we conclude the following.

matrix3

Theorem 3.2.6. *For a superring R, if R is associative and full then $M_n(R)$ is a full superring, that is non-commutative if $n \geq 2$.*

We also have a generalized version of Lemma 3.2.5 (with the proof similar to the one given there).

matrix4

Lemma 3.2.7. *Let R be a superring and A,B,C,D,E,F matrices with $A \in M_{m\times n}(R)$, $B,C \in M_{n\times p}(R)$, $D,E \in M_{p\times m}(R)$ and $F \in M_{p\times q}(R)$. Then:*

a - $A \cdot 0_{n\times p} = \{0_{m\times p}\}$ and $0_{p\times n} \cdot A = \{0_{p\times n}\}$.

b - $A \cdot 1_{n\times n} = 1_{m\times m} \cdot A = \{A\}$.

c - $A(B+C) \subseteq AB + AC$, with equality if R is full.

d - $(D+E)A \subseteq DA + EA$, with equality if R is full.

e - If R is associative and full, then $(AB)F = A(BF)$.

Despite the fact that full associativity do not hold in $M_n(R)$ for a general superring R, we have the following useful results. We start with a technical Definition:

Definition 3.2.8. *Let R be a superring. We say that R is **proto-full** if for all $a, b, c, d \in R$*

$$[(ab + ac)d] \cap [a(bd + cd)] \neq \emptyset.$$

Lemma 3.2.9. *Let R be an associative and proto-full superring. Then for all $a, b_1, ..., b_n, d \in R$ we have*

$$[(ab_1 + ... + ab_n)d] \cap [a(b_1 d + ... + b_n d)] \neq \emptyset.$$

Then rewriting the proof of Lemma 3.2.7(e) we get the following.

matrix5

Lemma 3.2.10. *Let R be an associative and proto full superring and A, B, C matrices with $A \in M_{m\times n}(R)$, $B \in M_{n\times p}(R)$ and $C \in M_{p\times q}(R)$. Then*

$$[(AB)C] \cap [A(BC)] \neq \emptyset.$$

determinant

Definition 3.2.11. *Let $\mathcal{A} \subseteq M_n(R)$. We define the **determinant** of $\mathcal{A}$ as the* subset $\det(\mathcal{A}) \subseteq R$ *given by the rule*

$$\det(\mathcal{A}) = \bigcup_{A\in\mathcal{A}} \left\{ \sum_{\sigma\in S_n} sgn(\sigma) \prod_{j=1}^{n} a_{j\sigma(j)} \right\}.$$

If $\mathcal{A} = \{A\}$ we simply write $\det(A)$ *for the above formula.*

Lemma 3.2.12 (Properties of Determinant)**.** *Let R be associative and $A, B \in M_n(R)$, $A = (a_{ij})$, $B = (b_{ij})$ and $\lambda \in R$. Then:*

a - $\det(\lambda A) \subseteq \lambda^n \det(A)$, with equality if R is full;

b - if there is an entire row or column of zeros in A then $\det(A) = \{0\}$.

c - if $A = (a_{ij})$ is a triangular matrix (and in particular, diagonal matrix) then $\det(A) = a_{11}a_{22}...a_{nn}$.

Proof.

a - Using the very Definition we get

$$\det(\lambda A) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} (\lambda a_{j\sigma(j)}) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\lambda^n \prod_{j=1}^{n} a_{j\sigma(j)}$$
$$\subseteq \lambda^n \left(\sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} a_{j\sigma(j)} \right) = \lambda^n \det(A)$$

b - In this case we have $0 \in \{a_{1\sigma(1)}, a_{2\sigma(2)}, ..., a_{n\sigma(n)}\}$ for all $n \in S_n$. Then

$$\prod_{j=1}^{n} a_{j\sigma(j)} = \{0\} \text{ for all } \sigma \in S_n,$$

implying $\det(A) = \{0\}$.

c - Follow immediately from Definition 3.2.11.

□

3.3 Linear systems over superfields

Throughout this entire Section fix a superfield F.

lin-equation

Definition 3.3.1. *A **linear equation** is an equation (term in the language of superfields) of type*

$$Ax \subseteq B$$

where $A \in M_{1\times n}(F)$ ($n \in \mathbb{N}$), x is a $n \times 1$ vector of variables and $B \subseteq F$.

Remark 3.3.2. *We are defining "linear equations" (and more lately, "linear systems") in terms of matrices. We do this because for superfields we cannot agglutinate scalars and variables as we do in general linear algebra. For example, there is no reason for "$a_1x_1 + b_1x_1$" be equal to "$(a_1 + b_1)x_1$"*[3].

Despite this Remark, given a linear equation $Ax \subseteq B$, we can "colloquially" write

$$a_1x_1 + a_2x_2 + ... + a_nx_n \subseteq B,$$

with $a_1, ..., a_n \in F$. Of course, we could consider the equation

$$a_1x_1 + a_2x_2 + ... + a_nx_n \supseteq B$$

as a linear one and proceed with two types of linear equations. But the type considered in 3.3.1 seems to be (at first sight) more "natural".

We can use to this "coloquial" to write our equations (and further, systems), and while we are dealing with one equation (system), we will proceed with this "coloquial" language. But in order to get more general proofs and Definitions, we will always proceed with matrices.

Definition 3.3.3. *A **solution (weak solution)** of a linear equation $Ax \subseteq B$, is a matrix $d \in M_{n\times 1}(F)$ such that $Ad \subseteq B$ ($Ad \cap B \neq \emptyset$).*

Definition 3.3.4. *A **linear system** is a conjunction of equations (term in the language of superfields) of type*

$$Ax \subseteq B$$

where $A \in M_{m\times n}(F)$ ($n \in \mathbb{N}$), x is a $n \times 1$ vector of variables and $B \subseteq M_{m\times 1}(F)$.

[3]Or saying in another words, in order to obtain $a_1x_1 + b_1x_1 = (a_1 + b_1)x_1$ we should Define what would be a "full" variable, which is not a standard procedure in logic.

In this sense, a Linear system can be colloquially represented as usual

$$S:\begin{cases} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n \subseteq B_1 \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n \subseteq B_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n \subseteq B_m \end{cases}$$

A **(weak) solution** of a Linear system is a tuple $(d_1, ..., d_n)$ such that $Ad \subseteq B$ ($Ad \cap B \neq \emptyset$).

Definition 3.3.5. *A Linear system $Ax \subseteq B$ is **scaled** if A is a upper triangular matrix.*

In the usual representation, a scaled linear system has the form:

$$\begin{cases} a_{1r_1}x_1 + \qquad\qquad ... \quad + a_{1n}x_n \subseteq B_1 \\ \qquad a_{2r_2}x_2 + \qquad ... \quad + a_{1n}x_n \subseteq B_2 \\ \vdots \\ \qquad\qquad a_{nr_k}x_k + \quad ... \quad + a_{nn}x_n \subseteq B_k \end{cases}$$

with $r_j \geq 1$, and $a_{jr_j} \neq 0$, $j = 1, ..., k$ e $r_1 < r_2 < ... < r_k$. For a scaled system we have three situations:

I - The last equation is of type

$$0x_1 + ... + 0x_n \subseteq B_p \text{ with } 0 \notin B_p.$$

In this case S is impossible.

II - There is no equation of type (I) and $p = n$.

III - There is no equation of type (I) and $p < n$.

Suppose S of type (II). Then we have a situation

$$\begin{cases} a_{11}x_1 + \qquad\qquad ... \quad + a_{1n}x_n \subseteq B_1 \\ \qquad a_{23}x_3 + \qquad ... \quad + a_{2n}x_n \subseteq B_2 \\ \vdots \\ \qquad\qquad\qquad ... + a_{nn}x_n \subseteq B_n \end{cases}$$

with $a_{ii} \neq 0$ for all $i = 1, ..., n$. Getting $x_1, ..., x_n$ recursively by suitable choices

rec-sol

$$\begin{cases} x_n & \in a_{nn}^{-1}B_n \\ x_k & \in a_{kk}^{-1}B_k - [a_{kk}^{-1}a_{k(k+1)}]x_{k+1} - ... - [a_{kk}^{-1}a_{kn}]x_n \text{ for } k = n-1, ..., 1 \end{cases} \tag{3.1}$$

we have a weak solution of the system S (this solution is weak basically because $a_{kk}^{-1}a_{kn}$ is not a singleton in general). The same reasoning shows that for a scaled system of type (III), we can find a parametric weak solution for the system.

sistem-solved

Example 3.3.6. *Consider $n = 2$ and the system over an associative superfield F,*

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \subseteq \begin{pmatrix} D_1 \\ D_2 \end{pmatrix}$$

or in our "coloquial" representation, the system

$$\begin{cases} ax + by \subseteq D_1 \\ \qquad cy \subseteq D_2 \end{cases} \quad \text{with } a, c \neq 0.$$

Since $D_2 \subseteq c(c^{-1}D_2)$, for all $d_2 \in D_2$ there exist $z \in c^{-1}D_2$ with $d_2 \in cz$. Pick $y_0 = z$. So we have

$$cy_0 \subseteq c(c^{-1}D_2) \text{ with } cy_0 \cap D_2 \neq \emptyset.$$

Hence we get $y_0 \in c^{-1}D_2$ and we can choose $x_0 \in a^{-1}D_1 - by_0$ in order to obtain

$$ax_0 + by_0 \subseteq a(a^{-1}D_1 - by_0) + by_0 \subseteq aa^{-1}D_1 - aa^{-1}by_0 + by_0 \text{ and } ax_0 + by_0 \cap D_1 \neq \emptyset.$$

Of course, linear systems over superfields yields to more flexibility than linear systems over fields. It is "easier" to get a weak solution of a linear systems over superfields than over a field as we see in the Example below.

Example 3.3.7. *Let $F = \mathbb{Q}/_m\mathbb{Q}^{*2}$. We have $2, 5 \notin D(\langle 1, 1\rangle)$, because $2 = 1 \cdot 1^2 + 1 \cdot 1^2$ and $5 = 1 \cdot 2^2 + 1 \cdot 1^2$. Then $\overline{2}, \overline{5} \in \overline{1} + \overline{1}$ and the system*

$$\begin{cases} x + y \subseteq \{\overline{1}\} \\ \qquad y \subseteq \{\overline{5}\} \end{cases}$$

over F has at least a weak solution $x = y = 1$.

Definition 3.3.8 (Elementary Operations)**.** *Let $A \in M_{m\times n}(F)$. The **elementary operations are**:*

*I - **Permute** lines i e j; which will be indicated by $L_i \leftrightarrow L_j$;*

*II - **Multiply** each coefficient of a line i by an element $\lambda \neq 0$ in F; which will be indicated by $L_i \leftarrow \lambda L_i$;*

*III - **Sum** line i with line j and keep the result in line i; which will be indicated by $L_i \leftarrow L_i + L_j$.*

Of course, given a linear system $Ax \subseteq B$, we generate more than one system after the application of a sequence of elementary operations on the matrices A and B. We denote the systems obtained by a set of systems $Ax \subseteq B$ (with $A \subseteq M_{m\times n}(F)$, $B \subseteq M_{m\times 1}(F)$) after the sequence of elementary operations $O = \{o_1, ..., o_n\}$ by $(Ax \subseteq B)^O$.

The elementary operations defined above could be described in terms of matrix multiplication (as we usually do for fields). For example, considering the matrix $A \in M_{2\times 2}(F)$ given by

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

the application of $L_1 \leftrightarrow L_2$ is just

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & d \\ a & b \end{pmatrix}$$

If R is a proto-full superfield, to realize an elementary operation on the system $Ax \subseteq B$ is equivalent to multiply A and B by an elementary matrix[4] $E \in M_{m\times m}(F)$ in order to obtain the system $(EA)x \subseteq (EB)$.

element-sol

Lemma 3.3.9. *Let $Ax \subseteq B$ be a set of Linear systems and $O = \{o_1, ..., o_n\}$. Then every solution of a system in $Ax \subseteq B$ is a solution in some system in $(Ax \subseteq B)^O$. If F is full, then every weak solution of a system in $Ax \subseteq B$ is a weak solution in some system in $(Ax \subseteq B)^O$.*

Proof. We only need to deal with the elementary operations. Consider a system

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & d_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \subseteq \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix}$$

We already know that operations (I) and (II) preserves solutions. Now consider without loss of generalization the elementary operation $L_1 \leftarrow L_1 + L_2$. Then we arrive at the set of systems

$$\begin{pmatrix} a_{11}+a_{21} & a_{12}+a_{22} & \dots & a_{1n}+a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & d_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \subseteq \begin{pmatrix} B_1+B_2 \\ B_2 \\ \vdots \\ B_n \end{pmatrix}$$

If we get $d_1, ..., d_n$ with

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & d_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} \subseteq \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix}$$

in particular

$$(a_{11}d_1 + ... + d_{1n}d_n) + (a_{21}d_1 + ... + d_{2n}d_n) \subseteq B_1 + B_2,$$

and

$$\begin{pmatrix} a_{11}+a_{21} & a_{12}+a_{22} & \dots & a_{1n}+a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & d_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} \subseteq \begin{pmatrix} B_1+B_2 \\ B_2 \\ \vdots \\ B_n \end{pmatrix}$$

proving (after induction) that every solution of $Ax \subseteq B$ is a solution $(Ax \subseteq B)^O$. For the weak solution part, suppose F is full and $d_1, ..., d_n$ with

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & d_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} \cap \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix} \neq \emptyset$$

[4]Elementary matrices are a standard topic in many Linear Algebra books, but for a quick reference, consult `https://en.wikipedia.org/wiki/Elementary_matrix`.

In particular

$$[(a_{11}+a_{21})d_1+...+(a_{1n}+a_{2n})d_n]=(a_{11}d_1+...+d_{1n}d_n)+(a_{21}d_1+...+d_{2n}d_n)\cap(B_1+B_2)\neq\emptyset,$$

and

$$\begin{pmatrix} a_{11}+a_{21} & a_{12}+a_{22} & \dots & a_{1n}+a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & d_{m2} & \dots & a_{mn} \end{pmatrix}\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix}\cap\begin{pmatrix} B_1+B_2 \\ B_2 \\ \vdots \\ B_n \end{pmatrix}\neq\emptyset.$$

proving (after induction) that every weak solution of $Ax\subseteq B$ is weak a solution $(Ax\subseteq B)^O$. □

Given a system $Ax\subseteq B$, we can obtain a set of scaled systems $(Ax\subseteq B)^{scaled}$, after a finite sequence of elementary operations in the same way as usual. Unfortunately, despite the result obtained in Lemma 3.3.9 we do not know if solutions of $(Ax\subseteq B)^{scaled}$ are solutions of $Ax\subseteq B$.

From now on, given a system $Ax\subseteq B$, **to solve** $Ax\subseteq B$ will have the meaning **to find a weak solution of** $Ax\subseteq B$, and a $n\times n$ **system** will mean a system $Ax\subseteq B$ with $A\in M_{n\times n}(F)$ (and $B\in M_{n\times 1}(F)$).

Definition 3.3.10. *Let $A=(a_{ij})\in M_n(F)$ and denote $A_i=(a_{i1},...,a_{in})$ the i-th row and $A^j=(a_{1j},...,a_{nj})$ the j-th column We say that A_i is a* ***linear combination*** *of $\{A_1,...,A_{i-1},A_{i+1},...,A_n\}$ if there exist $a_1,...,a_{i-1},a_{i+1},...,a_n\in F$ such that*

$$A_i\cap\left[\left(\sum_{j=1}^{r_1}\lambda_{j1}\right)A_1+...+\left(\sum_{j=1}^{r_{i-1}}\lambda_{j(i-1)}\right)A_{i-1}+\left(\sum_{j=1}^{r_{i+1}}\lambda_{j(i+1)}\right)A_{i+1}+...+\left(\sum_{j=1}^{r_n}\lambda_{jn}\right)A_n\right]\neq\emptyset.$$

`scal4`

Lemma 3.3.11. *Let F be a superfield and $A\in M_n(F)$ a upper triangular matrix. Then A is invertible iff $0\notin\det(A)$.*

Proof. Let

$$A=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}$$

We already know that $\det(A)=a_{11}a_{22}...a_{nn}$. Then, we need to prove that A is invertible iff $a_{ii}\neq 0$ for all $i=1,2,...,n$.

Now, let $B\in M_n(F)$ be another upper triangular matrix, saying

$$B=\begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ 0 & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & b_{nn} \end{pmatrix}$$

We also know that

$$AB=\begin{pmatrix} a_{11}b_{11} & a_{11}b_{12}+a_{12}b_{22} & a_{11}b_{13}+a_{12}b_{23}+a_{13}b_{33} & \dots & \sum_{k=1}^n a_{1k}b_{kn} \\ 0 & a_{22}b_{22} & a_{22}b_{23}+a_{23}b_{33} & \dots & \sum_{k=2}^n a_{2k}b_{kn} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_{nn}b_{nn} \end{pmatrix}$$

and

$$BA = \begin{pmatrix} b_{11}a_{11} & b_{11}a_{12}+b_{12}a_{22} & b_{11}a_{13}+b_{12}a_{23}+b_{13}a_{33} & \dots & \sum_{k=1}^{n} b_{1k}a_{kn} \\ 0 & b_{22}a_{22} & b_{22}a_{23}+b_{23}a_{33} & \dots & \sum_{k=2}^{n} b_{2k}a_{kn} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & b_{nn}a_{nn} \end{pmatrix}$$

Then, if $a_{ii}=0$ for some $i\in\{1,2,...,n\}$, we have $I_n\notin AB\cap BA$ for all $B\in M_n(F)$. This is enough to prove that A cannot be invertible.

Now, suppose $a_{ii}\neq 0$ for all $i=1,2,...,n$. We will choose the elements b_{ij} in order to get

$$I_n\in AB\cap BA.$$

First, choose $b_{ii}=a_{ii}^{-1}$. Then, considering $AB=(P_{ij})$ and $BA=(Q_{ij})$, we want to get $0\in P_{ij}$ and $0\in Q_{ij}$ for all $i\neq j$. We need to choose $b_{(n-1)n}$ in order to get

$$\begin{aligned} &0\in a_{(n-1)(n-1)}b_{(n-1)n}+a_{(n-1)n}b_{nn} \text{ and}\\ &0\in b_{(n-1)(n-1)}a_{(n-1)n}+b_{(n-1)n}a_{nn}. \end{aligned}$$

Then (remember that $b_{ii}=a_{ii}^{-1}$) we need

$$b_{(n-1)n}\in -[a_{(n-1)n}a_{(n-1)(n-1)}^{-1}]a_{nn}^{-1}.$$

Then we choose $b_{nn},b_{(n-1)(n-1)}$ and $b_{(n-1)n}$ (i,e, we complete the process for the n-th and $(n-1)$-th rows of B).

Now, we need to choose $b_{(n-2)(n-1)}$ and $b_{(n-2)n}$ in order to get

$$\begin{aligned} &0\in a_{(n-2)(n-2)}b_{(n-2)(n-1)}+a_{(n-2)(n-1)}b_{(n-1)(n-1)}+a_{(n-2)n}b_{n(n-1)} \text{ and}\\ &0\in a_{(n-2)(n-2)}b_{(n-2)n}+a_{(n-2)(n-1)}b_{(n-1)n}+a_{(n-2)n}b_{nn} \end{aligned}$$

and

$$\begin{aligned} &0\in b_{(n-2)(n-2)}a_{(n-2)(n-1)}+b_{(n-2)(n-1)}a_{(n-1)(n-1)}+b_{(n-2)n}a_{n(n-1)} \text{ and}\\ &0\in b_{(n-2)(n-2)}a_{(n-2)n}+b_{(n-2)(n-1)}a_{(n-1)n}+b_{(n-2)n}a_{nn} \end{aligned}$$

Picking $b_{(n-2)(n-1)}$ and $b_{(n-2)n}$ such that

$$\begin{aligned} b_{(n-2)n}&\in -[a_{(n-2)(n-2)}^{-1}a_{(n-2)(n-1)}]b_{(n-1)n}-[a_{(n-2)(n-2)}^{-1}a_{(n-2)n}]b_{nn} \text{ and}\\ b_{(n-2)(n-1)}&\in -[a_{(n-2)(n-2)}^{-1}a_{(n-2)(n-1)}]b_{(n-1)(n-1)}-[a_{(n-2)(n-2)}^{-1}a_{(n-2)n}]b_{n(n-1)} \end{aligned}$$

we complete the process for the n-th, $(n-1)$-th and $(n-2)$-th rows of B. Repeating this process more $n-3$ times we arrive at a matrix B such that $I_n\in AB\cap BA$, as desired. □

3.4 Multipolynomials

secpol

Even if the rings-like multi-algebraic structure have been studied for more than 70 years, the developments of notions of polynomials in the ring-like multialgebraic structure seems to have a more significant development only from the last decade: for instance in [41] some notion of multi polynomials is introduced to obtain some applications to algebraic and tropical geometry, in [6] a more detailed account of variants of concept of multipolynomials over hyperrings is applied to get a form of Hilbert's Basissatz.

Here we will stay close to the perspective in [6]: let $(R,+,-,\cdot,0,1)$ be a superring and set

$$R[X] := \{(a_n)_{n\in\omega} \in R^\omega : \exists t\,\forall n(n \geq t \to a_n = 0)\}.$$

Of course, we define the **degree** of $(a_n)_{n\in\omega} \neq \mathbf{0}$ to be the smallest t such that $a_n = 0$ for all $n > t$.

Now define the binary multioperations $+,\cdot : R[X]\times R[X] \to \mathcal{P}^*(R[X])$, a unary operation $- : R[X] \to R[X]$ and elements $0, 1 \in R[X]$ by

$$\begin{aligned}
(c_n)_{n\in\omega} \in (a_n)_{n\in\omega} + (b_n)_{n\in\omega} &\text{ iff } \forall\, n(c_n \in a_n + b_n)\\
(c_n)_{n\in\omega} \in ((a_n)_{n\in\omega} \cdot (b_n)_{n\in\omega} &\text{ iff } \forall\, n(c_n \in a_0\cdot b_n + a_1\cdot b_{n-1} + ... + a_n\cdot b_0)\\
-(a_n)_{n\in\omega} &= (-a_n)_{n\in\omega}\\
0 &:= (0)_{n\in\omega}\\
1 &:= (1,0,...,0,...)
\end{aligned}$$

For convenience, we denote elements of $R[X]$ by $\alpha = (a_n)_{n\in\omega}$. Beside this, we denote

$$\begin{aligned}
1 &:= (1,0,0,...),\\
X &:= (0,1,0,...),\\
X^2 &:= (0,0,1,0,...)
\end{aligned}$$

etc. In this sense, our "monomial" a_iX^i is denoted by $(0,...0,a_i,0,...)$, where a_i is in the i-th position; in particular, we will denote $\underline{b} = (b,0,0,...)$ and we frequently identify $b \in R \leftrightsquigarrow \underline{b} \in R[X]$.

The properties stated in the Lemma below immediately follows from the definitions involving $R[X]$:

`lemperm`

Lemma 3.4.1. *Let R be a superring and $R[X]$ as above and $n,m \in \mathbb{N}$.*

a - $\{X^{n+m}\} = X^n\cdot X^m$.

b - For all $a \in R$, $\{aX^n\} = \underline{a}\cdot X^n$.

c - Given $\alpha = (a_0,a_1,...,a_n,0,0,...) \in R[X]$, with with $\deg\alpha \leq n$ and $m \geq 1$, we have

$$\alpha X^m = (0,0,...,0,a_0,a_1,...,a_n,0,0,...) = a_0X^m + a_1X^{m+1} + ... + a_nX^{m+n}.$$

d - For $\alpha = (a_n)_{n\in\omega} \in R[X]$, with $\deg\alpha = t$,

$$\{\alpha\} = a_0\cdot 1 + a_1\cdot X + ... + a_t\cdot X^t = a_0 + X(a_1 + a_2X + ... + a_nX^{t-1}).$$

e - $R[X]$ is a non-associative superring. If R is associative and full then $R[X]$ is an associative superring.

f - $R[X]$ is a superdomain iff R is a superdomain.

g - The map $a \in R \mapsto \underline{a} = (a,0,\cdots,0,\cdots)$ defines a full embedding $R \rightarrowtail R[X]$.

h - For an ordinary ring R (identified with a strict superring), the superring $R[X]$ is naturally isomorphic to (the superring associated to) the ordinary ring of polynomials in one variable over R.

Lemma 3.4.1 allow us to deal with the superring $R[X]$ as usual. In other words, we can assume that for $\alpha \in R[x]$, there exists $a_0, a_1, ..., a_n \in R$ such that $\alpha = a_0 + a_1X + ... + a_nX^n$, and then, we can work simply denoting $\alpha = f(X)$, as usual. For example, combining the definitions and all facts above we get

$$(x-a)(x-b) = x^2 + (a-b)x + ab = \{x^2 + dx + e : d \in a-b \text{ and } e \in ab\}.$$

Here we have a situation similar to the matrix case: the general structure $R[X]$ will be associative only if R is full.

teo-rxfull

Theorem 3.4.2. *Let R be an associative proto-full superring. Then $R[X]$ is a proto-full superring. Moreover, if R is full then $R[X]$ is an associative superring.*

Proof. In fact, we already know that $R[X]$ is a non-associative superring. To prove the desired affirmations, we deal with elements in $R[X]$ as sequences: we denote $a = (a_0, a_1, ..., a_n, ...) \in R[X]$, and for $n \geq 0$, $[a]_n := a_n$. We extend this notation for the operations $+$ and $\cdot$ over $R[X]$:

$$[a+b]_n := a_n + b_n$$
$$[ab]_n := \sum_{i=0}^{n} a_i b_{n-i}$$

With these notations, for all $a, b, c \in R[X]$ and all $n \geq 0$ we get

$$[(ab)c]_n = \sum_{i=0}^{n} [[ab]_i]\, c_n = \sum_{i=0}^{n} \left[\sum_{p=0}^{i} a_p b_{i-p}\right] c_n$$
$$[a(bc)]_n = \sum_{i=0}^{n} a_i\, [[bc]_{n-i}] = \sum_{i=0}^{n} a_i \left[\sum_{p=0}^{n-i} b_p c_{n-i-p}\right]$$

If R is full (proto-full), then (after some reindexation) we get $[(ab)c]_n = [a(bc)]_n$ $([[(ab)c]_n] \cap [[a(bc)]_n] \neq \emptyset)$ for all $n \geq 0$, and then, $(ab)c = a(bc)$. $\square$

Remark 3.4.3. *If R is a full superdomain, does not hold in general that $R[X]$ is also a full superdomain. In fact, even if R is a hyperfield, there are examples, e.g. $R = K, Q_2$, such that $R[X]$ is not a full superdomain (see [6]).*

Definition 3.4.4. *The structure $R[X]$ will be called* ***polynomials*** *in one variable over R. The elements of $R[X]$ will be called polynomials. We denote $R[X_1, ..., X_n] := (R[X_1, ..., X_{n-1}])[X_n]$.*

degreelemma

Lemma 3.4.5 (Adapted from Theorem 5 of [6])**.** *Let R be a superring and $f, g \in R[X] \setminus \{0\}$.*

i - If $t(X) \in f(X) + g(X)$ and $f \neq -g$ then

$$\min\{\deg(f), \deg(g)\} \leq \deg(t) \leq \max\{\deg(f), \deg(g)\}.$$

ii - If R is a superdomain and $t(X) \in f(X)g(X)$, then $\deg(t) = \deg(f) + \deg(g)$. In particular, if $f_1(X), f_2(X), ..., f_n(X) \neq 0$ and $t(X) \in f_1(X)f_2(X)...f_n(X)$, then

$$\deg(t) = \deg(f_1) + \deg(f_2) + ... + \deg(f_n).$$

iii - *(Partial Factorization) Let R be a superdomain,* $\deg(f)=n$ *and* $f\in(X-a_1)(X-a_n)...(X-a_p)$*. Then $p=n$.*

Let $f(X)=a_0+...+a_nX^n$ and $g(X)=b_0+...+b_mX^m$ with $a_n,b_m\neq 0$. We establish the following notation: for $k\in\mathbb{N}$ with $k\leq\deg(f)$ we define $(f)_k:=a_k$ (the k-th coefficient of f).

Proof of Lemma 3.4.5. For item (i), we have

$$f(X)+g(X)=(a_0+b_0)X+...+(a_n+b_m)X^m.$$

Since $f(X)\neq -g(X)$, $0\notin a_n+b_n$, establishing item (i).

Now, suppose without loss of generality that $m\geq n$ and in this case, write

$$f(X)=a_0+...+a_mX^m$$

with $a_k=0$ for $n<k\leq m$. We have $(fg)_{m+n}\in a_nb_m$ and since R is a superdomain, $(fg)_{m+n}\neq 0$. This and induction proves item (ii).

For item (iii), let $g\in(X-a_1)(X-a_n)...(X-a_p)$. By item (ii) and induction, $\deg(g)=p$. Then $n=\deg(f)=p$. □

Despite the fact that $R[X]$ is not full in general, we have a powerful Lemma to get around this situation.

`lemfator`

Lemma 3.4.6. *Let R be a superring and $f\in R[X]$ with $f(X)=a_nX^n+...+a_1X+a_0$. Then:*

i - *For all $b,c\in R$, $(b+cX)f(X)=bf(X)+cXf(X)$.*

ii - *For all $b,c\in R$ and all $p,q\in\omega$ with $p<q$,*

$$(bX^p+cX^q)f(X)=bX^pf(X)+cX^pf(X).$$

iii - *For all $b,c,d\in R$ and all $p,q,r\in\omega$ with $p<q<r$,*

$$(bX^p+cX^q+dX^r)f(X)=bX^pf(X)+cX^pf(X)+dX^rf(X).$$

iv - *For all $b_0,....,b_m\in R$,*

$$(b_0+b_1X+b_2X^2+...+b_mX^m)f(X)=$$
$$b_0f(X)+(b_1X+b_2X^2+...+b_mX^m)f(X).$$

v - *For all $b_0,....,b_m\in R$,*

$$(b_0+b_1X+b_2X^2+...+b_{m-1}X^{m-1}+b_mX^m)f(X)=$$
$$(b_0+b_1X+b_2X^2+...+b_{m-1}X^{m-1})f(X)+b_mX^mf(X).$$

vi - *For all $b_0,....,b_m\in R$,*

$$(b_0+b_1X+...+b_jX^j+b_{j+1}X^{j+1}+...+b_mX^m)f(X)=$$
$$(b_0+b_1X+...+b_jX^j)f(X)+(b_{j+1}X^{j+1}+...+b_mX^m)f(X).$$

In particular, if $d \in R$*,* $g(X) \in R[X]$ *and* $r > \deg(g(X))$*, then*

$$(g(X) + dX^r)f(X) = g(X)f(X) + dX^r f(X).$$

Proof.

i - We can suppose without loss of generality that $b, c \neq 0$. Here is convenient keep in mind that an element in $R[X]$ is a sequence of elements in R. Denote $b + cX = (b_n)_{n\in\omega} \in R[X]$ with $b_0 = b$, $b_1 = c$ and $b_n = 0$ for all $n \geq 2$. By definition, for an element $h(X) \in R[X]$, say

$$h(X) = e_0 + e_1 X + ... + e_{n+1}X^{n+1} = (e_n)_{n\in\omega} \in R[X],$$

we have

$$h(X) \in (b + cX)f(X) \text{ iff } e_p \in \sum_{j=0}^{p} a_j b_{p-j},\ p \in \omega.$$

Since $a_j = 0$ for all $j > n$ and $b_j = 0$ for all $j \geq 2$, we have $e_p = 0$ for all $p > n+1$. Moreover, by the same reason we have that $e_0 \in a_0 b_0$, $e_{n+1} \in a_n b_1$ and for $0 < p < n + 1$, that

$$e_p \in \sum_{j=0}^{p} a_j b_{p-j} = a_p b_0 + a_{p-1} b_1.$$

Summarizing, we conclude that

$$h(X) \in (b + cX)f(X) \text{ iff } e_0 \in a_0 b_0,\ e_{n+1} \in a_n b_1 \text{ and } e_p \in a_p b_0 + a_{p-1} b_1 \text{ for } 0 < p < n + 1. \tag{*}$$

On the other hand, we have that

$$\begin{aligned} bf(X) + cXf(X) &= b[a_n X^n + ... + a_1 X + a_0] + cX[a_n X^n + ... + a_1 X + a_0] \\ &= (a_n b X^n + ... + a_1 b X + a_0 b) + (a_n c X^{n+1} + ... + a_1 c X^2 + a_0 X) \\ &= a_n c X^{n+1} + (a_n b + a_{n-1} c)X^n + ... + (a_2 b + a_1 c)X^2 + (a_1 b + a_0 c)X + a_0 b. \end{aligned} \tag{**}$$

Joining $(*)$ and $(**)$ we conclude that

$$h(X) \in (b + cX)f(X) \text{ iff } h(X) \in bf(X) + cXf(X).$$

ii - Just use the same reasoning of item (i).

iii - Using distributivity, item (i) and (ii) we conclude that

$$(bX^p + cX^q + dX^r)f(X) \subseteq bX^p f(X) + cX^p f(X) + dX^r f(X) = (bX^p + cX^p)f(X) + dX^r f(X). \tag{***}$$

Now with $(***)$ on hand, just proceed with the same reasoning of $(*)$ and $(**)$ to obtain the desired.

iv - This is an immediate consequence of item (iii) and a convenient induction.

v - This is an immediate consequence of item (iii) and a convenient induction.

vi - This is just the combination of previous items.

□

euclid

Theorem 3.4.7 (Euclid's Division Algorithm (3.4 in [11]))**.** *Let K be a superfield. Given polynomials $f(X), g(X) \in K[X]$ with $g(X) \neq 0$, there exists $q(X), r(X) \in K[X]$ such that $f(X) \in q(X)g(X) + r(X)$, with $\deg r(X) < \deg g(X)$ or $r(X) = 0$.*

Proof. This is a generalized version of Theorem 3.4 in [11], which states Euclid's Algorithm for hyperfields. Write

$$\begin{aligned} f(X) &= a_n X^n + \cdots + a_1 X + a_0 \\ g(X) &= b_m X^m + \cdots + b_1 X + b_0 \end{aligned}$$

with $a_n, b_m \neq 0$ and let $b_m^{-1} \in K$ be an element satisfying $1 \in b_m \cdot b_m^{-1}$.

We proceed by induction on n. Note that if $m \geq n$, then is sufficient take $q(X) = 0$ and $r(X) = f(X)$, so we can suppose $m \leq n$. If $m = n = 0$, then $f(X) = a_0$ and $g(X) = b_0$ are both non zero constants, so is sufficient take $q(X) \in a_0 \cdot b_0^{-1}$ and $r(X) = 0$.

Now, suppose $n \geq 1$. Then, since $0 \in a - a$, there exist some $t(X) \in f(X) - a_n b_m^{-1} X^{n-m} g(X)$ with $\deg t(X) < n$. So, by induction hypothesis,

$$t(X) \in q(X)g(X) + r(X) \text{ for some } q(X), r(X) \in R[X] \text{ with } \deg r(X) < \deg g(X) \text{ or } r(X) = 0.$$

Therefore, $\deg t(X) = \deg q(X) + m$ and since $f(X) \in t(X) + a_n b_m^{-1} X^{n-m} g(X)$, we have

$$\begin{aligned} f(X) &\in t(X) + a_n b_m^{-1} X^{n-m} g(X) \\ &\subseteq q(X)g(X) + a_n b_m^{-1} X^{n-m} g(X) + r(X). \end{aligned}$$

But since $\deg q(X) = \deg t(X) - m < n - m$, we have (see Lemma 3.4.6 (vi)) that

$$[q(X) + a_n b_m^{-1} X^{n-m}] g(X) = q(X)g(X) + a_n b_m^{-1} X^{n-m} g(X).$$

So there exist some $q'(X) \in q(X) + a_n b_m^{-1} X^{n-m}$ with $f(X) \in q'(X)g(X) + r(X)$ and $\deg r(X) < \deg g(X)$ or $r(X) = 0$, completing the proof. □

Remark 3.4.8.

i - Note that the polynomials q and r of Theorem 3.4.7 are not unique in general: if $f \in gq + r$, then $f \in g(q + 1 - 1) + r$ and $f \in gq + (r + 1 - 1)$, then, if $\{0\} \neq 1 - 1$, we have many q's and r's.

ii - However, if R is a ring, then Theorem 3.4.7 provide the usual Euclid Algorithm, with the uniqueness of the quotient and remainder.

teoPID

Theorem 3.4.9 (Adapted from Theorem 6 of [6])**.** *Let F be a full associative superfield. Then $F[X]$ is a principal ideal superdomain.*

Proof. Let I be a ideal of $F[X]$. If $I = 0$ then $I = \langle 0 \rangle$ and if there is some $a \in F \setminus \{0\}$ with $a \in I$, then $I = F[X] = \langle 1 \rangle$ (because F is full).

Now let $p(X) \in I$ be a polynomial with minimal degree $m \geq 1$. Let $f(X) \in I$ be another polynomial. By Euclid's Algorithm, there exists $q(X), r(X) \in F[X]$ with $f(X) \in p(X)q(X) + r(X)$ and $r(X) = 0$ or $\deg(r) < \deg(p) = m$. Since $f, p \in I$ and $r(X) \in f(X) - p(X)q(X)$, we have

$r \in I$. Note that by the minimality of m, all nonzero polynomial in $f(X) - p(X)q(X)$ has degree at least m. If $r \neq 0$ then

$$\min\{\deg f, \deg(p) + \deg(q)\} \leq \deg r \leq \max\{\deg f, \deg(p) + \deg(q)\}.$$

In particular $\deg(r) \geq m$ (because $\deg(f) \leq m$), contradicting $deg(r) < m$. Hence $r = 0$ and $I = \langle p \rangle$. In particular, $I = F[X] \cdot p(X)$. $\square$

3.5 Evaluation and Roots

Let R, S be superrings and $h : R \to S$ be a morphism. Then h extends naturally to a morphism in the proto-superrings multipolynomials $h^X : R[X] \to S[X]$:

$$(a_n)_{n\in\mathbb{N}} \in R[X] \;\mapsto\; (h(a_n))_{n\in\mathbb{N}} \in S[X]$$

Now let $s \in S$. We define the h-**evaluation** of s at $f(X) \in R[X]$ with $f(X) = a_0 + a_1X + ... + a_nX^n$ by

$$f^h(s) = ev^h(s, f) := \{s' \in S : s' \in h(a_0) + h(a_1)s + h(a_2)(s^2) + ... + h(a_n)(s^n)\}.$$

In order to easy our presentation, we just denote $ab^n := a(b^n)$. We define the h-**evaluation** for a subset $I \subseteq S$ by

$$f^h(I) = \bigcup_{s\in I} f^h(s).$$

In particular if $S \supseteq R$ are superrings and $\alpha \in S$, we have the **evaluation** of α at $f(X) \in R[X]$ by

$$f(\alpha, S) = ev(\alpha, f, S) = \{b \in S : b \in a_0 + a_1\alpha + a_2\alpha^2 + ... + a_n\alpha^n\} \subseteq S.$$

Note that the evaluation **depends** on the choice of S. When $S = R$ we just denote $f(\alpha, R)$ by $f(\alpha)$.

A **root** of f in S is an element $\alpha \in S$ such that $0 \in ev(\alpha, f, S)$. In this case we say that α is S-**algebraic** over R. An **effective root** of f in S is an element $\alpha \in S$ such that $f \in (X - \alpha) \cdot g(X)$ for some $g(X) \in R[X]$. A superring R is **algebraically closed** if every non constant polynomial in $R[X]$ has a root in R.

Observe that, if F is a field, the evaluation of $F[X]$ as a ring coincide with the usual evaluation, and, of course, root and effective roots are the same thing. Therefore, if F is algebraically closed as hyperfield and superfield, then will be algebraically closed in the usual sense.

`unexpected-rem`

Remark 3.5.1. *The expansion of the above field-theoretical concepts to the multialgebraic theory of superfields (hyperfields, in particular) brings new phenomena:*

- *i- (Polynomials can have infinite roots): Let F be a infinite pre-special hyperfield ([24]). Then F has characteristic 0, $a^2 = 1$ for all $a \neq 0$ so the polynomial $f(X) = X^2 - 1$ has infinite roots (i.e, $0 \in ev(f, \alpha)$ for all $\alpha \in \dot{F}$).*

- *ii- (Finite hyperfields can be algebraically closed). The hyperfield $K = \{0, 1\}$ is algebraically closed. In fact, if $p(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n \in K[X]$, with $a_n \neq 0$, then $0 \in p(0)$ (if $a_0 = 0$) or $p(1) = K$, since $1 + 1 = \{0, 1\}$.*

We have good results concerning irreducibly (see for instance, Theorem 3.5.4 below). These results are the key to the development of superfields extensions, which leads us to some kind of algebraic closure.

Definition 3.5.2 (Irreducibility)**.** *Let R be a superfield and $f, d \in R[X]$. We say that d divides f if and only if $f \in \langle d\rangle$, and denote $d|f$. We say that f is **irreducible** if $\deg f \geq 1$ and $u|f$ for some $u \in R[X]$ (i.e, $f \in \langle u\rangle$), then $\langle f\rangle = \langle u\rangle$.*

lemquadext2

Theorem 3.5.3. *Let F be a full associative superfield and $p(X) \in F[X]$ be an irreducible polynomial. Then $\langle p(X)\rangle$ is a maximal ideal.*

Proof. Let $p(X)$ be irreducible and $I \subseteq F[X]$ an ideal with $\langle p(X)\rangle \subseteq I$. By Theorem 3.4.9,

$$I = \langle f(X)\rangle = F[X] \cdot f(X)$$

for some $f(X) \in F[X]$. Since $p(X) \in I = \langle f(X)\rangle$, then $p(X) = f(X)g(X)$ for some $g(X) \in F[X]$. Since $p(X)$ is irreducible, either $f(X)$ or $g(X)$ is a constant polynomial. If $f(X)$ is constant, then $I = F[X]$, and if $g(X)$ is constant, $I = \langle p(X)\rangle$, which proves that $\langle p(X)\rangle$ is maximal. $\square$

If F is not full, we cannot prove that $\langle p(X)\rangle$ is a maximal ideal. But we still have that $F[X]/\langle p\rangle$ is a superfield.

lemquadext

Theorem 3.5.4. *Let F be a superfield and $p \in F[X]$ be an irreducible polynomial. Then $F[X]/\langle p\rangle$ is a superfield.*

Proof. Let $p(X) = d_0 + a_1X + ... + a_{n+1}X^{n+1}$. Note that

tret

$$\begin{aligned} F(p(X)) := F[x]/\langle p\rangle &= \{[a_0 + a_1X + ... + a_nX^n] : a_0, ..., a_n \in F\} \\ &= \{[f(X)] : f(X) = a_0 + a_1X + ... + a_rX^r \text{ with } a_0, ..., a_r \in F,\ r \leq n\}. \quad (3.2) \end{aligned}$$

Let $f(X) = a_0 + a_1X + ... + a_rX^r$ and $g(X) = b_0 + b_1X + ... + b_sX^s$ with and suppose

$$[0] \in [f(X)][g(X)].$$

There exist

$$h(X) \in (f(X)g(X)) \cap \langle p(X)\rangle.$$

Since F is a superdomain, every nonzero polynomial in $\langle p\rangle$ has degree at least $n+1 = \deg(p)$. Now get a nonzero element in $[t(x)] \in [f(X)][g(X)]$. Using Equation 3.2 we have $t(X) \in f(X)g(X)$ with $\deg(t) \leq n$. Then $h(X) = 0$ and $0 \in f(X)g(X)$, which imply $f(X) = 0$ or $g(X) = 0$ (because $F[X]$ is a superdomain). Then $[F(X)] = 0$ or $[g(X)] = [0]$, proving that $F[p(X)]$ is a superdomain (and then, $\langle p(X)\rangle$ is strongly prime).

Now we prove that $F[p(X)]$ is a superfield, i.e, that for all nonzero $[f(X)] \in F[p(X)]$, there exist a nonzero $[g(X)] \in F[p(X)]$ with $[1] \in [f(X)][g(X)]$. We proceed by induction on $n = \deg(f(X))$.

If $n = 0$, then $f(X) = a$ for some $a \in \dot{F}$, and there exist $a^{-1} \in \dot{F}$[5] with $1 \in a \cdot a^{-1}$, and then $[1] \in [f(X)][a^{-1}]$. If $n = 1$, then $f(X) = aX + b$, $a, b \in F$ $(a \neq 0)$. By Euclid's Algorithm, there exists $q(X), r(X)$ with $p(X) \in f(X)q(X) + r(X)$ with $r(X) = 0$ or $\deg(r(X)) < \deg(f(X))$. Since $p(X)$ is irreducible, $r(X) \neq 0$ and $r(X) = d \in \dot{F}$. Moreover for some $d^{-1} \in \dot{F}$ with $1 \in d \cdot d^{-1}$ we

[5] Of course, not necessarily unique.

have

$$p(X) \in f(X)q(X) + d \Rightarrow [0] \in [f(X)][q(X)] + [d] \Rightarrow -[d] \in [f(X)][q(X)]$$
$$\Rightarrow [dd^{-1}] \subseteq [f(X)](-[d^{-1}][q(X)]) \Rightarrow [1] \in [f(X)](-[d^{-1}][q(X)]),$$

and then, there exist $[t(X)] \in -[d^{-1}][q(X)]$ with $[1] \in [f(X)][t(X)]$.

Now, suppose by induction that all polynomial of degree at most n has an inverse and let $f(X) \in F[X]$ with $\deg(f(X)) = n+1$. By Euclid's Algorithm, there exists $q(X), r(X)$ with $p(X) \in f(X)q(X) + r(X)$ with $r(X) = 0$ or $\deg(r(X)) < \deg(f(X))$ and since $p(X)$ is irreducible, we have $r(X) \neq 0$. By induction hypothesis, there exist $g(X) \in F[X]$ with $[1] \in [r(X)][g(X)]$. Then

$$\begin{aligned} p(X) \in f(X)q(X) + r(X) &\Rightarrow [0] \in [f(X)][q(X)] + [r(X)] \\ &\Rightarrow [r(X)] \in -[f(X)][q(X)] \\ &\Rightarrow [r(X)][g(X)] \subseteq -[f(X)][q(X)][g(X)] \\ &\Rightarrow 1 \in [r(X)][g(X)] \subseteq [f(X)](-[q(X)][g(X)]), \end{aligned}$$

then there exist $[t(X)] \in -[q(X)][g(X)]$ with $[1] \in [f(X)][t(X)]$, completing the proof. □

Using Theorem 3.5.4, we obtain an algorithm to determine the invertible elements in $F[p(X)]$ particularly useful in the field case:

lemquadext3

Corollary 3.5.5. *Let F be a field and $p(X) \in F[X]$ be an irreducible polynomial. If $f(X) \neq 0$ and $p(X) = f(X)q(X) + r(X)$ with $r(X) \neq 0$, then*

$$[f(X)]^{-1} = -[q(X)][r(X)]^{-1} \in F[p(X)].$$

Definition 3.5.6. *Let F be a superfield and $p(X) \in F[X]$ be an irreducible polynomial. We denote $F(p) := F(p(X)) = F[X]/\langle p(X)\rangle$.*

lemfator2

Lemma 3.5.7. *Let F be a superfield and $p(X) \in F[X]$ be an irreducible polynomial. Denote $\overline{X} = \lambda$ and let $f \in F(p)$ with $f = \overline{a_n}\lambda^n + ... + \overline{a_1}\lambda + \overline{a}_0$. Then:*

i - For all $b, c \in F$, $(\overline{b} + \overline{c}\lambda)f = \overline{b}f + \overline{c}\lambda f$.

ii - For all $b_0, ..., b_m \in F$,

$$(\overline{b_0} + \overline{b_1}\lambda + ... + \overline{b_j}\lambda^j + \overline{b_{j+1}}\lambda^{j+1} + ... + \overline{b_m}\lambda^m)f =$$
$$(\overline{b_0} + \overline{b_1}\lambda + ... + \overline{b_j}\lambda^j)f + (\overline{b_{j+1}}\lambda^{j+1} + ... + \overline{b_m}\lambda^m)f.$$

In particular, if $d \in F$, $g \in F(p)$ with $g = \overline{b_0} + \overline{b_1}\lambda + \overline{b_2}\lambda^2 + ... + \overline{b_m}\lambda^m$ and $r > m$, then

$$(g + \overline{d}\lambda^r)f = gf + \overline{d}\lambda^r f.$$

Proof. Similar to Lemma 3.4.6. □

root1

Theorem 3.5.8. *Let F be a superfield and $p(X) \in F[X]$ be a polynomial of degree greater or equal to 1. Then there exist a superfield L such that $F \subseteq L$, F is a sub superfield of L (i.e, the inclusion $F \hookrightarrow L$ is a full morphism) and $p(X)$ has a root.*

Proof. It is enough to show the result for $p(X)$ irreducible. In this case, the ideal $\langle p(X)\rangle \subseteq F[X]$ is maximal and $K' = F[X]/\langle p(X)\rangle$ is a superfield. If we consider the canonical injection $\iota : F \to F[X]/\langle p\rangle$ given by $a \mapsto \overline{a}$, we have a full morphism (basically because $F \hookrightarrow F[X]$ is full). Putting $F' = \iota(F)$ we have that $F \cong F'$, $F' \hookrightarrow L$ is a full morphism and the polynomial p^{ι} (given by the application of ι in each coefficient) has a root $\overline{x}$.

Next, let $K = F \cup X$ for some X of cardinality $K' \setminus F'$. We construct a bijection $\varphi : K \to K'$ which restrict ton F is equal to ι. This bijection transport the structure of superfield for K (in the obvious way), in order to get an extension $K|F$ such that f has a root $\varphi^{-1}(\overline{x})$. □

Corollary 3.5.9. *Let F be a superfield and $f \in F[X]$ be a polynomial with $n = \deg(f) \geq 1$. Then there exist a non-associative superfield L such that $F \subseteq L$ and f has at least n roots.*

Corollary 3.5.10. *Let F be a superfield and $f_1, ..., f_n \in F[X]$ be polynomials with $1 \leq \deg(f_j) = r_j$, $j = 1, ..., n$. Then there exist a superfield L such that $F \subseteq L$ and each f_j has at least r_j roots.*

3.6 Extensions

We have some possibilities to consider in order to define the notion of extension for superfields:

`extension`

Definition 3.6.1 (Extensions)**.** *Let F and K be superfields.*

*i - We say that K is a **proto superfield extension (or just a proto extension)** of F, notation $K|_pF$, if $F \subseteq K$.*

*ii - We say that K is a **superfield extension (or just an extension)** of F, notation $K|F$ if $F \subseteq K$ and the inclusion map $F \hookrightarrow K$ is a superfield morphism.*

*iii - We say that K is a **full superfield extension (or just a full extension)** of F, notation $K|_fF$ if $F \subseteq K$ and the inclusion map $F \hookrightarrow K$ is a full superfield morphism.*

Example 3.6.2.

i - Of course, all full extension is an extension and all extension is a proto extension.

ii - We have $K \subseteq Q_2$ but the inclusion map $K \hookrightarrow Q_2$ is not a morphism. Then we have a proto extension $Q_2|_pK$ that is not an extension.

iii - For p, q prime integers with $q \geq p$ we have an inclusion morphism $H_p \hookrightarrow H_q$, but this morphism is not full. Then we have an extension $H_q|H_p$ that is not a full extension.

iv - Let F be a superfield, $p \in F[X]$ an irreducible polynomial and $F(p) = F[X]/\langle p\rangle$ be the superfield built in Theorem 3.5.8. Then we have a full morphism $F \hookrightarrow F(p)$ so we have a full extension $F(p)|_fF$.

v - Let F, K be fields such that $F \subseteq K$. Then the field extension $K|F$ satisfy all conditions in Definition 3.6.1.

The result below justify a deeper look at full superfield extensions.

`unicityext`

Theorem 3.6.3. *Let $K_1|_fF$ and $K_2|_fF$ be full superfield extensions and suppose that $\gamma \in K_1 \cap K_2$. Then*

$$F[\gamma, K_1] = F[\gamma, K_2].$$

Proof. Suppose first that $K_2|_f K_1$ is a full extension. Then for all $f \in F[X]$, $ev(f, K_1) = ev(f, K_2)$, so $F[\gamma, K_1] = F[\gamma, K_2]$.

Now, for the general case just note that $K_1|_f(K_1 \cap K_2)$ and $K_2|_f(K_1 \cap K_2)$. Then

$$F[\gamma, K_1] = F[\gamma, K_1 \cap K_2] = F[\gamma, K_2].$$

□

Definition 3.6.4 (Algebraic Extensions)**.** *We say that a proto extension $K|_pF$ is* ***algebraic*** *if all element $\alpha \in K$ is K-algebraic over F. We denote the same for extensions and full extensions.*

Definition 3.6.5 (Linear Independency, Basis, Degree)**.** *Let $K|_pF$ be a proto extension and $I \subseteq K$. We say that I is F****-linearly independent*** *if for all distinct $\lambda_1, ..., \lambda_n \in I$, $n \in \mathbb{N}$, the following hold:*

$$\text{If } 0 \in a_1\lambda_1 + ... + a_n\lambda_n \text{ then } a_1 = ... = a_n = 0$$

*and I is F****-linearly dependent*** *if it is not F-linearly independent. We say that I is a F****-basis*** *of K if I is linearly independent and K is* ***generated by*** *I, i.e,*

$$K = \bigcup_{n \geq 0} \left\{ \sum_{i=0}^{n} a_i\lambda_i : a_i \in F,\ \lambda_i \in I \right\}.$$

In this case, we write $K = F[I]$. We define the ***degree*** *of $K|_pF$, notation $[K : F]$, by the following*

$$[K : F] := \infty \text{ or } [K : F] := \max\{n : \text{the set } \{1, \lambda, \lambda^2, ..., \lambda^n\} \text{ is linearly independent for all } \lambda \in K\}.$$

rem1

Remark 3.6.6. *There are these immediate consequences of the above definitions:*

a - *If $I \subseteq K$ is linearly independent and $J \subseteq I$ then J is also linearly independent.*

b - *An element $\alpha \in K$ is F-algebraic if and only if $\{\alpha^k : k \in \mathbb{N}\}$ is F-linearly dependent.*

c - *If $[K : F] < \infty$ then all $\alpha \in K$ is F-algebraic.*

d - *Let F be a superfield and $p \in F[X]$ an irreducible polynomial, say $p(X) = a_0 + a_1X + ... + a_nX^{n-1} + X^n$. Then $\{\overline{1}, \overline{X}, ..., \overline{X}^{n-1}\}$ is a F-basis of $F(p)$.*

Now, let $K|_pF$ be a proto extension and $\gamma \in K$ algebraic. Then there exist an irreducible polynomial $f(X)$ such that $0 \in f(\gamma, K)$. Let $\mathrm{Irr}_F(\gamma, K)$ be the minimum degree irreducible polynomial $f(X)$ such that $0 \in f(\gamma, K)$. Let $F[\gamma, K] \subseteq K$ be the set

$$F[\gamma, K] := \bigcup_{f \in F[X]} ev(f, \gamma, K) \subseteq K,$$

and $I_{\gamma,K} \subseteq F[\gamma, K]$ the set

$$I_{\gamma,K} := \bigcup_{f \in \langle \mathrm{Irr}_F(\gamma,K) \rangle} ev(f, \gamma, K) \subseteq K.$$

Note that for all $g \in F[X]$ and all $a_0, ..., a_n \in F$, applying the "Newton's binom formula" we get

$$ev(g, (a_0 + a_1\gamma + a_2\gamma^2 + ... + a_{n-1}\gamma^{n-1} + a_n\gamma^n), K) \subseteq F[\gamma, K].$$

Remark 3.6.7.

i - *If $K|F$ is a field extension then our $F[\gamma, K]$ coincide with the usual simple extension $F(\gamma)$.*

ii - *If $K|F$ is a superfield extension and $\gamma \in K$, then $F[\gamma, K]$* ***depends on the choice of*** *K. For example, consider $H_3|H_1$ and $H_5|H_1$ and the element $2 \in H_3$ (and of course, in H_5). Then*

$$H_2[2, H_3] = \bigcup_{f \in H_2[X]} ev(f, \gamma, H_3) = H_3,$$
$$H_2[2, H_5] = \bigcup_{f \in H_2[X]} ev(f, \gamma, H_5) = H_5,$$

and then, $H_2[2, H_3] \neq H_2[2, H_5]$.

iii - *For a proto extension $K|_p F$ the set $F[\gamma, K]$ may not be a superfield! Let $F = H_2$, $K = \mathbb{R}$ and $\gamma = 2$. Then*

$$H_2[2, \mathbb{R}] = 2\mathbb{Z}$$

which is not a superfield.

At this point, our goal is to obtain an appropriate notion for simple extensions of superfields. In other words, given a full extension $K|_f F$ and $\alpha \in K$ algebraic, it is highly desirable to obtain a superfield $F(\alpha)$ that:

1. $F \cup \{\alpha\} \subseteq F(\alpha)$;

2. $F(\alpha)$ is the minimal superfield (with respect to inclusion) satisfying (1);

3. $F(\alpha)$ is "computable" in some way (or saying it in a more realistic manner, we want that $F(\alpha) \cong F(p)$ with $p(X) = \mathrm{Irr}_F(\alpha)$)[6].

For general superfields there are some obstacles to achieve this goal. The very first one is the fact that $R[X]$ is not full in general. However, we have an interesting property valid for all $a, b \in R[X]$:

$$a(1 + X) = a + aX \text{ and } (a + b)X = aX + bX.$$

This property is the inspiration for the following definition.

almostfull

Definition 3.6.8. *Let $K|_p F$ be a proto superfield extension and $\gamma \in K$. Suppose that K is F-generated by $\{1, \gamma^2, ..., \gamma^n\}$. We say that K is* ***F-almost full relative to γ (or just almost full)*** *if for all $a, b, c \in F$, and all $p, q, r \in \mathbb{N}$ distinct*

$$(a\gamma^p + b\gamma^q + c\gamma^r)\gamma = a\gamma^{p+1} + b\gamma^{q+1} + c\gamma^{r+1}.$$

Here are some immediate consequences of Definition 3.6.8:

lemfator3

Lemma 3.6.9. *Let $K|_f F$ be a full extension F-almost full relative to γ and let $A = a_0 + a_1\gamma + a_2^2 + ... + a_n\gamma^n$. Then:*

i - *For all $b, c \in F$, $(b + c\gamma)A = bA + c\gamma A$.*

[6] As we will see later, simple calculations with superfield are highly demanding...

ii - For all $b_0, ..., b_m \in F$,

$$(b_0 + b_1\gamma + ... + b_j\gamma^j + b_{j+1}\gamma^{j+1} + ... + b_m\gamma^m)A =$$
$$(b_0 + b_1\gamma + ... + b_j\gamma^j)A + (b_{j+1}\gamma^{j+1} + ... + b_m\gamma^m)A.$$

In particular, if $d \in F$, $B \subseteq K$ *with* $B = b_0 + b_1\gamma + b_2\gamma^2 + ... + b_m\gamma^m$ *and* $r > m$, *then*

$$(B + d\gamma^r)A = AB + d\gamma^r A.$$

Proof. Similar to Lemma 3.4.6. □

almostfact

Lemma 3.6.10. *Let* $K|_f F$ *be a full extension* F*-almost full relative to* γ*. Then:*

i - $K = F[\gamma, K]$;

ii - If $K|_f F$ *and* $L|_f K$ *are almost full then* $L|F$ *is almost full;*

iii - If $L|_f F$ *is another full extension and* $\pi : K \to L$ *is a full surjective morphism, then* $L|_f F$ *is* F*-almost full relative to* $\pi(\gamma)$*;*

iv - For all $a_0, ..., a_n, b_0, ..., b_n \in F$,

$$(a_0 + a_1\gamma + a_2\gamma^2 + ... + a_{n-1}\gamma^{n-1} + a_n\gamma^n)(b_0 + b_1\gamma + b_2\gamma^2 + ... + b_{n-1}\gamma^{n-1} + b_n\gamma^n) \subseteq$$
$$a_0b_0 + \left(\sum_{j=0}^{1} a_jb_{1-j}\right)\gamma + ... + \left(\sum_{j=0}^{2n-1} a_jb_{(2n-1)-j}\right)\gamma^{2n-1} + \left(\sum_{j=0}^{2n} a_jb_{1-j}\right)\gamma^{2n}$$

with the convention $a_j = b_j = 0$ *if* $j > n$.

Let $K|_f F$ be a full extension and $\alpha \in K$ algebraic over F. Our aim is to provide an almost full algebraic extension $F(\alpha)|_f F$ containing F and α. The key to that is to find a way to describe algebraic elements of K. Here we have a first result in this direction.

Theorem 3.6.11 (Almost Full Newton's Binom)**.** *Let* $K|F$ *be an almost full superfield extension* F*-generated by* $\{1, \gamma, ..., \gamma^n\}$, $\gamma \in K$*. Then for all* $a, b \in F$,

$$(a + b\gamma)^n = \sum_{j=0}^{n} \binom{n}{j} a^j (b\gamma)^{n-j}.$$

Proof. By induction is enough to prove the case $n = 2$. We have

$$(a + b\gamma)^2 := (a + b\gamma)(a + b\gamma) \overset{3.6.9}{=} a(a + b\gamma) + b\gamma(a + b\gamma) = a^2 + ab\gamma + b\gamma a + (b\gamma)^2$$
$$= a^2 + ab\gamma + ab\gamma + (b\gamma)^2 = a^2 + 2ab\gamma + (b\gamma)^2 := \sum_{j=0}^{2} \binom{n}{j} a^j (b\gamma)^{n-j}.$$

□

In the sequence, we have a key result, which states that our "best candidate for simple extension", $F(p)$, is an full algebraic and almost full extension of F.

teohell2

Theorem 3.6.12. *Let* F *be a superfield and* $p \in F[X]$ *be an irreducible polynomial. Then* $F(p)|_f F$ *is an algebraic extension. Moreover, if* $\deg p = n + 1$ *then* $[F(p) : F] \leq n + 1$.

Proof. Remember that $F(p)$ is generated by $\{1,\gamma,...,\gamma^n\}$ with $\gamma=\overline{X}$, $n\in\mathbb{N}$. Also, we can consider n as the minimal integer such that there exist $a_0,...,a_{n+1}$ with

$$0\in a_0+a_1\gamma+...+a_{n+1}\gamma^{n+1}.$$

Now let $b_0+b_1\gamma+...+b_n\gamma^n\in F(p)^*$. Since $x\cdot y\neq\emptyset$ for all $x,y\in F(P)$, for all $k=0,...,n$, there exist

$$d_{k0}+d_{k1}\gamma+...+d_{kn}\gamma^n\in(b_0+b_1\gamma+...+b_n\gamma^n)^k$$

for suitable $d_{ij}\in F$. Writing this in matrix notation, we have

$$D\begin{pmatrix}1\\ \gamma\\ \vdots\\ \gamma^n\end{pmatrix}\subseteq\begin{pmatrix}(b_0+b_1\gamma+...+b_n\gamma^n)^0\\ (b_0+b_1\gamma+...+b_n\gamma^n)^1\\ \vdots\\ (b_0+b_1\gamma+...+b_n\gamma^n)^n\end{pmatrix}$$

with

$$D=\begin{pmatrix}d_{00} & d_{01} & \dots & d_{1n}\\ d_{10} & d_{11} & \dots & d_{1n}\\ \vdots & \vdots & \ddots & \vdots\\ d_{n0} & d_{n1} & \dots & d_{nn}\end{pmatrix}$$

The fact that $F(p)$ is almost full enable us to scale the matrix D, saying

$$D_{scaled}=\begin{pmatrix}e_{00} & e_{01} & \dots & e_{1n}\\ 0 & e_{11} & \dots & e_{1n}\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \dots & e_{nn}\end{pmatrix}$$

and getting

$$\begin{pmatrix}e_{00} & e_{01} & \dots & e_{1n}\\ 0 & e_{11} & \dots & e_{1n}\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \dots & e_{nn}\end{pmatrix}\begin{pmatrix}1\\ \gamma\\ \vdots\\ \gamma^n\end{pmatrix}\in\begin{pmatrix}\sum_{j=0}^n g_{0j}(b_0+b_1\gamma+...+b_n\gamma^n)^j\\ \sum_{j=0}^n g_{1j}(b_0+b_1\gamma+...+b_n\gamma^n)^j\\ \vdots\\ \sum_{j=0}^n g_{nj}(b_0+b_1\gamma+...+b_n\gamma^n)^j\end{pmatrix}\qquad(*)$$

for suitable $g_{ij}\in F$.

If D_{scaled} is not invertible then $0\in\det(D_{scaled})=e_{11}e_{22}...e_{nn}$ and then, $e_{ii}=0$ for some $i\in\{1,...,n\}$ (see Lemma 3.3.11), which imply (by the very scalation process) that there exist a row i with L_i being a linear combination of the others. Suppose without loss of generality that

$$L_{n+1}\cap\left[\left(\sum_{j=1}^{r_1}\lambda_{j1}\right)L_1+...+\left(\sum_{j=1}^{r_n}\lambda_{jn}\right)L_n\right]\neq\emptyset.$$

This means

$$0\in z_0+z_1(b_0+b_1\gamma+...+b_n\gamma^n)^1+...+z_n(b_0+b_1\gamma+...+b_n\gamma^n)^{n-1}-(b_0+b_1\gamma+...+b_n\gamma^n)^{n+1},$$

for suitable $z_0, ..., z_n \in F$, and then, for $f(X) = z_0 + z_1X + ... + z_nX^n - X^{n+1}$, we have

$$0 \in f(b_0 + b_1\gamma + ... + b_n\gamma^n),$$

which means $b_0 + b_1\gamma + ... + b_n\gamma^n$ is algebraic. If D_{scaled} is invertible, since $F(p)|_f F$ is almost full we get

$$\begin{pmatrix} 1 \\ \gamma \\ \vdots \\ \gamma^n \end{pmatrix} \in D^{-1}_{scaled} \left[D_{scaled} \begin{pmatrix} 1 \\ \gamma \\ \vdots \\ \gamma^n \end{pmatrix} \right].$$

After multiplying the equation $(*)$ by D^{-1}_{scaled} we arrive at a system

$$\begin{pmatrix} 1 \\ \gamma \\ \vdots \\ \gamma^n \end{pmatrix} \in D^{-1}_{scaled} \left[D_{scaled} \begin{pmatrix} 1 \\ \gamma \\ \vdots \\ \gamma^n \end{pmatrix} \right] \subseteq D^{-1}_{scaled} \begin{pmatrix} \sum_{j=0}^n g_{0j}(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \\ \sum_{j=0}^n g_{1j}(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \\ \vdots \\ \sum_{j=0}^n g_{nj}(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \end{pmatrix}$$

then our situation is

$$\begin{pmatrix} 1 \\ \gamma \\ \vdots \\ \gamma^n \end{pmatrix} \in D^{-1}_{Scaled} \begin{pmatrix} \sum_{j=0}^n g_{0j}(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \\ \sum_{j=0}^n g_{1j}(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \\ \vdots \\ \sum_{j=0}^n g_{nj}(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \end{pmatrix} \tag{$**$}$$

Let $D^{-1}_{Scaled} = (h_{ij})$. From $(**)$, after calculating the matrix product we get (remember the almost fullness)

$$\begin{cases} \gamma^0 \in \sum_{j=0}^n g_{0j}h_{0j}(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \\ \gamma_1 \in \sum_{j=0}^n g_{1j}h_{1j}(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \\ \vdots \\ \gamma^n \in \sum_{j=0}^n g_{nj}h_{nj}(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \end{cases}$$

which imply

$$\begin{cases} a_0\gamma^0 \in \sum_{j=0}^n a_0(g_{0j}h_{0j})(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \\ a_1\gamma_1 \in \sum_{j=0}^n a_1(g_{1j}h_{1j})(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \\ \vdots \\ a_n\gamma^n \in \sum_{j=0}^n a_n(g_{nj}h_{nj})(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \end{cases}$$

Then

$$a_1a_n\gamma^{n+1} \subseteq \left(\sum_{j=0}^n a_1(g_{1j}h_{1j})(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \right) \left(\sum_{j=0}^n a_n(g_{nj}h_{nj})(b_0 + b_1\gamma + ... + b_n\gamma^n)^j \right)$$

and

$$
\begin{aligned}
&0 \in a_0 + a_1\gamma + ... + a_{n+1}\gamma^{n+1} \subseteq \\
&\sum_{p=0}^{n}\left[\sum_{j=0}^{n} a_p(g_{pj}h_{pj})(b_0 + b_1\gamma + ... + b_n\gamma^n)^j\right] + \\
&\left(\sum_{j=0}^{n} a_1(g_{1j}h_{1j})(b_0 + b_1\gamma + ... + b_n\gamma^n)^j\right)\left(\sum_{j=0}^{n} a_n(g_{nj}h_{nj})(b_0 + b_1\gamma + ... + b_n\gamma^n)^j\right).
\end{aligned}
$$

Now, thinking with polynomials, we have

$$
\begin{aligned}
A(X) := \sum_{p=0}^{n}\left[\sum_{j=0}^{n} a_p(g_{pj}h_{pj})X^j\right] + \left(\sum_{j=0}^{n} a_1(g_{1j}h_{1j})X^j\right)\left(\sum_{j=0}^{n} a_n(g_{nj}h_{nj})X^j\right) = \\
\left[\sum_{p=0}^{n}\sum_{j=0}^{n} a_p(g_{pj}h_{pj})\right]X^j + \left(\sum_{j=0}^{n} a_1(g_{1j}h_{1j})X^j\right)\left(\sum_{j=0}^{n} a_n(g_{nj}h_{nj})X^j\right) = \\
= P(X) + S(X)T(X),
\end{aligned}
$$

with

$$
\begin{aligned}
P(X) &= \left[\sum_{p=0}^{n}\sum_{j=0}^{n} a_p(g_{pj}h_{pj})\right]X^j \\
S(X) &= \sum_{j=0}^{n} a_1(g_{1j}h_{1j})X^j \\
T(X) &= \sum_{j=0}^{n} a_n(g_{nj}h_{nj})X^j
\end{aligned}
$$

Then

$$0 \in ev\left(A(X), b_0 + b_1\gamma + ... + b_n\gamma^n\right);$$

which means that there exists at least a polynomial $f(X) \in A(X) = P(X) + S(X)T(X)$ with

$$0 \in f(b_0 + b_1\gamma + ... + b_n\gamma^n).$$

Then $b_0 + b_1\gamma + ... + b_n\gamma^n$ is algebraic. Of course, this also imply that $[F(p) : F] \leq n + 1$. □

Keeping on hands the Theorem 3.6.12, we work in order to legitimate $F(p)$ as the simple extension of F by α. But before we do that, lets make some considerations about general almost full extensions.

The proof of Theorem 3.6.12 strongly rely in the fact that $a_0 + a_1\omega + ... + a_{n-1}\omega^{n-1}$ is unitary. It is a special property of $F(p)$, and is not necessarily valid for a general almost full full extension.

For an almost full extension $K|_f F$ denote

$$\mathrm{Alg}(K, F) = \{\alpha \in K : \alpha \text{ is algebraic over } F\}.$$

We do not know if $\mathrm{Alg}(K, F)$ is a superfield in general. The difficult here is that despite the fact that Theorem 3.6.12 is still available, we cannot use it to conclude that all elements in $\alpha\beta$ and $\alpha+\beta$ are algebraic if α and β are algebraic.

It is time to define a notion of simple extension.

Definition 3.6.13 (Simple Extension)**.** *Let $K|_f F$ be a full extension and $\alpha \in K$ algebraic. We define the **simple extension** $F(\alpha, K)$ by*

$$F(\alpha, K) := \bigcap\{L : L|_f F \textit{ is full and } F[\alpha] \subseteq L\}.$$

Note that we have a full extension $F(\alpha, K)|_f F$. If $\lambda_1, ..., \lambda_n \in K$ are algebraic, we define

$$F(\lambda_1, ..., \lambda_n, K) := F(\lambda_1, ..., \lambda_{n-1}, K)(\lambda_n, K).$$

By Theorem 3.6.3 we can simply write $F(\alpha)$ to indicate $F(\alpha, K)$

Theorem 3.6.14.

i - Let $K|_f F$ be a full extension with $\alpha \in K$ algebraic. Let $p(X) = Irr_F(\alpha, K)$. Then $F(\alpha) \cong F(p)$.

ii - Let $K|_f F$ be a full extension and $\alpha, \beta \in K$ algebraic such that $F(\alpha)(\beta)|_f F(\alpha)$ and $F(\beta)(\alpha)|_f F(\beta)$ are almost full extensions relative to α and β respectively. Then

$$F(\alpha)(\beta) \cong F(\beta)(\alpha).$$

iii - Let $K|_f F$ be a full extension. For all $\alpha_1, ..., \alpha_n \in K$ and all $\sigma \in S_n$ we have

$$F(\alpha_1, ..., \alpha_n) \cong F(\alpha_{\sigma(1)}, ..., \alpha_{\sigma(n)}).$$

Proof.

i - We have that $F(p)|_f F$ is a full extension containing $F[\alpha, K]$ (see Theorem 3.5.8), so $F(\alpha) \subseteq F(p)$. Moreover, $F(p)$ is generated by $\{1, \alpha, ..., \alpha^{n-1}\}$, where $n = \deg(p)$. Then $F[\alpha] = F[\{1, \alpha, ..., \alpha^{n-1}\}]$ already is a superfield and

$$F(p) \cong F[\{1, \alpha, ..., \alpha^{n-1}\}] = F(\alpha).$$

ii - By construction, $ev(p, \alpha, F(\alpha)[X]) \subseteq F(\beta)(\alpha)$ for all $p \in F(\alpha)[X]$. Then $F(\alpha)(\beta) \subseteq F(\beta)(\alpha)$. Reverting the argument we conclude $F(\beta)(\alpha) \subseteq F(\alpha)(\beta)$.

iii - Just use previous item and induction.

□

Corollary 3.6.15. *Let $K|_f F$ be a full extension with $\alpha \in K$ algebraic and $\deg(Irr_F(\alpha)) = n$. Then*

$$F(\alpha) \cong \{a_0 + a_1\alpha + ... + a_n\alpha^n : a_0, ..., a_n \in F\},$$

with operations in the set on the right inherited from $F[X]$.

Of course, deal with $F(p)$ is much easier to deal with the general expression

$$\bigcap\{L : L|_f F \text{ is full and } F[\alpha] \subseteq L\}$$

in the sense of make calculations. But the task of determining $F(p)$ "by hand" was already difficult in the field case. In the superfield case this difficult is accentuate, even for low degree polynomials.

ext1ex

Example 3.6.16 (Quadratic Extensions of H_3)**.** *Of course, the only irreducible polynomial of degree 2 over H_2 is $f(X) = X^2 + 2$. We want to describe some possibilities for $H_3(\sqrt{2}, K)$ (even in the case of non full extensions).*

We first use Theorem 3.5.8. Let $Irr_{H_3}(\sqrt{2}) = p(X) = X^2 + 2$ and consider $K = H_3(p)$. Lets look closely at the operations on K. Denote an element in K by $[f] \in K$, $f \in H_3[X]$. We have

$$K = \{[0], [1], [2], [X], [2X], [1 + X], [2 + X], [1 + 2X], [2 + 2X]\}.$$

By definition, for $[f], [g] \in K$ we have

$$[f] + [g] := \{[h] : h \in f + g\} \text{ and } [f] \cdot [g] := \{[h] : h \in fg\}.$$

With these rules is easy to show that $K|H_3$ is an algebraic full extension (for example, $[1 + X]$ is a root of $f(X) = X^2 + 1$). In fact, $K = H_3(\sqrt{2})$. Moreover K is not a hyperfield because

$$([1 + X])([1 + X]) = \dot{K}.$$

Now let $L = H_3 \times_h H_5$. Note that $|L| = (3 - 1)(5 - 1) + 1 = 2 \cdot 4 + 1 = 9$. Moreover, we have a morphism $i : H_3 \hookrightarrow H_5$ given by the rule $i(x) = (1, x^2)$. Denoting $\omega = (1, 2)$, we have

$$\omega^2 = (1, 2)^2 = (1, 2) \cdot (1, 2) = (1, 2^2) = (1, 4) = i(2).$$

More explicitly, doing the following identifications

$$\begin{aligned} (1,1) &\mapsto 1, & (2,1) &\mapsto a, \\ (1,2) &\mapsto \omega, & (2,2) &\mapsto b, \\ (1,3) &\mapsto 2\omega, & (2,3) &\mapsto c, \\ (1,4) &\mapsto 2, & (2,4) &\mapsto d, \end{aligned}$$

we have that

$$L \cong \{0, 1, 2, \omega, 2\omega, a, b, c, d\}$$

with the following table of operations:

$+$	ω	2ω	a	b	c	d
1	$\{1, \omega, a, b\}$	$\{1, 2\omega, a, c\}$	$K \setminus \{0\}$	$\{1, \omega, a, b\}$	$\{1, 2\omega, a, c\}$	$\{1, 2, a, d\}$
2	$\{2, \omega, b, d\}$	$\{2, 2\omega, c, d\}$	$\{1, 2, a, d\}$	$\{2, \omega, b, d\}$	$\{2, 2\omega, c, d\}$	$K \setminus \{0\}$
ω	K	$\{\omega, 2\omega, b, c\}$	$\{1, \omega, a, b\}$	$K \setminus \{0\}$	$\{\omega, 2\omega, b, c\}$	$\{2, \omega, b, d\}$
2ω	$\{\omega, 2\omega, b, c\}$	K	$\{1, 2\omega, a, c\}$	$\{\omega, 2\omega, b, c\}$	$K \setminus \{0\}$	$\{2, 2\omega, c, d\}$
a	$\{1, \omega, a, b\}$	$\{1, 2\omega, a, c\}$	K	$\{1, \omega, a, b\}$	$\{1, 2\omega, a, c\}$	$\{1, 2, a, d\}$
b	$K \setminus \{0\}$	$\{\omega, 2\omega, b, c\}$	$\{1, \omega, a, b\}$	K	$\{\omega, 2\omega, b, c\}$	$\{2, \omega, b, d\}$
c	$\{\omega, 2\omega, b, c\}$	$K \setminus \{0\}$	$\{1, 2\omega, a, c\}$	$\{\omega, 2\omega, b, c\}$	K	$\{2, 2\omega, c, d\}$
d	$\{2, \omega, b, d\}$	$\{2, 2\omega, c, d\}$	$\{1, 2, a, d\}$	$\{2, \omega, b, d\}$	$\{2, 2\omega, c, d\}$	K

$\cdot$	2	ω	2ω	a	b	c	d
2	1	2ω	ω	d	c	b	a
ω	2ω	2	1	b	d	a	c
2ω	ω	1	2	c	a	d	b
a	d	b	c	1	ω	2ω	2
b	c	d	a	ω	2	1	2ω
c	b	a	d	2ω	1	2	ω
d	a	c	b	2	2ω	ω	1

and of course, $1+1=2+2=L$, $0+x=\{x\}$, $1\cdot x=x$ and $0\cdot x=0$ for all $x\in L$. With these calculations we immediately have that L is an algebraic extension of H_3.

Now Let q be an odd prime integer greater than 3. The same calculations (with $\omega=(1,2)$) proves that $H_3\times_h H_q$ is another algebraic extension of H_3. Of course, we clearly have $H_3\times_h H_5\not\cong H_3\times_h H_q$ for $g\geq 7$. And since all these $H_3\times_h H_q$ are hyperfields and K is a superfield that is not a hyperfield we have $K\not\cong H_3\times_h H_q$ for all prime $q\geq 5$. Conclusion: we have infinite non isomorphic algebraic (and non full) hyperfield extensions of H_3.

3.7 Algebraic Closure

As expected, there are some generalizations to the classic notion of algebraic closure for fields.

alg-closure

Definition 3.7.1 (Algebraic Closures). *Let F and K be superfields.*

*i - We say that K is a **proto algebraic closure** of F if K is algebraically closed and $K|_pF$ is algebraic.*

*ii - We say that K is an **algebraic closure** of F if K is algebraically closed and $K|F$ is algebraic.*

*iii - We say that K is a **full algebraic closure** of F if K is algebraically closed and $K|_fF$ is algebraic.*

Of course, all these notions coincide if we choose a field F.

lemuinq1

Lemma 3.7.2. *Let F be a superfield and $K|_fF$ be an algebraic extension. If K is a full algebraic closure of F then $K|_fF$ is a maximal full algebraic extension.*

Proof. If $K|_fF$ is not maximal, there is a nontrivial full algebraic extension $L|_fK$. In particular, there is a nontrivial simple extension $K(\alpha)|_fK$, then K is not an algebraic closure. $\square$

Here we achieve the main result of this present paper.

algclos

Theorem 3.7.3 (Existence of the full Algebraic Closure). *Let F be a superfield. Then exists a full superfield extension $K|_fF$ such that K is algebraically closed (and then, a full algebraic closure of F). Moreover, we can choose K in order that $K|_fF$ is algebraic.*

Proof. Let F be a superfield. Consider the following set

$$A:=\{\omega_i^f : f\in F[X],\,\deg(f)\geq 1,\, i=1,...,\deg(f)\}.$$

In other words, for each f of degree greater or equal to 1, we are choosing elements $\omega_1^f, ..., \omega_{\deg(f)}^f$ to represent "some possible roots for f". For each $a \in F$, a is the root of $f_a(X) = X - a$, and hence there is an element $\omega_1^{f_a} \in A$. Let

$$\Omega = \left(\mathcal{P}(A) \setminus \bigcup_{a\in F}\{\omega_1^{f_a}\}\right) \cup F.$$

Then $F \subseteq \Omega$. Now, consider all the possible superfields that can be defined on elements of Ω. Denote the set of all such superfields by $\mathcal{E}$. Since $\mathcal{E} \subseteq \Omega$, it is in fact a set, and since $F \in \mathcal{E}$, it is a non-empty set.

Let $E|_f F$ be an almost full algebraic extension of F-generated by $\{1, \gamma, ..., \gamma^n\}$ where $\gamma \in E \setminus F$ is a root of f in $F[X]$. In other words, we have $E = F(\gamma)$. Let $\omega \in \Omega \setminus F$. We can "make the variable change" $\gamma \mapsto \omega$ and choose distinct elements for all elements in $F(\gamma)$ in order to get a field $F(\omega) \cong F(\gamma)$, such that $F \subseteq F(\omega) \subseteq \Omega$.

Then, for all almost full algebraic extension $E_j \subseteq \Omega$ obtained by the above process, we can take the set

$$S = \{E_j : j \in J\}.$$

We have $F \in S$ and S is partially ordered by inclusion.

Let $T = \{E_{kj} : k \in K\}$ be a chain in S and

$$W = \bigcup_{k\in K} E_{kj}.$$

Since W is an algebraic extension of F, we get $W \in S$. By Zorn's Lemma, there exist some maximal element $\overline{F} \in S$. We prove that $\overline{F}$ is an algebraic closure of F.

In fact, suppose that exists $f(X) \in F[X]$ such that f has no roots in $\overline{F}[X]$. Then, take $\omega \in \Omega$ such that $\omega \notin \overline{F}$ and ω is a root of $f(X)$. Consider the field $\overline{F}(\omega)$ as we did above. Then $\overline{F}(\omega)$ is an algebraic extension with $\overline{F} \subsetneq \overline{F}(\omega)$, contradicting the maximality of $\overline{F}$, which complete the proof. □

We are surprisingly able to prove the uniqueness of full algebraic closures.

uniq

Theorem 3.7.4 (Uniqueness of the full Algebraic Closure)**.** *Let F be a superfield. Let K_1, K_2 be two full algebraic closures of F. Then $K_1 \cong K_2$.*

To prove Theorem 3.7.4 we need two Lemmas. Let $L|_f F$ be a full superfield extension and N be another superfield. An **F-embedding** is a full embedding $\iota : L \to N$ such that $\iota(a) = a, a \in F$.

uniq1

Lemma 3.7.5. *Let $L|_f F$ be an algebraic full extension and $N|_f L$ another algebraic full extension, and $\overline{F}$ some full algebraic closure of F. There is a F-embedding $i : L \to \overline{F}$ and once i is picked there exists a F-embedding $N \to \overline{F}$ extending i.*

Proof. Since a full embedding $i : L \to \overline{F}$ realizes the full algebraically closed $\overline{F}$ as an algebraic extension of L (and hence as a full algebraic closure of L), by renaming the base superfield as L it suffices to just prove the first part: any strong algebraic extension admits a full embedding into a specified full algebraic closure.

Let Σ to be the set of pairs (K, i) such that $K|_f F$, $L|_f K$ and the inclusion map $i : K \to \overline{F}$ is a F-embedding. Of course, $(F, i) \in \Sigma$, and using the partial order defined by

$$(K_1, i_1) \leq (K_2, i_2) \text{ iff } K_2|_f K_1,\ L|_f K_2 \text{ and } i_2|_{k_1} = i_1,$$

we obtain that every chain has an upper bound (the superfield obtained by directed union). Then we are under the hypothesis of Zorn's Lemma and there exists a maximal element $(N, i) \in \Sigma$.

We just have to show $N = L$. Pick $\alpha \in L$, so α is algebraic over N (as it is algebraic over F). We have $N(\alpha)|_f N$ and $\overline{F}|_f N(\alpha)$. In other words, the inclusion map $i : N(\alpha) \to \overline{F}$ is a full N-embedding. By maximality of N we get $N(\alpha) = N$ for all $\alpha \in L$, which imply $N = L$. □

uniq2

Lemma 3.7.6. *Let F be a superfield and $\overline{F}$ be some full algebraic closure of F. If $\phi : \overline{F} \to \overline{F}$ is a F-embedding then ϕ is an isomorphism.*

Proof. We only need to show that ϕ is surjective. Let $\gamma \in \overline{F}$. Then there exist $p(X) \in F[X]$, saying $p(X) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ with $0 \in p(\gamma)$. Since ϕ is a F-embedding, we have

$$p^{\phi}(X) := X^n + \phi(a_{n-1})X^{n-1} + ... + \phi(a_1)X + \phi(a_0) = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0 = p(X).$$

Then $\phi(\gamma)$ is a root of $p(X)$ because

$$0 \in a_n\gamma^n + a_{n-1}\gamma^{n-1} + ... + a_1\gamma + a_0 \Rightarrow \phi(0) \in \phi(a_n\gamma^n + a_{n-1}\gamma^{n-1} + ... + a_1\gamma + a_0) \Rightarrow$$
$$0 \in a_n\phi(\gamma)^n + a_{n-1}\phi(\gamma)^{n-1} + ... + a_1\phi(\gamma) + a_0.$$

Since ϕ is a full embedding, we have a full embedding $\phi(\overline{F}) \hookrightarrow \overline{F}$. Then $\overline{F}|_f\phi(\overline{F})$. Since $\overline{F}$ is algebraically closed, every non-constant polynomial $p(X) \in F[X]$ has a root $\gamma \in \overline{F}$, and then, a root $\phi(\gamma) \in \phi(\overline{F})$. If $\phi(\overline{F}) \neq \overline{F}$, we have a contradiction with the maximality of $\phi(\overline{F})$ obtained in Lemma 3.7.2. □

Proof of Theorem 3.7.4. By Lemma 3.7.5 applied to $L = K_1$ and $\overline{F} = K_2$ (a full algebraic closed superfield equipped with a structure of algebraic extension of F), there exists a F-embedding $i_1 : K_1 \to K_2$. By the very same argument, there also exists a F-embedding $i_2 : K_2 \to K_1$. Moreover, $i_1 \circ i_2 : K_1 \to K_1$ and $i_2 \circ i_1 : K_2 \to K_2$ are F-embeddings. By Lemma 3.7.6, both $i_1 \circ i_2$ and $i_2 \circ i_1$ are isomorphisms, implying that i_1 and i_2 are also isomorphisms. □

ext2ex

Example 3.7.7. *Lets look at H_3 again. Consider $L_1 = H_3 \times_h H_5$ and $L_2 = H_3 \times_h H_7$. We do not know precisely the relations between the full algebraic closures $\overline{H_3}$, $\overline{L_1}$ and $\overline{L_2}$.*

Of course, since $L_1|H_3$ and $L_2|H_3$ are algebraic extensions of H_3, we have that $\overline{L_1}$ and $\overline{L_2}$ are algebraic closures of $\overline{H_3}$. Since L_2 is an algebraic extension of L_1, we know that $\overline{L_2}$ is an algebraic closure of L_1. But we do not know if $\overline{H_3}$, $\overline{L_1}$ and $\overline{L_2}$ are isomorphic (or not).

It is desirable to achieve explicit calculations of $\overline{F}$ for some cases: F (reduced) special hyperfields/groups, in particular $F = \{-1, 0, 1\}$ and F the special hyperfield/group associated to a Boolean algebra, etc.

3.8 Vector Spaces

Since we already have available matrices and polynomials for superrings, a natural extension for the theory is a sort of "vector space" and some linear algebra methods. We start this program here, proceeding in a very similar fashion of Hofmann's and Kunze's Linear Algebra Book ([39]).

Throughout this Section, all superfields will be considered associative.

mvec

Definition 3.8.1. *A **(multi) vector space** over a superfield F is a tuple $(V, +, \cdot, 0)$ such that $(V, +, 0)$ is an abelian multigroup and $\cdot : F \times V \to \mathcal{P}^*(V)$ is a function (which image denoted by $\cdot(\lambda, v) := \lambda v$) satisfying the following properties for all $\lambda, \mu \in F$ and all $v, w \in V$:*

MV0 - $1v = \{v\}$ *and* $0 \cdot v = \{0\}$*;*

MV1 - $\lambda(\mu v) = (\lambda\mu)v$*.*

Here we adopt the following convention: if $A \subseteq F$ *and* $v \in V$*, we set*

$$Av := \bigcup\{\lambda v : \lambda \in A\}.$$

MV2 - $\lambda(v + w) \subseteq \lambda v + \lambda w$*;*

MV3 - $(\lambda + \mu)v \subseteq \lambda v + \mu v$*.*

The vector space $(V, +, 0)$ *is* ***full*** *if the equality holds in MV2 and MV3.*

We proceed similarly to the practice used with polynomials and matrices: we omit the word "multi" and just say "vector spaces" over superfields.

Of course, we stick to vectors spaces here but it is available the Definition for "modules", just replacing superfields in Definition 3.8.1 for superring.

Here are some natural examples of vector spaces.

extvec

Proposition 3.8.2. *Let* $K|F$ *be a superfield extension with* K *and* F *associative. Then* K *is a* F*-vector space, which is full iff the extension is full.*

Proof. Here $\cdot : F \to K \to \mathcal{P}^*(K)$ is just the restriction of multiplication to F on the first coordinate. M0 is immediate and M1-M3 are consequences of the axioms of superrings. It is immediate that K is a full vector space iff $K|_f F$. □

fnvec

Theorem 3.8.3. *Let* F^n *be the usual* n*-folded cartesian product* $F \times ... \times F$*. We already know that* F^n *with the induced sum is a multigroup. Now, for* $\lambda \in F$ *and* $v = (x_1, ..., x_n) \in F^n$ *define*

$$\lambda v := (\lambda x_1, ..., \lambda x_n) := \bigcup\{(a_1, a_2, ..., a_n) : a_j \in \lambda x_j,\ j \geq 1\}.$$

Then $(F^n, +, \cdot, 0)$ *is a vector space. Moreover* F^n *is full iff* F *is full.*

Proof. We already have that F^n is commutative a superring. By the very Definition of scalar product we get $1v = v$. Now let $v, w \in F^n$, $v = (x_1, ..., x_n)$, $w = (y_1, ..., y_n)$ and $\lambda, \mu \in F$. We have

$$\begin{aligned}(\lambda + \mu)v &:= ((\lambda + \mu)x_1, ..., (\lambda + \mu)x_n) \\ &\subseteq (\lambda x_1 + \mu x_1, ..., \lambda x_n + \mu x_n) \\ &= (\lambda x_1, ..., \lambda x_n) + (\mu x_1, ..., \mu x_n) = \lambda v + \mu w.\end{aligned}$$

Similarly we conclude that $(\lambda + \mu)v \subseteq \lambda v + \mu v$.

Then F^n is a vector space which is full if F is full.

Now suppose F^n full. Then for $\alpha, \lambda, \mu \in F$ and $v = (\alpha, 0, ..., 0)$ we have

$$(\lambda\alpha + \mu\alpha, 0, ..., 0) = \lambda v + \lambda v = (\lambda + \mu)v = ((\lambda + \mu)\alpha, 0, ..., 0);$$

which means $(\lambda + \mu)\alpha = \lambda\alpha + \mu\alpha$. Similarly we conclude that $\alpha(\lambda + \mu) = \alpha\lambda + \alpha\mu$. □

Theorem 3.8.4. *Let* F *be a superfield and* $m, n \geq 1$*. Then* $M_{m\times n}(F)$ *is a vector space which is full iff* F *is full.*

Proof. This is consequence of Lemma 3.2.7, identifying F with $M_{1\times 1}(F)$. □

Theorem 3.8.5. *Let F be a superfield and $n \geq 1$. Then $F[X_1, ..., X_n]$ is a vector space which is full iff F is full.*

Proof. The argument here is similar to the one in Theorem 3.8.3. □

Definition 3.8.6 (Subspace)**.** *Let V be a F-vector space and $W \subseteq V$. We say that W is a **subspace** if $0 \in W$ and for all $w_1, w_2 \in W$ and all $\lambda \in F$ we have $w_1 + w_2 \subseteq W$ and $\lambda w_1 \subseteq W$.*

Theorem 3.8.7. *Let F be a full superfield and consider a system $Ax = 0$, $A \in M_{n\times m}(F)$. Then*

$$Sol[Ax = 0] := \{v \in M_{n\times 1}(F) : 0 \in Av\}$$

is a subspace of $M_{n\times 1}(F)$.

Proof. This is another consequence of Lemma 3.2.7. We need F full in order to conclude that if $0 \in Av$ and $0 \in Aw$ then $0 \in A(v + w) = Av + Aw$. □

Definition 3.8.8 (Spanned Subspace)**.** *Let V be a F-vector space and $A \subseteq V$. The **subspace generated by** A is defined by*

$$\langle A\rangle := \bigcap\{W \subseteq V : W \text{ is a subspace and } A \subseteq W\}.$$

Definition 3.8.9 (Linear Combination)**.** *Let V be a F-vector space, $A \subseteq V$ and $w \in V$. We say that w is a **linear combination** of elements in A if there exist $\{v_1, ..., v_n\} \subseteq A$ with*

$$w \in \sum_{j=1}^{r_1} \lambda_{j1} v_1 + ... + \sum_{j=1}^{r_n} \lambda_{jn} v_n$$

for some $\lambda_{ij} \in F$. We denote the set of linear combinations of V by

$$\mathcal{CL}(A) = \bigcup \left\{ \sum_{j=1}^{r_1} \lambda_{j1} v_1 + ... + \sum_{j=1}^{r_n} \lambda_{jn} v_n : \{v_1, ..., v_n\} \subseteq A,\ \lambda_{ij} \in F,\ r_1, ..., r_n \in \mathbb{N} \right\}.$$

If V is full, then

$$\mathcal{CL}(A) := \bigcup\{\lambda_1 v_1 + ... + \lambda_n v_n : v_i \in A,\ \lambda_i \in F,\ i = 1, ..., n,\ n \geq 1\}.$$

gen1

Theorem 3.8.10. *Let V be a F-vector space and $A \subseteq V$. Then $\langle A\rangle = \mathcal{CL}(A)$.*

Proof. We have that $\mathcal{CL}(A)$ is a subspace, which provide $\langle A\rangle \subseteq \mathcal{CL}(A)$. If $W \subseteq V$ and $A \subseteq W$, by the very Definition of subspace (and induction) we have $\mathcal{CL}(A) \subseteq W$, which provide $\mathcal{CL}(A) \subseteq \langle A\rangle$. □

gen2

Lemma 3.8.11. *Let V be a F-vector space and $A, B \subseteq V$. Then*

i - $\langle\langle A\rangle\rangle = \langle A\rangle$;

ii - if $A \subseteq B$ then $\langle A\rangle$ is a subspace of $\langle B\rangle$;

iii - if $A \subseteq B$ and for all $v \in B$, $v \in \langle A\rangle$ then $\langle A\rangle = \langle B\rangle$.

Definition 3.8.12 (Linear Independence)**.** *Let V be a F-vector space and $A\subseteq V$. We say that A is F-**linearly independent** if for all distinct $v_1,...,v_n\in A$, $n\in\mathbb{N}$, the following hold:*

$$\textit{If } 0\in\sum_{j=1}^{r_1}(\lambda_{j1}v_1)+...+\sum_{j=1}^{r_n}(\lambda_{jn}v_n) \textit{ then } 0\in\sum_{j=1}^{r_1}\lambda_{ji} \textit{ for all } i=1,...,n.$$

*and I is F-**linearly dependent** if it is not F-linearly independent.*

Definition 3.8.13 (Base)**.** *Let V be a F-vector space and $B\subseteq V$. We say that B is a F-**basis** if B is linear independent and $V=\langle B\rangle$.*

Definition 3.8.14. *We say that a F-vector space is **finitely generated** if $V=\langle S\rangle$ for some $S\subseteq V$ finite.*

basis1

Theorem 3.8.15. *Let F be a hyperfield and V be a finitely generated F-vector. If V is full then V has a basis.*

Proof. Let F be a hyperfield and V be a finitely generated F-vector space with $V=\langle v_1,...,v_n\rangle$ $(v_1,...,v_n\in V)$. If $\{v_1,...,v_n\}$ is LI we are done. If not, after a rearrangement of indexes if necessary, we can suppose without loss of generality that $v_1\in\mathcal{CL}(\{v_2,...,v_n\})$. Then (using Theorem 3.8.10 and Lemma 3.8.11) we have

$$V=\mathcal{CL}(\{v_1,...,v_n\})=\mathcal{CL}(\{v_2,...,v_n\}).$$

If $\{v_2,...,v_n\}$ we are done. If not, suppose without loss of generality that $v_2\in\mathcal{CL}(\{v_3,...,v_n\})$. Then we have

$$V=\mathcal{CL}(\{v_1,...,v_n\})=\mathcal{CL}(\{v_2,...,v_n\})=\mathcal{CL}(\{v_3,...,v_n\}).$$

Repeating this process, after a number finite of steps we arrive at a basis $\{v_k,v_{k+1},...,v_n\}$ of V for some k with $1\le k\le n$. □

Unfortunately, we do not know if, for general superfields F, all basis in a finitely generated F-vector spaces has the same dimension. In order to deal with this question, we propose the following concept.

linearly-closed

Definition 3.8.16. *Let F be superfield. We say that F is **linearly closed** if the system $Ax=0$ has at least a non trivial solution weak solution for all $A\in M_{n\times m}(F)$ with $m>n$.*

Of course, every field is a linearly closed superfield. As we will see later (Theorem 3.8.23), this is also the case for hyperbolic and double distributive hyperfields. The concept of linearly closeness is useful to get the notion of dimension for a subclass of finitely generated F-vector spaces.

Definition 3.8.17. *Let F be a linearly closed superfield and V be a full F-vector space with $V=\langle A\rangle$. We say that V is **rigidly generated** by A if for all $w\in V$ there exists $v_{i_1},...,v_{i_n}\in A$ and $\lambda_1,...,\lambda_n\in F$ with*

$$\{w\}=\lambda_1v_{i_1}+...+\lambda_nv_{i_n}.$$

basis2

Theorem 3.8.18. *Let F be a linearly closed superfield and V be a full and finitely generated F-vector space with $V=\langle v_1,...,v_n\rangle$ $(v_1,...,v_n\in V)$. If V is rigidly generated by $\{v_1,....,v_n\}$ then every linear independent subset of V has at most n elements.*

Proof. We just need to prove that if $S \subseteq V$ and $|S| > n$ then S is linearly dependent.

Let S be such set with $S = \{w_1, ..., w_m\}$, $m > n$. Since $V = \langle v_1, ..., v_n\rangle$, then there exists scalars $a_{ij} \in F$ with

$$w_j = a_{1j}v_1 + ... + a_{nj}v_n,\ j = 1, ..., m.$$

Then for all $\lambda_1, ..., \lambda_m \in F$ we get

$$\lambda_1 w_1 + ... + \lambda_m w_m = \sum_{j=1}^{m} \lambda_j w_j = \sum_{j=1}^{m} \lambda_j \left(\sum_{i=1}^{n} a_{ij} v_i\right) = \sum_{j=1}^{m}\sum_{i=1}^{n} (\lambda_j a_{ij}) v_i = \sum_{i=1}^{n} \left[\sum_{j=1}^{m} \lambda_j a_{ij}\right] v_i$$

Then $0 \in \lambda_1 w_1 + ... + \lambda_m w_m$ iff

$$0 \in \sum_{i=1}^{n} \left[\sum_{j=1}^{m} \lambda_j a_{ij}\right] v_i,$$

providing

$$0 \in \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{21} & a_{22} & \dots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_m \end{pmatrix}$$

Let

$$A = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{21} & a_{22} & \dots & a_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix}$$

Since F is linearly closed, the system $Ax = 0$ has a weak solution if $m > n$, and we have that S is linear dependent if $m > n$. □

Definition 3.8.19. *Let F be a linearly closed superfield and V be a full F-vector space. We say that $\{v_1, ..., v_n\}$ is a **rigid basis** of V if $\{v_1, ..., v_n\}$ is LI and V is rigidly generated by $\{v_1, ..., v_n\}$.*

Example 3.8.20. *For a hyperfield F, the F-vector spaces $F^n, M_{m\times n}(F)$ and $F[X_1, ..., X_n]$ are all rigidly generated by the analogous canonical basis. In fact, the respective canonical basis is a rigid basis for those spaces.*

`basis4`

Theorem 3.8.21. *Let F be a linearly closed superfield and V be a F-vector space. If B_1 and B_2 are rigid basis of V then $|B_1| = |B_2|$.*

Proof. Let $B_1 = \{v_1, ..., v_n\}$ and $B_2 = \{w_1, ..., w_m\}$. Since $V = \langle B_1\rangle$ and B_2 is linearly independent, by Theorem 3.8.18 we get $m \leq n$. Since $V = \langle B_2\rangle$ and B_1 is linearly independent, by Theorem 3.8.18 we get $n \leq m$. Then $m = n$. □

Definition 3.8.22. *Let F be a linearly closed superfield and V be a F-vector space finitely generated with a rigid basis. We define the **dimension** of V by $\dim(V) := |B|$ where $B \subseteq V$ is any rigid basis of V.*

Of course, it is not clear whether or not a superfield is linearly closed. In the sequence we provide some surprisingly examples, provenient from the structures which we were working until now: hyperbolic hyperfields, which arise naturally in the context of abstract theories of quadratic forms. In particular, there is available the machinery of K-theory for hyperbolic hyperfields ([18]).

basis5

Theorem 3.8.23. *Every hyperbolic hyperfield is a linearly closed superfield.*

Proof. First, remember that every hyperfield is full. Now, let $A \in M_{n\times m}(F)$ with $m > n$. Second, since F is a hyperfield, considering the vector space F^n, we have a full F-vector space such that for all $\lambda \in F$ and all $v \in F^n$, λv is a singleton set.

Keeping this in mind, we will construct a weak solution $b \in M_{m\times 1}(F)$ dividing the proof in some cases.

Case I - $n = 1$ (which imply $m \geq 2$). In this case, let $A \in M_{1\times m}(F)$ with

$$A = \begin{pmatrix} a_1 & a_2 & ... & a_m \end{pmatrix}$$

We need to find $x_1, ..., x_m \in F$ (not all zero) such that

$$0 \in a_1x_1 + a_2x_2 + ... + a_mx_m.$$

If $a_i = 0$ for some i, just choose $x_i = 1$ and $x_j = 0$ for all $j \neq i$. Otherwise, choose $x_i = 0$ for all $i \geq 3$, $x_2 = 1$ and $x_1 = -a_1^{-1}a_2$. Then

$$a_1x_1 + a_2x_2 + a_3x_3 + ... + a_mx_m = a_1x_1 + a_2x_2 = a_1[-a_1^{-1}a_2] + a_2 = a_2 - a_2 \text{ with } 0 \in a_2 - a_2.$$

We further refer to this tactic to find $x_1, x_2, ..., x_m$ as "the Case I method". case-I-method

* * * * * * * * *

Case II - $n = 2$ (which imply $m \geq 3$). In this case, let $A \in M_{2\times m}(F)$ with

$$A = \begin{pmatrix} a_1 & a_2 & ... & a_m \\ b_1 & b_2 & ... & b_m \end{pmatrix}$$

We need to find $x_1, ..., x_m \in F$ (not all zero) such that

$$\begin{aligned} 0 &\in a_1x_1 + a_2x_2 + ... + a_mx_m \\ 0 &\in b_1x_1 + b_2x_2 + ... + b_mx_m \end{aligned} \tag{3.3}$$

eq-01-sys-case-II

We have some cases here. If $a_j = b_j = 0$ for some j, just choose $x_j = 1$ and $x_i = 0$ for all $i \neq j$. Now let $0 \in \{a_1, ..., a_m, b_1, ..., b_m\}$, saying $b_1 = 0$ and $a_1 \neq 0$. Then we are reduced to

$$\begin{aligned} 0 &\in a_1x_1 + a_2x_2 + ... + a_mx_m \\ 0 &\in b_2x_2 + ... + b_mx_m \end{aligned} \tag{3.4}$$

eq-02-sys-case-II

Now find some $d_2, ..., d_m \in F$ (not all zero) with $0 \in b_2d_2 + ... + b_md_m$ (as in the Case I method) and choose d_1 in order to get $d_1 \in -a_1^{-1}[a_2d_2 + ... + a_md_m]$. So $(d_1, ..., d_m)$ is a non trivial weak solution of the reduced system 3.4. Now, let $0 \notin \{a_1, ..., a_m, b_1, ..., b_m\}$. If $\{(a_1, ..., a_m), (b_1, ..., b_m)\}$ is LD, saying $(b_1, ..., b_m) = \lambda(a_1, ..., a_m)$, we just need to choose $d_1, d_2, ..., d_m \in F$ not all zero (as in case I) such that $0 \in a_1d_1 + a_2d_2 + ... + a_md_m$ in order to get a solution of 3.3 for this case.

Now, suppose $0 \notin \{a_1, ..., a_m, b_1, ..., b_m\}$ and $\{(a_1, ..., a_m), (b_1, ..., b_m)\}$ LI. Since F is a hyperfield, to find a non trivial weak solution of 3.3 is equivalent to find a non trivial weak solution of

$$\begin{aligned} 0 &\in x_1 + a_1^{-1}a_2x_2 + ... + a_1^{-1}a_mx_m \\ 0 &\in x_1 + b_1^{-1}b_2x_2 + ... + b_1^{-1}b_mx_m \end{aligned}$$

Then we can suppose without loss of generality that $a_1 = b_1 = 1$, and we need to find a weak solution of

$$\begin{aligned} 0 &\in x_1 + a_2x_2 + ... + a_mx_m \\ 0 &\in x_1 + b_2x_2 + ... + b_mx_m \end{aligned} \tag{3.5}$$

eq-03-sys-case-II

Now, consider the set of systems obtained after the elementary operation $L_2 \leftarrow L_2 - L_1$:

$$\begin{aligned} 0 &\in x_1 + a_2x_2 + ... + a_mx_m \\ 0 &\in (1-1)x_1 + (b_2 - a_2)x_2 + ... + (b_m - a_m)x_m \end{aligned} \tag{3.6}$$

eq-04-sys-case-II

As in Case I, let $d_2, ..., d_m \in F$ (not all zero) with

$$0 \in (b_2 - a_2)d_2 + ... + (b_m - a_m)d_m.$$

In particular, there exist $z \in F$ with

$$z \in (a_2d_2 + ... + a_md_m) \cap (b_2d_2 + ... + b_md_m).$$

Let $x_1 = -z$. Then $(-z, d_2, d_3, ..., d_m)$ is a weak solution of both 3.5 and 3.6, completing the proof for Case II. We further refer to this tactic to find z as "the Case II method". case-II-method

$* * * \qquad * * * \qquad * * *$

Case III - $n = 3$ (which imply $m \geq 4$). In this case, let $A \in M_{3\times m}(F)$ with

$$A = \begin{pmatrix} a_1 & a_2 & ... & a_m \\ b_1 & b_2 & ... & b_m \\ c_1 & c_2 & ... & c_m \end{pmatrix}$$

We need to find $x_1, ..., x_m \in F$ (not all zero) such that

$$\begin{aligned} 0 &\in a_1x_1 + a_2x_2 + ... + a_mx_m \\ 0 &\in b_1x_1 + b_2x_2 + ... + b_mx_m \\ 0 &\in c_1x_1 + c_2x_2 + ... + c_mx_m \end{aligned} \tag{3.7}$$

eq-01-sys-case-III

Choosing $x_j = 0$ for $j \geq 5$, we are reduced to the system

$$\begin{aligned} 0 &\in a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 \\ 0 &\in b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4 \\ 0 &\in c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 \end{aligned} \tag{3.8}$$

eq-02-sys-case-III

We have some subcases to deal with:

If $a_j = b_j = c_j = 0$ for some j, just choose $x_j = 1$ and $x_i = 0$ for all $i \neq j$.

$* * *$

The second subcase is the one with two elements in $\{a_j, b_j, c_j\}$ are equal to zero for some j. Say for instance that $j = 1$ and $a_1 \neq 0$, $b_1 = c_1 = 0$ (the other cases are analogous). Our situation here is

$$\begin{aligned}
0 &\in a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 \\
0 &\in b_2x_2 + b_3x_3 + b_4x_4 \\
0 &\in c_2x_2 + c_3x_3 + c_4x_4
\end{aligned}$$

Then we just apply the Case II method 3.8 to get a solution $(d_2, ..., d_m)$ of the last two equations and for

$$d_1 \in -a_1^{-1}a_2d_2 - a_1^{-1}a_3d_3 - ... - a_1^{-1}a_md_3$$

we have that $(d_1, d_2, ..., d_m)$ is a solution of 3.7.

* * *

The third subcase is the one with for all j, only one element in $\{a_j, b_j, c_j\}$ is equal to zero. By the pigeon hole principle, one of the sets $\{a_1, a_2, a_3, a_4\}$, $\{b_1, b_2, b_3, b_4\}$ and $\{c_1, c_2, c_3, c_4\}$ has two elements equal to zero. For instance, say that $a_1 = a_4 = 0$, $b_2 = 0$ and $c_3 = 0$ (the other cases are analogous). Our situation here is

$$\begin{aligned}
0 &\in a_2x_2 + a_3x_3 \\
0 &\in b_1x_1 + b_3x_3 + b_4x_4 \\
0 &\in c_1x_1 + c_2x_2 + c_4x_4
\end{aligned}$$

with all these coefficients different from zero. Then, multiplying the first, second and third equation by a_2^{-1}, b_1^{-1} and c_1^{-1} respectively, we get

$$\begin{aligned}
0 &\in x_2 + a_2^{-1}a_3x_3 \\
0 &\in x_1 + b_1^{-1}b_3x_3 + b_1^{-1}b_4x_4 \\
0 &\in x_1 + c_1^{-1}c_2x_2 + c_1^{-1}c_4x_4
\end{aligned}$$

Then we can suppose without loss of generality that $a_2 = b_1 = c_1 = 1$, and our situation is now

$$\begin{aligned}
0 &\in x_2 + a_3x_3 \\
0 &\in x_1 + b_3x_3 + b_4x_4 \\
0 &\in x_1 + c_2x_2 + c_4x_4
\end{aligned}$$

Pick $d_1 = 1$, $d_2 = -c_2^{-1}$, $d_3 = a_3^{-1}c_2^{-1}$ and $d_4 = -b_4^{-1}a_3^{-1}b_3c_2^{-1}$. We have (using the fact that F is hyperbolic) that

$$d_2 + a_3d_3 = -c_2^{-1} + a_3(a_3^{-1}c_2^{-1}) = c_2^{-1} - c_2^{-1} = F$$

and

$$\begin{aligned}
d_1 + b_3d_3 + b_4d_4 &= 1 + b_3(a_3^{-1}c_2^{-1}) + b_4(-b_4^{-1}a_3^{-1}b_3c_2^{-1}) \\
&= 1 + a_3^{-1}b_3c_2^{-1} - a_3^{-1}b_3c_2^{-1} = F
\end{aligned}$$

and finally

$$\begin{aligned} d_1 + c_2 d_2 + c_4 d_4 &= 1 + c_2(-c_2^{-1}) + c_4(-b_4^{-1} a_3^{-1} b_3 c_2^{-1}) \\ &= 1 - 1 - a_3^{-1} b_3 b_4^{-1} c_2^{-1} c_4 = F. \end{aligned}$$

Then,

$$\begin{aligned} 0 &\in F = d_2 + a_3 d_3 \\ 0 &\in F = d_1 + b_3 d_3 + b_4 d_4 \\ 0 &\in F = d_1 + c_2 d_2 + c_4 d_4, \end{aligned}$$

which prove that (d_1, d_2, d_3, d_4) is a solution for this case.

* * *

Then fourth subcase is the one where $0 \notin \{a_j, b_j, c_j\}$ for some j. Suppose without loss of generality that $0 \notin \{a_1, b_1, c_1\}$. Since F is a hyperfield, to find a non trivial weak solution of 3.8 is equivalent to find a non trivial weak solution of

$$\begin{aligned} 0 &\in x_1 + a_1^{-1} a_2 x_2 + a_1^{-1} a_3 x_3 + a_1^{-1} a_4 x_4 \\ 0 &\in x_1 + b_1^{-1} b_2 x_2 + b_1^{-1} b_3 x_3 + b_1^{-1} b_4 x_4 \\ 0 &\in x_1 + c_1^{-1} c_2 x_2 + c_1^{-1} c_3 x_3 + c_1^{-1} c_4 x_4 \end{aligned}$$

Then we can suppose without loss of generality that $a_1 = b_1 = c_1 = 1$ and only deal with the new system

$$\begin{aligned} 0 &\in x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4 \\ 0 &\in x_1 + b_2 x_2 + b_3 x_3 + b_4 x_4 \\ 0 &\in x_1 + c_2 x_2 + c_3 x_3 + c_4 x_4 \end{aligned} \qquad \text{eq-03-sys-case-III} \quad (3.9)$$

Note that, even in this reduced system we can suppose that for $j = 2, 3, 4$ we have at most one element in $\{a_j, b_j, c_j\}$ equal to zero (because if one of the sets $\{a_2, b_2, c_2\}, \{a_3, b_3, c_3\}, \{a_4, b_4, c_4\}$ has two elements equal to zero, we are in the subcase two of the case III!). Then suppose without loss of generality that $a_2 \neq 0$, $b_3 \neq 0$ and $c_4 \neq 0$.

Here we use again the fact that F is hyperbolic: more specifically, we use that every hyperbolic hyperfield is rooted, in the sense that $\{a, b\} \subseteq a + b$ for all $a, b \in F^*$. Choose $d_2 = -a_2^{-1}$, $d_3 = -b_3^{-1}$ and $d_4 = -c_4^{-1}$. Since $-1 = a_2 d_2 = b_3 d_3 = b_4 d_4$ we have

$$\begin{aligned} -1 &\in a_2 d_2 + a_3 d_3 + a_4 d_4 \\ -1 &\in b_2 d_2 + b_3 d_3 + b_4 d_4 \\ -1 &\in c_2 d_2 + c_3 d_3 + c_4 d_4 \end{aligned}$$

Picking now $d_1 = 1$, we have

$$\begin{aligned} 1 - 1 &\subseteq d_1 + a_2 d_2 + a_3 d_3 + a_4 d_4 \\ 1 - 1 &\subseteq d_1 + b_2 d_2 + b_3 d_3 + b_4 d_4 \\ 1 - 1 &\subseteq d_1 + c_2 d_2 + c_3 d_3 + c_4 d_4 \end{aligned}$$

and then, (d_1, d_2, d_3, d_4) is a non-trivial solution of the systems 3.9, which complete the proof for Case III. We further refer to this tactic to find (d_1, d_2, d_3, d_4) as "the Case III method". case-III-method

* * *   * * *   * * *

Case IV - the general case $m > n$ (and $n \geq 3$). Just proceed by induction on m. The base cases are Case I and II and the induction step is an argument similar to the the Case III method (3.8). □

As application of these fragment of linear algebra for superfields, we get the following Theorem, which is a consequence of combining Theorem 3.6.12, Proposition 3.8.2, Theorem 3.8.18 and Theorem 3.8.23.

Theorem 3.8.24. *Let F be a linearly closed superfield and $p \in F[X]$ be an irreducible polynomial with $\deg p = n + 1$. Then $F(p)$ is a full F-vector space and $\dim(F(p)) = n + 1$.*

teolnc

Theorem 3.8.25. *Let F is a linearly closed superfield and $p \in F[X]$ be an irreducible polynomial with $\deg p = n + 1$. Then $F(p)$ is also linearly closed.*

Proof. Remember that $F(p)$ is generated by $\{1, \gamma, ..., \gamma^n\}$ with $\gamma = \overline{X}$, $n \in \mathbb{N}$. Also, we can consider n as the minimal integer such that there exist $a_0, ..., a_{n+1}$ with

$$0 \in d_0 + d_1\gamma + ... + d_{n+1}\gamma^{n+1}.$$

Let $A \in M_{m\times q}(F(p))$, saying, $A = (\alpha_{ij})$. We can write each α_{ij} as

$$\alpha_{ij} = a_{0ij} + a_{1ij}\gamma + ... + a_{nij}\gamma^n$$

for suitable $a_{kij} \in F$. Then a system $Ax = 0$ over $F(p)$ can be split into $n + 1$ systems $A_kx = 0$ over F, where $A_k = (a_{kij})$ for each $k = 0, 1, ..., n$ (in fact, $Ax = 0$ means $A_0x + \gamma A_1x + \gamma^2 A_2x + ... + \gamma^n A_nx = 0$). Since F is linearly closed, each $A_kx = 0$ has at least a non-trivial solution, providing a non-trivial solution for $Ax = 0$. □

As we can see, we had a lot of effort in order to prove Theorem 3.8.23. In this sense, we propose the following questions.

As we can see, we had a lot of effort in order to prove Theorem 3.8.23. In this sense, we propose the following questions.

Question 3.8.26.

1. *Is every hyperfield F a linearly closed superfield?*
2. *Is every full superfield F a linearly closed superfield?*
3. *What are the necessary conditions for a superfield F be a linearly closed one?*

In the context of algebraic and abstract theories of quadratic forms, there are at least two interesting Corollaries obtained applying Theorem 3.8.23 to the hyperfield $M(F) := F/_m(F^2 \setminus \{0\})$ where F is a field of characteristic not 2, or more generally, $M(G)$ for a formally real special group G (for a deeper understanding of $M(F)$ and $M(G)$, the reader can consult [47], [24], [23], [12], [17] or [45]).

cor-01

Corollary 3.8.27 (Isotropy Interpolation). *Let $K = M(F) := F/_m(F^2 \setminus \{0\})$ for a field F (of characteristic not 2) or $K = M(G)$ for a formally real special group G. Consider a matrix $A \in M_{n\times m}(K)$, saying $A = (a_{ij})$. If $m > n$, there exists $d_1, ..., d_n \in F$, not all zero, such that all the forms $\{\varphi_1, ..., \varphi_n\}$ with*

$$\varphi_i := \langle a_{i1}d_1, a_{i2}d_2, ..., a_{im}d_m\rangle$$

are isotropic.

cor-02

Corollary 3.8.28 (Hyperbolic Interpolation). *Let $K = M(F)/_m(M(F)^2 \setminus \{0\})$ where $M(F) := F/_m(F^2 \setminus \{0\})$ for a field F (of characteristic not 2) or $K = M(G)$ for a formally real reduced special group G. Consider a matrix $A \in M_{n\times m}(K)$, saying $A = (a_{ij})$. If $m > n$ is even, there exists $d_1, ..., d_n \in F$, not all zero, such that all the forms $\{\varphi_1, ..., \varphi_n\}$ with*

$$\varphi_i := \langle a_{i1}d_1, a_{i2}d_2, ..., a_{im}d_m\rangle$$

are hyperbolic.

Also in the context of abstract theories of quadratic forms, Isotropic and Hyperbolic Interpolations (3.8.27 and 3.8.28) suggests interesting questions:

Question 3.8.29.

1. *In Corollaries 3.8.27 and 3.8.28, are we able to get $d_1, ..., d_n \in F$, not all zero, such that all the* ***Pfister forms*** *$\{\varphi_1, ..., \varphi_n\}$ with*

$$\varphi_i := \langle\langle a_{i1}d_1, a_{i2}d_2, ..., a_{im}d_m\rangle\rangle$$

   are hyperbolic?

2. *Are we able to get Corollary 3.8.28 for general fields or general special-groups (not necessarily reduced)?*

As application of these fragment of linear algebra for superfields, we get the following Theorem, which is a consequence of combining Theorem 3.6.12, Proposition 3.8.2, Theorem 3.8.18 and Theorem 3.8.23.

Theorem 3.8.30. *Let F be a linearly closed superfield and $p \in F[X]$ be an irreducible polynomial with $\deg p = n+1$. Then $F(p)$ is a full F-vector space, with a rigid basis $\{1, \gamma, ..., \gamma^n\}$ ($\gamma := [X] \in F[X]/\langle p(X)\rangle$) and $\dim(F(p)) = n+1$.*

3.9 A quantifier elimination procedure

We also have a quantifier elimination procedure for any *infinite* algebraically closed associative superfield. This is a variation of Theorem 9.2.1 in [36] and a generalization of the results in [19].

Throughout this Section, all superfields will be considered associative.

lem1.1

Lemma 3.9.1 (Lemma 1.27 of [19]). *Let A be a superring.*

i - For all $n \in \mathbb{N}$ and all $a_0, ..., a_{n-1} \in A$, the sum $a_0 + ... + a_{n-1}$ and product $a_0 \cdot ... \cdot a_{n-1}$ does not depends on the order of the entries.

ii - *For every term $t(y_1,...,y_n)$ on the 2-ring language, exists variables x_{ij} such that A satisfies the formula*

$$t(y_1,...,y_n) \sqsubseteq \sum_{i<p} \prod_{j<m_i} x_{ij}.$$

Moreover, if A is a full *2-ring, it satisfies the formula*

$$t(y_1,...,y_n) =_s \sum_{i<p} \prod_{j<m_i} x_{ij}.$$

`reduc`

Lemma 3.9.2 (Lemma 3.2 of [19])**.** *Let A be a superring, $t_1(\bar{x}), t_2(\bar{x})$ be terms on the full superring language and let $v = \bar{a} : \bar{x} \to A$*

i - $t_1^A(\bar{a}) \subseteq t_2^A(\bar{a})$ *iff* $0 \in (t_2 - t_1)^A(\bar{a})$.

ii - *Given any atomic formula, $t_1(\bar{x}) \sqsubseteq t_2(\bar{x})$, there is a polynomial term $p(\bar{x}) \in R[\bar{x}]$ such that*

$$A \models_v (t_1(\bar{x}) \sqsubseteq t_2(\bar{x})) \;\leftrightarrow\; (0 \sqsubseteq p(\bar{x})).$$

Let $\mathcal{L}$ be the language of superrings. For each superring R, let $\mathcal{L}(R)$ be the language extending $\mathcal{L}$ by adding all elements of R as *strict* constant symbols. Let Γ' be the superring axioms. Let extend Γ' by (in)equalities and relations of the form

$$a_0 \neq b_0;\; c_1 = a_1.b_1;\; c_2 \in a_2 + b_2;\; a_i, b_i, c_i \in R$$

that are true in R ("the diagram of R"). Denote the set of formulas obtained by $\Gamma'(R)$. A model of $\Gamma'(R)$ is a superring that contains a subset $\overline{R} = \{\overline{a} : a \in R\}$ and $\overline{R}$ is an isomomorphic copy of R inside this model. If $R = K$ is a superfield and Γ is the superfield axioms, then a model of $\Gamma(K)$ is a superfield that contains a subset $\overline{K} = \{\overline{a} : a \in K\}$ and $\overline{K}$ is a superfield isomorphic to K. Then a model of $\Gamma(K)$ is (up to a isomorphism) a superfield containing K. Now, we extend $\Gamma(K)$ to a new set of axioms $\tilde{\Gamma}(K)$ adding axioms to obtain an algebraic closure superfield

$$\forall z_0...\forall z_n \,\exists x[0 \in z_0 + z_1x + ... + z_{n-1}x^{n-1} + x^n],\; n \geq 1. \tag{AC}$$

We add also the family of axioms $\exists z_0...\exists z_{n-1} \bigvee_{i<j<n} [z_i \neq z_j],\; n \geq 2.$

A model F of $\Gamma(K)$ is also a model of $\tilde{\Gamma}(K)$ iff F is infinite and algebraically closed. Our aim is to describe a quantifier elimination procedure for $\tilde{\Gamma}(F)$. By the reduction Lemma 3.9.2, F regards every atomic formula as equivalent modulo $\Gamma(K)$ to a polynomial "equation" $0 \in f(X_1,...,X_n)$. Since $K[\bar{X}]$ is a superdomain, a conjunction of inequations $\bigwedge_{i=1}^{m} [0 \neq g_i(\bar{X})]$ is equivalent to the "inequation" $0 \notin g_1(\bar{X})...g_n(\bar{X})$. Then, to obtain a quantifier elimination for $\tilde{\Gamma}(K)$ is sufficient eliminate Y from the formula

`qe1`

$$\exists Y[0 \in f_1(\bar{X}, Y) \wedge ... \wedge 0 \in f_m(\bar{X}, Y) \wedge 0 \notin g(\bar{X}, Y)] \tag{3.10}$$

with $f_1, ..., f_m, g \in R[X_1, ..., X_m, Y]$.

`quantfield`

Theorem 3.9.3 (Quantifier Elimination Procedure, Adapted from Theorem 3.3 of [19])**.** *Let K be an infinite superfield and $\varphi(X_1, ..., X_n, Y)$ the formula in 3.10. Then $\varphi(X_1, ..., X_n, Y)$ is equivalent modulo $\tilde{\Gamma}(R)$ to a Boolean combination of atomic formulas $\psi(X_1, ..., X_r)$, $r \geq n$.*

Proof. The proof consists in three parts:

A - Reduction to the case that only one of $f_1, ..., f_m$ involves Y. Move each conjunction that appears in (3.10) and that does not involve Y to the left of $\exists Y$ according to the rule "$\exists Y[\varphi \wedge \psi] \equiv \varphi \wedge \exists Y[\psi]$ if Y does not appear in φ". Thus we assume $\deg_Y(f_i(\bar{X}, Y)) \geq 1$, $i = 1, ..., m$ and $m \geq 2$. We now perform an induction on $\sum \deg_Y(f_i(\bar{X}, Y))$: Let $p(\bar{X}, Y)$ and $q(\bar{X}, Y)$ be multipolynomials with coefficients in R such that $0 \leq \deg_Y p(\bar{X}, Y) \leq \deg_Y q(\bar{X}, Y) = d$. Write $p(\bar{X}, Y)$ in the form

$$p(\bar{X}, Y) = a_k(\bar{X})Y^k + a_{k-1}(\bar{X})Y^{k-1} + ... + a_0(\bar{X}) \tag{3.11}$$

with $a_j \in R[\bar{X}]$. For each j with $0 \leq j \leq k$ let

$$p_j(\bar{X}, Y) = a_j(\bar{X})Y^j + a_{j-1}(\bar{X})Y^{j-1} + ... + a_0(\bar{X})$$

If $0 \notin a_j(\bar{X})$, division of $q(\bar{X}, Y)$ by $p_j(\bar{X}, Y)$ produces $q_j(\bar{X}, Y)$ and $r_j(\bar{X}, Y)$ in $R[\bar{X}, Y]$ for which

$$a_j(\bar{X})^d q(\bar{X}, Y) \subseteq q_j(\bar{X}, Y)p_j(\bar{X}, Y) + r_j(\bar{X}, Y), \tag{3.12}$$

and $\deg_Y(r_j) < \deg_Y(p_j) \leq d$. Let F be a model of $\Gamma(K)$. If $x_1, ..., x_n, y$ are elements of F such that $0 \in a_l(\bar{x})$ for $l = j+1, ..., k$ and $0 \notin a_j(\bar{x})$, then $[0 \in p(\bar{x}, y) \wedge 0 \in q(\bar{x}, y)]$ is equivalent in F to $[0 \in p_j(\bar{x}, y) \wedge 0 \in r_j(\bar{x}, y)]$. Therefore, the formula $[0 \in p(\bar{X}, Y) \wedge 0 \in q(\bar{X}, Y)]$ is equivalent modulo $\Gamma(K)$ to the formula

$$\begin{aligned}&\left(\bigvee_{j=0}^{k}[0 \in a_k(\bar{X}) \wedge ... \wedge 0 \in a_{j+1}(\bar{X}) \wedge 0 \notin a_j(\bar{X}) \wedge 0 \in p_j(\bar{X}, Y) \wedge 0 \in r_j(\bar{X}, Y)]\right)\\ &\vee [0 \in a_k(\bar{X}) \wedge ... \wedge 0 \in a_0(\bar{X}) \wedge 0 \in q(\bar{X}, Y)].\end{aligned} \tag{3.13}$$

Apply the outcome of (3.13) to $f_1(\bar{X}, Y)$ and $f_m(\bar{X}, Y)$ (of 3.10). With the rule "$\exists Y[\varphi \vee \psi] \equiv \exists Y \varphi \vee \exists Y \psi$" we have replaced (3.10) by disjunction of statements of form (3.10) in each which the sum corresponding to $\sum \deg_Y(f_i(\bar{X}, Y))$ is smaller. Using the induction assumption, we conclude that m may be taken to be at most 1.

B - Reduction to the case that $m = 0$. Continue the notation of part A which left us at the point of considering how to eliminate Y from $p(\bar{X}, Y)$ in

$$\exists Y[0 \in p(\bar{X}, Y) \wedge 0 \notin g(\bar{X}, Y)]. \tag{3.14}$$

Consider a model F of $\tilde{\Gamma}(K)$ and elements $x_1, ..., x_n \in F$. If $0 \notin p(\bar{x}, Y)$ then (since F is algebraically closed) the statement "$F \models \exists Y[0 \in p(\bar{x}, Y) \wedge 0 \notin g(\bar{x}, Y)]$" is equivalent to the statement "$p(\bar{x}, Y)$ does not divide $g(\bar{x}, Y)^k$ in $F[X]$". Therefore, with $q(\bar{X}, Y) = g(\bar{X}, Y)^k$ and in the notation of (3.11) and (3.12), formula (3.14) is equivalent modulo $\tilde{\Gamma}(K)$ to the formula

$$\begin{aligned}&\left(\bigvee_{j=0}^{k}[0 \in a_k(\bar{X}) \wedge ... \wedge 0 \in a_{j+1}(\bar{X}) \wedge 0 \notin a_j(\bar{X}) \wedge \exists Y[\in r_j(\bar{X}, Y)]]\right)\\ &\qquad \vee[0 \in a_k(\bar{X}) \wedge ... \wedge 0 \in a_0(\bar{X}) \wedge \exists Y[0 \in g(\bar{X}, Y)]]\end{aligned}$$

a disjunction of statements of form (3.10) with $m = 0$.

C - Completion of the proof. By part B we are in the point of removing Y from a statement of the form $\exists Y[0 \notin a_l(\bar{X})Y^l + a_{l-1}(\bar{X})Y^{l-1} + ... + a_0(\bar{X})]$. Since models of $\tilde{\Gamma}(K)$ are infinite superfields, this formula is equivalent modulo $\tilde{\Gamma}(K)$ to $0 \notin a_l(\bar{X}) \vee ... \vee 0 \notin a_0(\bar{X})$, completing the quantifier elimination procedure. $\square$

Chapter 4

K-theories: the rise of (universal) Inductive Graded Rings

Concerning Abstract Theories of Quadratic forms (in particular special groups and real semigroups), the references [28], [32] and [33] are central. The theory of special groups deals simultaneously reduced and non-reduced theories but focuses on rings with an "expressive amount" of invertible coefficients to quadratic forms and the theory of real semigroups consider general coefficients of a ring, but only addresses the reduced case. Both are first-order theory, thus they allow the use of model theoretic methods.

M. Marshall in [47] introduced an approach to (reduced) theory of quadratic forms through the concept of multiring [1]: this seems more intuitive for an algebraist since it encompasses (generalizes, in fact) some techniques of ordinary Commutative Algebra. Moreover, the multirings encode copies of special groups and real semigroups (see [24]) and still allows the use of model-theoretic tools, since multirings (hyperrings) endowed with convenient notion of morphisms constitutes a category that is isomorphic to a category of appropriate first-order structures.

In the recent work [17]: (i) we have considered interesting pairs (A, T) where A is a multiring and $T \subseteq A$ is a certain multiplicative subset in such a way to obtain models of abstract theories of quadratic forms (special groups and real semigroups) via natural quotients - Marshall's quotient construction and (ii) we have used this new setting to motivate a "non reduced" expansion of the theory of real semigroups to deal the formally real case, isolating axioms over pairs involving multirings and a multiplicative subset with some properties.

The uses of K-theoretic (and Boolean) methods in abstract theories of quadratic forms has been proved a very successful method, see for instance, these two papers of Dickmann and Miraglia: [27] where they give an affirmative answer to Marshall's Conjecture, and [29], where they give an affirmative answer to Lam's Conjecture.

These two central papers makes us take a deeper look at the theory of Special Groups by itself. This is not mere exercise in abstraction: from Marshall's and Lam's Conjecture many questions arise in the abstract and concrete context of quadratic forms. Even in the algebraic theory of quadratic forms, there are simple (and unsolved questions), some of them solved just in the last decade, as showed by [40].

With these two paragraphs in mind, the purpose of this Chapter is to prepare the land for further generalizations (with applications) of the "Milnor's triangle K-theory – quadratic forms

[1]The main terminology in the literature is "hyperring". Moreover, M. Marshall makes a distinction between "multiring" and "hyperrings" which is important in the context of quadratic forms. But throughout this entire work, we deal essentially with multifields/hyperfields and then, the main terminology here will be "hyperfield".

– Galois cohomology". The main results are Theorems 4.5.6 and its Corollaries, which provides interchanging formulas between the three K-theories considered here.

4.1 Milnor's K-theory

For further references, in this section we get some definitions and results about Milnor's K-theory, as developed in [52]. Before deal with Milnor's K-theory, lets make a brief summary on graded rings.

Definition 4.1.1 (Graded Ring [9]). *Let $(G, \cdot)$ be a monoid. A ring A is said to be **G-graded** if its additive group $(A, +)$ admits a decomposition in direct sum of abelian groups*

$$A = \bigoplus_{g \in G} A_g,$$

satisfying $A_g \cdot A_h \subseteq A_{g \cdot h}$ for all $g, h \in G$, or in other words,

$$a_g \in A_g,\, a_h \in A_h \Rightarrow a_g a_h \in A_{g \cdot h}\, (g, h \in G).$$

*The elements $a_g \in A_g \subseteq A$ are called **homogeneous of degree** g. Then, every element of A can be written uniquely as a sum $a = \sum_{g \in G} a_g$ of homogeneous elements $a_g \in A_g$. We call a_g of **homogeneous component of degree** g of the element a.*

*A **morphism** of G-graded rings is a ring homomorphism $\varphi : A \to B$ that respect the graduation, i.e, such that for all $g \in G$, $\varphi(A_g) \subseteq B_g$. The category of G-graded rings and its morphisms will be denoted by $Grad_G$.*

The most important cases are those when $G = \mathbb{Z}$ or $G = \mathbb{N}$. Since a $\mathbb{N}$-graded ring can be seen as a $\mathbb{Z}$-graded ring with components of negative degree equal to zero, unless we mention, we call the $\mathbb{Z}$-graded rings just by graded rings and we will denote grad := $\text{grad}_{\mathbb{Z}}$.

Example 4.1.2. *Let A be a ring. The "canonical" example of graded ring is $A[x_1, ..., x_n]$, that admits a graduation*

$$A[x_1, ..., x_n] = \bigoplus_{d \geq 0} A[x_1, ..., x_n]_d$$

when $A[x_1, ..., x_n]_d$ is the free A-module of rank $\binom{n+d-1}{d}$ with basis given by the monomials $x_1^{e_1} x_2^{e_2} ... x_n^{e_n}$ of degree $d = e_1 + ... + e_n$.

Definition 4.1.3 (Homogeneous Ideal). *Let A be a G-graded ring. An ideal $I \subseteq A$ is said to be **an homogeneous ideal** if $(I, +)$ admits a decomposition*

$$I = \bigoplus_{g \in G} (I \cap A_g).$$

Lemma 4.1.4. *Let $(G, +)$ be an abelian group, $A = \bigoplus_{g \in G} A_g$ a G-graded ring and $I \subseteq A$ an ideal. For each element $a \in A$, denotes by $a_g \in A_g$ its homogeneous component of degree g. Are equivalent:*

i - I is an homogeneous ideal;

ii - for all $a \in A$,

$$a \in I \Leftrightarrow a_g \in I \text{ for all } g \in G;$$

iii - I is generated by homogeneous elements (possibly of different degrees).

Proof. (i)⇔(ii) and (ii)⇒(iii) are direct consequences of the definitions involved in. For (iii)⇒(ii), suppose that I is generated by homogeneous elements a_i (i in some set of index Λ) and let $a \in I$. Then we can write $a = b_1 a_{i_1} + ... + b_n a_{i_n}$ with $b_i \in A = \bigoplus_{g \in G} A_g$. Expanding each $b_i = \sum_{g \in G} b_{ig}$ as sum of its homogeneous components in $b_{ig} \in A_g$, the degree g term of a is

$$a_g = b_{1(g-\deg(a_{i_1})} a_{i_1} + .. + b_{n(g-\deg(a_{i_n})} a_{i_n} \in I.$$

□

Lemma 4.1.5 (Generating Homogeneous Ideals)**.** *Let $A = \bigoplus_{n \geq 0} A_n$ be a graded ring. Let $a \in A_0$. Consider the following recursive construction:*

$$I_0 := \langle a \rangle \subseteq A_0 \, (\text{the ideal generated by } a \text{ on } A_0)$$
$$I_n := \langle x \cdot y : x \in I_p, \, y \in I_q \text{ with } p + q = n \rangle \subseteq A_n.$$

Then $I = (I_n)_{n \geq 0}$ is an homogeneous ideal of A, called ***the homogeneous ideal generated by*** *a.*

So lets present the basic definitions and properties of Milnor's K-theory (as described in [52]).

milkt

Definition 4.1.6 (The Milnor's K-theory of a Field [52])**.** *For a field F (of characteristic not 2), K_*F is the graded ring*

$$K_*F = (K_0F, K_1F, K_2F, ...)$$

defined by the following rules: $K_0F := \mathbb{Z}$. K_1F is the multiplicative group $\dot{F}$ written additively. With this purpose, we fix the canonical "logarithm" isomorphism

$$l : \dot{F} \to K_1F,$$

where $l(ab) = l(a) + l(b)$. Then K_nF is defined to be the quotient of the tensor algebra

$$K_1F \otimes K_1F \otimes ... \otimes K_1F \, (n \text{ times})$$

by the (homogeneous) ideal generated by all $l(a) \otimes l(1-a)$, with $a \neq 0, 1$. We also have the reduced K-theory graded ring $k_*F = (k_0F, k_1F, ..., k_nF, ...)$, which is defined by the rule $k_nF := K_nF/2K_nF$ for all $n \geq 0$.

With these definitions, the K-theory structure gives us the following three basic Lemmas:

Lemma 4.1.7 (1.1 [52])**.** *For every $\xi \in K_mF$ and $\eta \in K_nF$, the identity*

$$\eta\xi = (-1)^{mn} \xi\eta$$

is valid in $K_{n+m}F$.

Lemma 4.1.8 (1.2 [52])**.** *The identity $l(a) \otimes l(a) = l(a) \otimes l(-1)$ is valid for every $l(a) \in K_1F$.*

Lemma 4.1.9 (1.3 [52])**.** *If the sum $a_1 + ... + a_n$ of non-zero field elements is equal to either 0 or 1, then $l(a_1) \otimes ... \otimes l(a_n) = 0$.*

Theorem 4.1.10 (Theorem 4.1 of [52])**.** *there is only one morphism*

$$s_n : k_nF \to I^nF/I^{n+1}F$$

which carries each product $l(a_1)...l(a_n)$ in $K_nF/2K_nF$ to the product $(\langle a_1\rangle - \langle 1\rangle)...(\langle a_n\rangle - \langle 1\rangle)$ modulo $I^{n+1}F$.

These morphisms determines a surjective $s_* : k_*F \to W_g(F)$, where

$$W_g(F) = (WF/IF, IF/I^2F, ..., I^nF/I^{n+1}F, ...).$$

For a field F, let F_s be the a separable closure of F and $G_F = \mathrm{Gal}(F_s)$. Then, the exact sequence

$$1 \longrightarrow \{\pm 1\} \longrightarrow \dot{F}_s \xrightarrow{2} \dot{F}_s \longrightarrow 1$$

is taken to the following exact sequence

$$H^0(G_F, \dot{F}_s) \xrightarrow{2} H^0(G_F, \dot{F}_s) \xrightarrow{\delta} H^1(G_F, \{\pm 1\}) \longrightarrow H^1(G_F, \dot{F}_s)$$

of cohomology groups. Identifying the two first groups with $\dot{F}$, and $\{\pm 1\}$ with $\mathbb{Z}/2\mathbb{Z}$ and applying Hilbert's 90, we have

$$\dot{F} \xrightarrow{2} \dot{F} \xrightarrow{\qquad\delta\qquad} H^1(G_F, \mathbb{Z}/2\mathbb{Z}) \longrightarrow 0\ .$$

The quotient $\dot{F}/\dot{F}^2$ is identified with k_1F.

Theorem 4.1.11 (Lemma 6.1 of [52])**.** *The isomorphism $l(a) \mapsto \delta(a)$ from $K_1F/2K_1F$ to $H^1(G_F, \mathbb{Z}/2\mathbb{Z})$ admits a unique extension to a graded ring morphism*

$$h_f : k_*F \to H^*(G_F, \mathbb{Z}/2\mathbb{Z}).$$

Milnor's Conjecture consists to say that s and h are graded rings isomorphisms, which makes the fuctors $K_*F/2K_*F, W_g(F), H^*(G, \mathbb{Z}/2\mathbb{Z})$ isomorphic.

4.2 Dickmann-Miraglia K-theory for Special Groups

There are some generalizations of Milnor's K-theory. In the quadratic forms context, maybe the most significant one is the Dickmann-Miraglia K-theory of Special Groups. It is a main tool in the proof of Marshall's and Lam's Conjecture. In this section, we get some definitions and results from [28] and [30].

`defn:ksg`

Definition 4.2.1 (The Dickmann-Miraglia K-theory [30])**.** *For each special group G (written multiplicatively) we associate a graded ring*

$$k_*G = (k_0G, k_1G, ..., k_nG, ...)$$

as follow: $k_0G := \mathbb{F}_2$ and $k_1G := G$ written additively. With this purpose, we fix the canonical "logarithm" isomorphism $\lambda : G \to k_1G$, $\lambda(ab) = \lambda(a) + \lambda(b)$. Observe that $\lambda(1)$ is the zero of k_1G and k_1G has exponent 2, i.e, $\lambda(a) = -\lambda(a)$ for all $a \in G$. In the sequel, we define k_*G by the quotient of the $\mathbb{F}_2$-graded algebra

$$(\mathbb{F}_2, k_1G, k_1G \otimes_{\mathbb{F}_2} k_1G, k_1G \otimes_{\mathbb{F}_2} k_1G \otimes_{\mathbb{F}_2} k_1G, ...)$$

by the (graded) ideal generated by $\{\lambda(a)\otimes\lambda(ab),\ a\in D_G(1,b)\}$*. In other words, for each* $n\geq 2$*,*

$$k_nG := T^n(k_1G)/Q^n(G),$$

where

$$T^n(k_1G) := k_1G\otimes_{\mathbb{F}_2} k_1G\otimes_{\mathbb{F}_2} ...\otimes_{\mathbb{F}_2} k_1G$$

and $Q^n(G)$ *is the subgroup generated by all expressions of type* $\lambda(a_1)\otimes\lambda(a_2)\otimes...\otimes\lambda(a_n)$ *such that for some* i *with* $1\leq i<n$*, there exist* $b\in G$ *such that* $a_i\in D_G(1,b)$ *and* $a_i=a_{i+1}b$*, which in symbols, means*

$$\begin{aligned}Q^n(G) := \langle\{\lambda(a_1)\otimes\lambda(a_2)\otimes...\otimes\lambda(a_n):\ &\textit{exists } 1\leq i<n \textit{ and } b\in G\\ &\textit{such that } a_i=a_{i+1}b \textit{ and } a_i\in D_G(1,b)\}\rangle.\end{aligned}$$

Since $\lambda(a)+\lambda(a)=0$ for all $a\in k_1G$, follow that $\eta+\eta=0$ for all $\eta\in k_nG$, so this is a group of exponent 2. Moreover, for all $a,b\in G$,

$$\overline{\lambda(a)\otimes\lambda(ab)}=\overline{\lambda(a)\otimes[\lambda(a)+\lambda(b)]}=\overline{\lambda(a)\otimes\lambda(a)+\lambda(a)\otimes\lambda(b)}=\overline{\lambda(a)\otimes\lambda(a)}+\overline{\lambda(a)\otimes\lambda(b)},$$

hence

$$a\in D_G(1,b)\Rightarrow\overline{\lambda(a)\otimes\lambda(ab)}=\overline{0}\text{ in }k_2G,$$

or equivalently, $\overline{\lambda(a)\otimes\lambda(a)}=\overline{\lambda(a)\otimes\lambda(b)}$ in k_2G.

Before we proceed, lets make some abbreviations/simplifications to make the reading of this work more easy and comfortable. Firstly, whenever possible, we will omit the over line that indicates the equivalence classes. For example, the affirmation "$\overline{\lambda(a)\otimes\lambda(a)}=\overline{\lambda(a)\otimes\lambda(b)}$ in k_2G" will be expressible in the simplified manner by "$\lambda(a)\otimes\lambda(a)=\lambda(a)\otimes\lambda(b)$ in k_2G".

Moreover, we will denote "$\lambda(a_1)\otimes\lambda(a_2)\otimes...\otimes\lambda(a_n)$" simply by "$\lambda(a_1)\lambda(a_2)...\lambda(a_n)$". Sure, $k_*(G)$ is a graded ring, and in particular, a ring, so that we are able to multiply elements $\eta\in k_nG$, $\tau\in k_mG$. Whenever we want to do this, we will denote $\eta\cdot\tau$, in order to avoid confusion with the simplifications described above.

Finally, since we only take tensorial products with parameters in $\mathbb{F}_2$, we abbreviate "$A\otimes_{\mathbb{F}_2}B$" simply by "$A\otimes B$". In this way, $T^n(k_1G)$ we will be denoted simply by

$$T^n(k_1G)=k_1G\otimes k_1G\otimes...\otimes k_1G.$$

Next, we have a result that approximate Dickmann-Miraglia's K-theory with the Milnor's reduced K-theory:

2.1kt

Proposition 4.2.2 (2.1 [30])**.** *Let* G *be a special group,* $x,y,a_1,...,a_n\in G$ *and* σ *be a permutation on* n *elements.*

a - In k_2G*,* $\lambda(a)^2=\lambda(a)\lambda(-1)$*. Hence in* k_mG*,* $\lambda(a)^m=\lambda(a)\lambda(-1)^{m-1}$*,* $m\geq 2$*;*

b - In k_2G*,* $\lambda(a)\lambda(-a)=\lambda(a)^2=0$*;*

c - In k_nG*,* $\lambda(a_1)\lambda(a_2)...\lambda(a_n)=\lambda(a_{\sigma1})\lambda(a_{\sigma2})...\lambda(a_{\sigma n})$*;*

d - For $n\geq 1$ *and* $\xi\in k_nG$*,* $\xi^2=\lambda(-1)^n\xi$*;*

e - If G *is a reduced special group, then* $x\in D_G(1,y)$ *and* $\lambda(y)\lambda(a_1)...\lambda(a_n)=0$ *implies*

$$\lambda(x)\lambda(a_1)\lambda(a_2)...\lambda(a_n)=0.$$

An element $a \in G$ induces a graded morphism of degree 1, $\omega^a = \{\omega^a_n\}_{n\geq 1} : k_*G \to k_*G$, where $\omega^a_n : k_nG \to k_nG$ is the multiplication by $\lambda(-a)$. When $a = -1$, we write

$$\omega = \{\omega_n\}_{n\geq 1} = \{\omega^{-1}_n\}_{n\geq 1} = \omega^{-1}.$$

The Lemma 4.2.3 below generalizes Proposition 5.10 of [59]. Firstly, lets establish some notation. For $n \geq 0$ denote $P(n) := \mathcal{P}(\{0, ..., n-1\}) \setminus \{\emptyset\}$ and for $0 \leq i \leq n-1$, denote $P(n,i) := \{X \in P(n) : i \in X\}$. Now, let G be a pre-special group and $\{a_0, ..., a_{n-1}\} \subseteq G$ $\mathbb{F}_2$-linearly independent. If $S \in P(n)$ we denote

$$a_S := a_0^{\varepsilon_0} ... a_{n-1}^{\varepsilon_{n-1}},$$

where $\varepsilon_0 \in \{0,1\}$ for all $i = 0, .., n-1$ and $\varepsilon_i = 1$ if and only if $i \in S$. Remember that by the very definition of $k_n(G)$,

$$k_n(G) := [k_1(G) \otimes k_1(G)]/M,$$

where M is the subgroup of $k_1(G) \otimes k_1(G)$ generated by

$$\{\lambda(a)\lambda(b) : a \in D_G(1,b),\ a,b \in G\}.$$

fixsg2-ktheory

Lemma 4.2.3. *Let G be a pre-special group and $\{a_0, ..., a_{n-1}\} \subseteq G$ $\mathbb{F}_2$-linearly independent. Are equivalent:*

i - There exists $\{b_0, ..., b_{n-1}\} \subseteq G$ such that

$$\sum_{k<n} \lambda(a_k)\lambda(b_k) = 0 \text{ in } k_2(G).$$

ii - There exists subsets $\{c_0, ..., c_{m-1}\}, \{d_0, ..., d_{n-1}\}$ of G with $m \geq n$ such that

(a) $\{c_0, ..., c_{m-1}\}$ is linearly independent and $c_i = a_i$ for all $i < n$;

(b) $d_i = b_i$ for all $i < n$ and $d_i = 1$ for $i = n, ..., m-1$.

(c) For all $x \in C := [c_0, ..., c_{m-1}]$, there is some $r_x \in D_G(1,x)$ such that for each $i < m$

$$d_i = \prod_{x \in C_i} r_x$$

where

$$C_i = \left\{ \prod_{k<m} c_k^{\varepsilon_k} : \varepsilon_k \in \{0,1\} \text{ and } \varepsilon_i = 1 \right\}.$$

In other words, C_i is "counting" all products $c_0^{r_0} ... c_i^1 ... c_{m-1}^{r_{m-1}}$. Since for all $x \in C := [c_0, ..., c_{m-1}]$ there exist $S \in P(m)$ such that

$$x = \prod_{i \in S} c_i := c_S.$$

Denoting r_x by r_S we can rewrite

$$d_i = \prod_{x \in C_i} r_x = \prod_{S \in P(m)} r_S.$$

Proof of Lemma4.2.3. (i) $\Rightarrow$ (ii). Let

$$\sum_{k<n}\lambda(a_k)\lambda(b_k)=0 \text{ in } k_2(G).$$

Then there exist $u_0,...,u_{p-1},v_0,...,v_{p-1}\in G$ such that $v_i\in D_G(1,u_i)$ for $i=0,...,p-1$ and

$$\sum_{k<n}\lambda(a_k)\lambda(b_k)=\sum_{k<p}\lambda(u_k)\lambda(v_k) \text{ in } k_1(G)\otimes k_1(G).$$

Enlarge the set $\{a_0,...,a_{n-1}\}$ to a base $\{c_0,...,c_{m-1}\}$ of $[\{a_0,...,a_{n-1},u_0,...,u_{p-1}\}]$, with $c_i=a_i$ for all $i<n$. For all $x\in C:=[c_0,...,c_{m-1}]$ there exist an unique $S\in P(m)$ such that

$$x=\prod_{i\in S}c_i:=c_S.$$

Moreover, since $\{c_0,...,c_{m-1}\}$ is a basis, for each $i=0,...,p-1$ there is only one $S_i\in P(m)$ such that

$$u_i=c_{S_i}.$$

For each $S\in P(m)$, set

$$r_S:=\prod_{\substack{\text{those } j \text{ with}\\ S_j=S}}v_j.$$

If no $S_j=S$, set $r_S=1$. Note that if there is an index j with $S=S_j$, this index must be unique (because the expression $u_i=c_{S_i}$ is unique). Then by construction $r_S\in D_G(1,c_S)$ and in $k_2(G)$ we get

$$\begin{aligned}
\sum_{k<m}\lambda(a_k)\lambda(b_k)&=\sum_{k<n}\lambda(c_k)\lambda(d_k)=\sum_{k<p}\lambda(u_k)\lambda(v_k)\\
&=\sum_{S\in P(m)}\lambda\left(\prod_{\substack{\text{those } j \text{ with}\\ S_j=S}}c_j\right)\lambda(v_j)\\
&=\sum_{S\in P(m)}\sum_{\substack{\text{those } j \text{ with}\\ S_j=S}}\lambda(c_j)\lambda(v_j)\\
&=\sum_{S\in P(m)}\lambda(c_S)\lambda\left(\prod_{\substack{\text{those } j \text{ with}\\ S_j=S}}v_S\right)\\
&=\sum_{S\in P(m)}\lambda(c_S)\lambda(r_S)=\sum_{S\in P(m)}\sum_{k\in S}\lambda(c_k)\lambda(r_S)\\
&=\sum_{k<m}\lambda(c_k)\lambda\left(\prod_{S\in P(n)}r_S\right).
\end{aligned}$$

Since $\{c_0, ..., c_{m-1}\}$ is a basis, it follows that

$$d_i = \prod_{S\in P(n)} r_S$$

as desired.

(ii)⇒(i). Under the hypothesis of (ii) we get

$$\begin{aligned}\sum_{k<n}\lambda(a_k)\lambda(b_k) &= \sum_{k<m}\lambda(c_k)\lambda(d_k) = \sum_{k<m}\lambda(c_k)\lambda\left(\prod_{S\in P(n)} r_S\right) \\ &= \sum_{k<m}\sum_{S\in P(m)}\lambda(c_k)\lambda(r_S) = \sum_{S\in P(m)}\sum_{k<m}\lambda(c_i)\lambda(r_S) \\ &= \sum_{S\in P(m)}\lambda(c_S)\lambda(r_S) = 0.\end{aligned}$$

□

2.4kt

Definition 4.2.4 (2.4 [30]).

a - A reduced special group is [MC] if for all $n \leq 1$ and all form φ over G,

$$\text{For all } \sigma \in X_G, \text{ if } \sigma(\varphi) \equiv 0 \, mod \; 2^n \text{ then } \varphi \in I^nG.$$

b - A reduced special group is [SMC] if for all $n \geq 1$, the multiplication by $\lambda(-1)$ is an injection of k_nG in $k_{n+1}G$.

An useful criteria for a reduced special group be [SMC] is given by:

2.5kt

Proposition 4.2.5 (2.5 [30]). *Let G be a reduced special group. Are equivalent:*

a - G is SMC;

b - For all $n \geq 1$, $\varepsilon_G : k_nG \to B_G$ is injective.

Then, if G is SMC, then ε_G is an isomorphism between k_nG and the subgroup $B_G(n)$ of B_G, for all $n \geq 1$.

2.6kt

Proposition 4.2.6 (2.6 [30]). *Let G be a formally real special group and $f : H \to G$ a complete embedding. If H is [SMC], then f_* is a graded ring monomorphism such that, for all $n \geq 0$, f_n is injective.*

An inductive system of special groups

$$\mathcal{G} = (G_i; \{f_{ij} : i \leq j \in I\}),$$

provides an inductive system of graded ring, which nodes are k_*G_i and morphisms are

$$(f_{ij})_* : k_*G_i \to k_*G_j, \text{ for } i \leq j \text{ in } I.$$

4.5kt

Theorem 4.2.7 (4.5 [30]). *Let $\mathcal{G} = (G_i; \{f_{ij} : i, j \in I, i \leq j\})$ an inductive system of special groups over a directed poset I and $(G; \{f_i : i \in I\}) = \varinjlim \mathcal{G}$. Then $k_*G \cong \varinjlim_{i\in I} k_*G_i$.*

4.6kt

Corollary 4.2.8 (4.6 [30]). *The inductive limit of SMC groups is SMC.*

If S, T are $\mathbb{F}_2$-graded algebras with $S_0 = T_0 = \mathbb{F}_2$, the **direct sum**, $S \oplus T$, is the sequence of groups

$$(S \oplus T)_0 = \mathbb{F}_2 \text{ and } (S \oplus T)_n = S_n \oplus T_n,\ n \geq 1,$$

with the product defined by the rule $(x, y) \cdot (u, v) = (xu, yv)$. The $\mathbb{F}_2$-action on $S_n \oplus T_n$ is the usual action of $\mathbb{F}_2$-modules.

5.1kt

Theorem 4.2.9 (5.1 [30]). *Let $G_1, ..., G_m$ be special groups and $\prod_{i=1}^m G_i$. Then there exists a graded morphism*

$$\gamma : k_*P \to \bigoplus_{i=1}^m k_*G_i,$$

defined on the generators by the rule

$$\gamma_n(\lambda(a_1)...\lambda(a_n)) = \langle \lambda(\pi_1(a_1))...\lambda(\pi_1(a_n))...\lambda(\pi_m(a_1))...\lambda(\pi_m(a_n))\rangle$$

where $\pi_i : P \to G_i$ is the canonical projection, $i = 1, ..., m$. Moreover, γ send the multiplication by $\lambda(-1, ..., -1)$ on P in the product $\lambda(-1)...\lambda(-1)$ in $\bigoplus_{i=1}^m k_*G_i$.

5.4kt

Corollary 4.2.10 (5.4 [30]). *The finite product of SMC groups is SMC.*

5.6kt

Definition 4.2.11 (5.6 [30]). *Let $\{G_i\}_{i\in I}$ be a family of special groups. Denote by $\bigoplus_{i\in I}^* G_i$ the following pre-special subgroup of $G = \prod_{i\in I} G_i$:*

$$\bigoplus_{i\in I}^* G_i = \{x \in G : \textit{exists } J \subseteq I \textit{ finite such that } x_i = \pm 1,\ \forall i \in I \setminus J\}$$

with the special relation induced by the relation on G and $-1 = -1_G$. Such pre-special group will be called the SG-sum of the family $\{G_i\}_{i\in I}$.

In general, we do not have a canonical SG-embedding from G into $G \times H$. On the other side, if we introduce a $\mathbb{Z}_2$ factor we can get around this situation. Let $I \subseteq J$ be finite sets and G_j, $j \in J$ be formally real special groups. Consider

$$G_J := \prod_{j\in J} G_j,\ G_I := \prod_{i\in I} G_i.$$

Let $\{G_i\}_{i\in I}$ be a family of formally real special groups. For each subset $A \subseteq I$, let $G_A = \prod_{i\in A} G \times \mathbb{Z}_2$. If $A, B \subseteq I$ are finite subsets with $A \subseteq B$, we have a complete embedding $\alpha_{AB} : G_A \to G_B$. Since the set $\mathcal{P}_{Fin}(I)$ of finite parts of I with the inclusion order is up direct, we have the following inductive system of formally real special groups:

$$\mathcal{G} = (G_A; \{\alpha_{AB} : A, B \in \mathcal{P}_{Fin}(I),\ A \subseteq B\}).$$

5.7kt

Theorem 4.2.12 (5.7 [30]). *Let $\{G_i\}_{i\in I}$ be an infinite family of formally real special groups. Denote $S = \bigoplus_{i\in I}^* G_i$. With the above notations, we have $S = \varinjlim \mathcal{G}$. Moreover:*

a - $k_*S = \varinjlim \mathcal{K}\mathcal{G}$, where $\mathcal{K}$ is the inductive system of the K-theory rings associated to $\mathcal{G}$;

b - The SG-sum of SMC groups is SMC.

6.8kt

Proposition 4.2.13 (6.8 [30])**.** *Every extension of a SMC-group is SMC.*

6.10kt

Theorem 4.2.14 (6.10 [30])**.** *Let G be a special group and Δ a group of exponent 2 finite or countable, of dimension $d \geq 1$ where considered as a $\mathbb{F}_2$-vector space. For each $n \geq 1$*

$$k_nG[\Delta] = \begin{cases} \bigoplus_{j=0}^{d} (k_nG)^{\binom{d}{j}}, \text{ if } d \text{ is finite;} \\ k_nG \bigoplus \left[\bigoplus_{j=1}^{n} \left(\bigoplus_{d\geq 1} k_{n-j}G \right) \right], \text{ if } d \text{ is countable infinite.} \end{cases}$$

4.3 The K-theory for Multifields/Hyperfields

In this Section we introduce the notion of K-theory of a hyperfield essentially repeating the construction in 4.1.6 replacing the word "field" by "hyperfield" and explore some of this basic properties. In particular, Theorem 4.3.8 is an extension of a result [59], that gives us some evidence, that apart from the obvious resemblance, more technical aspects of this new theory can be developed (but with other proofs) in multi-structure setting in parallel with classical K-theory.

Definition 4.3.1 (The K-theory of a Hyperfield)**.** *For a hyperfield F, K_*F is the graded ring*

$$K_*F = (K_0F, K_1F, K_2F, ...)$$

defined by the following rules: $K_0F := \mathbb{Z}$. K_1F is the multiplicative group $\dot{F}$ written additively. With this purpose, we fix the canonical "logarithm" isomorphism

$$\rho : \dot{F} \to K_1F,$$

where $\rho(ab) = \rho(a) + \rho(b)$. Then K_nF is defined to be the quotient of the tensor algebra

$$K_1F \otimes K_1F \otimes ... \otimes K_1F \ (n \text{ times})$$

by the (homogeneous) ideal generated by all $\rho(a) \otimes \rho(b)$, with $a \neq 0, 1$ and $b \in 1 - a$.

In other words, for each $n \geq 2$,

$$K_nF := T^n(K_1F)/Q^n(K_1(F)),$$

where

$$T^n(K_1F) := K_1F \otimes_{\mathbb{Z}} K_1F \otimes_{\mathbb{Z}} ... \otimes_{\mathbb{Z}} K_1F$$

and $Q^n(K_1(F))$ is the subgroup generated by all expressions of type $\rho(a_1) \otimes \rho(a_2) \otimes ... \otimes \rho(a_n)$ such that $a_i \in 1 - a_j$ for some i, j with $1 \leq i, j \leq n$.

To avoid carrying the over line symbol, we will adopt all the conventions used in Dickmann-Miraglia's K-theory (as explained in above Definition 4.2.1). Just as it happens with the previous K-theories, a generic element $\eta \in K_nF$ has the pattern

$$\eta = \rho(a_1) \otimes \rho(a_2) \otimes ... \otimes \rho(a_n)$$

for some $a_1, ..., a_n \in \dot{F}$, with $a_i \in 1 - a_{i+1}$ for some $1 \leq i < n$. Note that if F is a field, then "$b \in 1 - a$" just means $b = 1 - a$, and the hyperfield and Milnor's K-theory for F coincide.

The very first task, is to extend the basic properties valid in Milnor's and Dickmann-Miraglia's K-theory to ours. Here we already need to restrict our attention to hyperbolic hyperfields:

bp1

Lemma 4.3.2 (Basic Properties I)**.** *Let F be an hyperbolic hyperfield. Then*

a - $\rho(1)=0$.

b - For all $a\in\dot{F}$, $\rho(a)\rho(-a)=0$ *in* K_2F.

c - For all $a,b\in\dot{F}$, $\rho(a)\rho(b)=-\rho(b)\rho(a)$ *in* K_2F.

d - For every $a_1,...,a_n\in\dot{F}$ *and every permutation* $\sigma\in S_n$,

$$\rho(a_1)...\rho(a_i)...\rho(a_n)=sgn(\sigma)\rho(a_1)...\rho(a_n)\ in\ K_nF.$$

e - For every $\xi\in K_mF$ *and* $\eta\in K_nF$, $\eta\xi=(-1)^{mn}\xi\eta$ *in* $K_{m+n}F$.

f - For all $a\in\dot{F}$, $\rho(a)^2=\rho(a)\rho(-1)$.

Proof.

a - Is an immediate consequence of the fact that ρ is an isomorphism.

b - Since F hyperbolic, $1-1=F$. Then $-a^{-1}\in 1-1$ for all $a\in\dot{F}$, and hence, $-1\in -1+a^{-1}$. Multiplying this by $-a$, we get $a\in 1-a$. By definition, this imply $\rho(a)\rho(-a)=0$.

c - By item (b), $\rho(ab)\rho(-ab)=0$ in K_2F. But

$$\begin{aligned}\rho(ab)\rho(-ab)&=\rho(a)\rho((-a)b)+\rho(b)\rho((-b)a)\\&=\rho(a)\rho(-a)+\rho(a)\rho(b)+\rho(b)\rho(-b)+\rho(b)\rho(a)\\&=\rho(a)\rho(b)+\rho(b)\rho(a).\end{aligned}$$

From $\rho(a)\rho(b)+\rho(b)\rho(a)=\rho(ab)\rho(-ab)=0$, we get the desired result $\rho(a)\rho(b)=-\rho(a)\rho(b)$ in K_2F.

d - This is a consequence of item (c) and an inductive argument.

e - This is a consequence of item (d) and an inductive argument, using the fact that an element in K_nF has pattern

$$\eta=\rho(a_1)\otimes\rho(a_2)\otimes...\otimes\rho(a_n)$$

for some $a_1,...,a_n\in\dot{F}$, with $a_i\in 1-a_j$ for some $1\le i<j\le n$.

f - Follow from the fact that F is hyperbolic i.e, for all $a\in\dot{F}$, $a\in 1-1$.

□

An element $a\in\dot{F}$ induces a morphism of graded rings $\omega^a=\{\omega^a_n\}_{n\ge1}:K_*F\to K_*F$ of degree 1, where $\omega^a_n:K_nF\to K_{n+1}F$ is the multiplication by $\lambda(-a)$. When $a=-1$, we write

$$\omega=\{\omega_n\}_{n\ge1}=\{\omega^{-1}_n\}_{n\ge1}=\omega^{-1}.$$

3.3ktmultiadap

Proposition 4.3.3 (Adapted from 3.3 of [30]). *Let F, K be hyperbolic hyperfields and $\varphi : F \to L$ be a morphism. Then φ induces a morphism of graded rings*

$$\varphi_* = \{\varphi_n : n \geq 0\} : K_*F \to K_*L,$$

where $\varphi_0 = Id_{\mathbb{Z}}$ and for all $n \geq 1$, φ_n is given by the following rule on generators

$$\varphi_n(\rho(a_1)...\rho(a_n)) = \rho(\varphi(a_1))...\rho(\varphi(a_n)).$$

Moreover if φ is surjective then φ_* is also surjective, and if $\psi : L \to M$ is another morphism then

a - $(\psi \circ \varphi)_* = \psi_* \circ \varphi_*$ and $Id_* = Id$.

b - For all $a \in \dot{F}$ the following diagram commute:

$$\begin{tikzcd} K_nF \arrow[r, "\omega_n^a"] \arrow[d, "\varphi_n"'] & K_{n+1}F \arrow[d, "\varphi_{n+1}"] \\ K_nL \arrow[r, "\omega_n^{\varphi(a)}"'] & K_{n+1}L \end{tikzcd}$$

c - If $\varphi(1) = 1$ then for all $n \geq 1$ the following diagram commute:

$$\begin{tikzcd} K_nF \arrow[r, "\omega_n^{-1}"] \arrow[d, "\varphi_n"'] & K_{n+1}F \arrow[d, "\varphi_{n+1}"] \\ K_nL \arrow[r, "\omega_n^{-1}"'] & K_{n+1}L \end{tikzcd}$$

Proof. Firstly, note that φ extends to a function $\varphi_1 : K_1F \to K_1L$ given by the rule

$$\varphi_1(\rho(a)) = \rho(\varphi(a)).$$

Certainly φ_1 is a morphism because

$$\varphi_1(0) = \varphi_1(\rho(1)) = \rho(\varphi(1)) = \rho(1) = 0,$$

and for all $\rho(a), \rho(b) \in K_1F$,

$$\varphi_1(\rho(a) + \rho(b)) = \varphi_1(\rho(ab)) = \rho(\varphi(ab)) = \rho(\varphi(a)\varphi(b)) = \rho(\varphi(a)) + \rho(\varphi(b)).$$

Proceeding inductively, for all $n \geq 1$ we extend φ to a function $\varphi_n : \prod_{i=1}^n K_1F \to K_nL$ given by the rule

$$\varphi(\rho(a_1), ..., \rho(a_n)) := \varphi_1(\rho(a_1))...\varphi_1(\rho(a_n)) = \rho(\varphi(a_1))...\rho(\varphi(a_n)).$$

Then if $i = 1, ..., n$ and $b_i \in k_1F$ we have

$$\begin{aligned}&\varphi_n(\rho(a_1), ..., \rho(a_i) + \rho(b_i), ..., \rho(a_n)) = \varphi_n(\rho(a_1), ..., \rho(a_ib_i), ..., \rho(a_n)) =\\ &\rho(\varphi(a_1))...\rho(\varphi(a_ib_i)...\rho(\varphi(a_n)) = \rho(\varphi(a_1))...\rho(\varphi(a_i)\varphi(b_i))...\rho(\varphi(a_n)) =\\ &\rho(\varphi(a_1)...[\rho(\varphi(a_i) + \varphi(b_i))]...\rho(\varphi(a_n)) =\\ &\rho(\varphi(a_1))...\rho(\varphi(a_i))...\rho(\varphi(a_n)) + \rho(\varphi(a_1))...\rho(\varphi(b_i))...\rho(\varphi(a_n)) =\\ &\varphi_n(\rho(a_1), ..., \rho(a_i), ..., \rho(a_n)) + \varphi_n(\rho(a_1), ..., \rho(b_i), ..., \rho(a_n)),\end{aligned}$$

then for each n, $\varphi_n : \prod_{i=1}^n K_1F \to K_nL$ is multilinear and by the universal property of tensor product there is an unique morphism

$$\tilde{\varphi}_n : \bigotimes_{j=1}^n K_1F \to K_nL$$

extending φ_n. By construction (and using the fact that φ is a morphism), $\text{Ker}(\tilde{\varphi}_n) = Q^n(K_1F)$, which provides an unique morphism $\overline{\varphi}_n : T^n(K_1F)/Q^n(K_1(F) \to K_nL$ such that $\tilde{\varphi}_n = \overline{\varphi}_n \circ \pi_n$, where π_n is the canonical projection $T^n(K_1F)$ in $Q^n(k_1F)$. Then taking $\varphi_0 = Id_{\mathbb{Z}}$, we get a morphism $\varphi_* : K_*F \to K_*L$, given by $\varphi_* = \{\overline{\varphi}_n : n \geq 0\}$.

For items (a) and (b), it is enough to note that these properties holds for $\tilde{\varphi}_n$, $n \geq 0$, and after the application of projection, we get the validity for $\overline{\varphi}_n = \pi_n \circ \tilde{\varphi}_n$.

Item (c) follows by the same argument of items (a) and (b), noting that $\varphi(1) = 1$ imply $\varphi(-1) = -1$. By abuse of notation, we denote

$$\varphi_* = \{\overline{\varphi}_n : n \geq 0\} = \{\varphi_n : n \geq 0\}.$$

□

We also have the reduced K-theory graded ring $k_*F = (k_0F, k_1F, ..., k_nF, ...)$ in the hyperfield context, which is defined by the rule $k_nF := K_nF/2K_nF$ for all $n \geq 0$. Of course for all $n \geq 0$ we have an epimorphism $q : K_nF \to k_nF$ simply denoted by $q(a) := [a]$, $a \in K_nF$. It is immediate that k_nF is additively generated by $\{[\rho(a_1)]..[\rho(a_n)] : a_1, ..., a_n \in \dot{F}\}$. We simply denote such a generator by $\tilde{\rho}(a_1)...\tilde{\rho}(a_n)$ or even $\rho(a_1)...\rho(a_n)$ whenever the context allows it.

We also have some basic properties of the reduced K-theory, which proof is just a translation of 2.1 of [30]:

2.1ktmulti

Lemma 4.3.4 (Adapted from 2.1 [30])**.** *Let F be a hyperbolic hyperfield, $x, y, a_1, ..., a_n \in \dot{F}$ and σ be a permutation on n elements.*

a - In k_2F, $\rho(a)^2 = \rho(a)\rho(-1)$. Hence in k_mF, $\rho(a)^m = \rho(a)\rho(-1)^{m-1}$, $m \geq 2$;

b - In k_2F, $\rho(a)\rho(-a) = \rho(a)^2 = 0$;

c - In k_nF, $\rho(a_1)\rho(a_2)...\rho(a_n) = \rho(a_{\sigma 1})\rho(a_{\sigma 2})...\rho(a_{\sigma n})$;

d - For $n \geq 1$ and $\xi \in k_nF$, $\xi^2 = \rho(-1)^n\xi$;

e - If F is a real reduced hyperfield, then $x \in 1 + y$ and $\rho(y)\rho(a_1)...\rho(a_n) = 0$ implies

$$\rho(x)\rho(a_1)\rho(a_2)...\rho(a_n) = 0.$$

Moreover the results in Proposition 4.3.3 continue to hold if we took $\varphi_* = \{\varphi_n : n \geq 0\} : k_*F \to k_*L$.

ktmarshall1

Proposition 4.3.5. *Let F be a hyperfield and $T \subseteq F$ be a multiplicative subset such that $F \subseteq T$. Then, for each $n \geq 1$*

$$K_n(F/_mT^*) \cong k_n(F/_mT^*).$$

Proof. Since $F^2 \subseteq T$, for all $a \in F/_mT^*$ we have

$$0 = \rho(a^2) = \rho(a) + \rho(a).$$

Then $2K(F/_mT^*) = 0$ and we get $K_n(F/_mT^*) \cong k_n(F/_mT^*), n \geq 1$. □

ktmarshall2

Theorem 4.3.6. *Let F be a hyperbolic hyperfield and $T \subseteq F$ be a multiplicative subset such that $F \subseteq T$. Then there is a surjective morphism*

$$k(F) \to k(F/_mT^*).$$

Moreover, for each $n \geq 1$,

$$k_n(F) \cong K_n(F/_m\dot{F}^2) \cong k_n(F/_m\dot{F}^2).$$

Before we prove it, we need a Lemma:

lemktmulti1

Lemma 4.3.7. *Let F be a hyperfield and $n \geq 1$. Then*

$$2K_n(F) = \left\{\sum_{j=1}^{p} \rho(a_{j1})...\rho(a_{jn}) : \textit{for all } j \textit{ there is an index } k \textit{ such that } a_{jk} = b_i^2,\, b_i \in \dot{F}\right\}.$$

Proof. Let $\eta \in 2K_nF$. Then

$$\eta = \left(\sum_{j=1}^{p} \rho(a_{j1})...\rho(a_{jn})\right) + \left(\sum_{j=1}^{p} \rho(a_{j1})...\rho(a_{jn})\right),\ d_{ij} \in \dot{F}.$$

By induction, we only need to consider the case $p = 1$, so

$$\rho(a_1)...\rho(a_n) + \rho(a_1)...\rho(a_n) = \rho(a_1^2)\rho(a_2)...\rho(a_n).$$

and we get $\subseteq$. The reverse inclusion follow by the same calculation. □

Proof of Theorem 4.3.6. Let $\pi : F \to F/_mT^*$ denote the canonical projection. By Proposition 4.3.3 there is a morphism $\pi_* : K(F) \to K(F/_mT^*)$. Since π is surjective, π_* is surjective.

Now, let $\pi : F \to F/_m\dot{F}^2$ and $q : K(F) \to k(F)$ the canonical projections. Denote elements in $F/_m\dot{F}^2$ by $[a] \in F/_m\dot{F}^2$, $a \in F$ and elements in $k_n(F)$ by $\tilde{\rho}(a_1)...\tilde{\rho}(a_n)$. For all $n \geq 1$ we have an induced morphism $\tilde{q}_n : K_n(F/_m\dot{F}^2) \to k_n(F)$ given by the rule

$$\tilde{q}_n(\rho([a_1])...\rho([a_n])) := \tilde{\rho}(a_1)...\tilde{\rho}(a_n).$$

This morphism $\tilde{\pi}_n$ makes the following diagram commute

$$\begin{tikzcd}
K_n(F) \arrow[r, "q"] \arrow[d, "\pi_n"'] & k_n(F) \\
K_n(F/_m\dot{F}^2) \arrow[ur, "\tilde{q}_n"'] &
\end{tikzcd}$$

and then, $\tilde{q}_n$ is surjective. Finally, if $\tilde{q}_n(\rho([a_1])...\rho([a_n])) = 0$, then $\tilde{\rho}(a_1)...\tilde{\rho}(a_n) = 0$, and hence $\rho(a_1)...\rho(a_n) \in 2K_n(F)$. By Lemma 4.3.7

$$\rho(a_1)...\rho(a_n) = \sum_{j=1}^{p} \rho(d_{j1})...\rho(d_{jn}),\ d_{ij} \in \dot{F}$$

and for all i there is an index k such that $a_{ik} = b_i^2$, $b_i \in \dot{F}$. Therefore

$$\begin{aligned}
\pi_n(\rho(a_1)...\rho(a_n)) &= \pi_n\left(\sum_{j=1}^{p} \rho(d_{j1})...\rho(d_{jn})\right) \\
&= \sum_{j=1}^{p} \pi_n(\rho(d_{j1})...\rho(d_{jn})) = \sum_{j=1}^{p} \rho([d_{j1}])...\rho([d_{jn}]) \\
&= \sum_{j=1}^{p} [d_{j1}])...\rho([1])...\rho([d_{jn})] = 0.
\end{aligned}$$

Then $\mathrm{Ker}(\tilde{q}_n) = [0]$, proving that $\tilde{q}_n$ is injective. Then $\tilde{q}_n$ is an isomorphism, and composing all the isomorphisms obtained here we get

$$k(F) \cong K(F/_m\dot{F}^2) \cong k(F/_m\dot{F}^2).$$

$\square$

The Theorem 4.3.8 below generalizes Proposition 5.10 of [59]: this constitutes a fundamental technical step to build profinite (Galois) groups associated to a pre-special hyperfield in [20].

Lets establish some notation: for $n \geq 0$ we denote

$$P(n) = \mathcal{P}(\{0, ..., n-1\}) \setminus \{\emptyset\}$$

and for $0 \leq i \leq n-1$, denote

$$P(n, i) = \{X \in P(n) : i \in X\}.$$

For a be a pre-special hyperfield F and $\{a_0, ..., a_{n-1}\} \subseteq F^*$ $\mathbb{F}_2$-linearly independent, if $S \in P(n)$ we denote

$$a_S := a_0^{\varepsilon_0}...a_{n-1}^{\varepsilon_{n-1}},$$

where $\varepsilon_0 \in \{0, 1\}$ for all $i = 0, .., n-1$ and $\varepsilon_i = 1$ if and only if $i \in S$.

Remember that by the very Definition of $k_n(F)$,

$$k_2(F) := [k_1(G) \otimes k_1(G)]/M,$$

where M is the subgroup of $k_1(G) \otimes k_1(G)$ generated by

$$\{\rho(a)\rho(b) : a \in D_G(1, -b)\}.$$

fixsg3-ktheory

Theorem 4.3.8. *Let F be a pre-special hyperfield and $\{a_0, ..., a_{n-1}\} \subseteq F^*$ $\mathbb{F}_2$-linearly independent. The following conditions are equivalent:*

i - There exists $\{b_0, ..., b_{n-1}\} \subseteq F^*$ such that

$$\sum_{k<n} \rho(a_k)\rho(b_k) = 0 \text{ in } k_2(F).$$

ii - There exist subsets $\{c_0, ..., c_{m-1}\}, \{d_0, ..., d_{n-1}\}$ of F^* with $m \geq n$ such that

(a) $\{c_0, ..., c_{m-1}\}$ is linearly independent and $c_i = a_i$ for all $i < n$;

(b) $d_i = b_i$ for all $i < n$ and $d_i = 1$ for $i = n, ..., m-1$.

(c) For all $x \in C := [c_0, ..., c_{m-1}]$, there is some $r_x \in (1-x) \setminus \{0\}$ such that for each $i < m$

$$d_i = \prod_{x \in C_i} r_x$$

where

$$C_i = \left\{ \prod_{k<m} c_k^{\varepsilon_k} : \varepsilon_k \in \{0, 1\} \text{ and } \varepsilon_i = 1 \right\}.$$

In other words, C_i is "counting" all products $c_0^{r_0}...c_i^1...c_{m-1}^{r_{m-1}}$. Since for all $x \in C := [c_0, ..., c_{m-1}]$ there exist $S \in P(m)$ such that

$$x = \prod_{i \in S} c_i := c_S.$$

Denoting r_x by r_S we can rewrite

$$d_i = \prod_{x \in C_i} r_x = \prod_{S \in P(m)} r_S.$$

Proof of Theorem 4.3.8. (i) $\Rightarrow$ (ii). Let

$$\sum_{k<n} \rho(a_k)\rho(b_k) = 0 \text{ in } k_2(F).$$

Then there exist $u_0, ..., u_{p-1}, v_0, ..., v_{p-1} \in F^*$ such that $v_i \in 1 + u_i$ for $i = 0, ..., p-1$ and

$$\sum_{k<n} \rho(a_k)\rho(b_k) = \sum_{k<n} \rho(a_k)\rho(b_k) \text{ in } k_1(F) \otimes k_1(F).$$

Enlarge the set $\{a_0, ..., a_{n-1}\}$ to a base $\{c_0, ..., c_{m-1}\}$ of $[\{a_0, ..., a_{n-1}, u_0, ..., u_{p-1}\}]$, with $c_i = a_i$ for all $i < n$. For all $x \in C := [c_0, ..., c_{m-1}]$ there exist $S \in P(m)$ such that

$$x = \prod_{i \in S} c_i := c_S.$$

Moreover, since $\{c_0, ..., c_{m-1}\}$ is a basis, for each $i = 0, ..., p-1$ there is only one $S_i \in P(m)$ such that $u_i = c_{S_i}$. For each $S \in P(m)$, set

$$r_S := \prod_{\substack{those\, j\, with \\ S_j = S}} v_j.$$

If no $S_j = S$, set $r_S = 1$. Note that if there is an index j with $S = S_j$, this index must be unique (because the expression $u_i = c_{S_i}$ is unique). Then by construction $r_S \in 1 + c_S \setminus \{0\}$ and in $k_2(F)$ we get

$$\begin{aligned}
\sum_{k<m} \rho(a_k)\rho(b_k) = \sum_{k<n} \rho(c_k)\rho(d_k) &= \sum_{k<p} \rho(u_k)\rho(v_k) \\
&= \sum_{S \in P(m)} \rho\left(\prod_{\substack{those\, j\, with \\ S_j = S}} c_j\right)\rho(v_j) \\
&= \sum_{S \in P(m)} \sum_{\substack{those\, j\, with \\ S_j = S}} \rho(c_j)\rho(v_j) \\
&= \sum_{S \in P(m)} \rho(c_S)\rho\left(\prod_{\substack{those\, j\, with \\ S_j = S}} v_S\right) \\
&= \sum_{S \in P(m)} \rho(c_S)\rho(r_S) = \sum_{S \in P(m)} \sum_{k \in S} \rho(c_k)\rho(r_S) \\
&= \sum_{k<m} \rho(c_k)\rho\left(\prod_{S \in P(n)} r_S\right).
\end{aligned}$$

Since $\{c_0, ..., c_{m-1}\}$ is a basis, it follows that $d_i = \prod_{S \in P(n)} r_S$ as desired.

(ii)$\Rightarrow$(i). Under the hypotheses of (ii) we get

$$\begin{aligned}
\sum_{k<n} \rho(a_k)\rho(b_k) = \sum_{k<m} \rho(c_k)\rho(d_k) &= \sum_{k<m} \rho(c_k)\rho\left(\prod_{S \in P(n)} r_S\right) \\
&= \sum_{k<m} \sum_{S \in P(m)} \rho(c_k)\rho(r_S) = \sum_{S \in P(m)} \sum_{k<m} \rho(c_i)\rho(r_S) \\
&= \sum_{S \in P(m)} \rho(c_S)\rho(r_S) = 0.
\end{aligned}$$

$\square$

4.4 Inductive Graded Rings: An Abstract Approach

After the three K-theories defined in the above sections, it is desirable (or, at least, suggestive) the rise of an abstract environment that encapsule all them, and of course, provide an axiomatic approach to guide new extensions of the concept of K-theory in the context of the algebraic and abstract theories of quadratic forms. The inductive graded rings fits this purpose. Here we will present three versions. The first one is:

igr1

Definition 4.4.1 (Inductive Graded Rings First Version (adapted from Definition 9.7 of [28]))**.** *An **inductive graded ring** (or **Igr** for short) is a structure $R = ((R_n)_{n\geq 0}, (h_n)_{n\geq 0}, *_{nm})$ where*

i - $R_0 \cong \mathbb{F}_2$.

ii - R_n *has a group structure* $(R_n, +, 0, \top_n)$ *of exponent 2 with a distinguished element* $\top_n$.

iii - $h_n : R_n \to R_{n+1}$ *is a group homomorphism such that* $h_n(\top_n) = \top_{n+1}$.

iv - For all $n \geq 1$, $h_n = *_{1n}(\top_1, \_)$.

v - The binary operations $*_{nm} : R_n \times R_m \to R_{n+m}$, $n, m \in \mathbb{N}$ *induces a commutative ring structure on the abelian group*

$$R = \bigoplus_{n\geq 0} R_n$$

with $1 = \top_0$.

vi - For $0 \leq s \leq t$ *define*

$$h_s^t = \begin{cases} Id_{R_s} \text{ if } s = t \\ h_{t-1} \circ ... \circ h_{s+1} \circ h_s \text{ if } s < t. \end{cases}$$

Then if $p \geq n$ *and* $q \geq m$, *for all* $x \in R_n$ *and* $y \in R_m$,

$$h_n^p(x) * h_m^q(y) = h_{n+m}^{p+q}(x * y).$$

*A **morphism** between Igr's* R *and* S *is a pair* $f = (f, (f_n)_{n\geq 0})$ *where* $f_n : R_n \to S_n$ *is a morphism of pointed groups and*

$$f = \bigoplus_{n\geq 0} f_n : R \to S$$

is a morphism of commutative rings with unity. The category of inductive graded rings (in first version) and their morphisms will be denoted by Igr.

A first consequence of these definitions is that: if

$$f : ((R_n)_{n\geq 0}, (h_n)_{n\geq 0}, *_{nm}) \to ((S_n)_{n\geq 0}, (l_n)_{n\geq 0}, *_{nm})$$

is a morphism of Igr's then $f_{n+1} \circ h_n = l_n \circ f_n$.

$$\begin{tikzcd}
R_0 \arrow[r, "h_0"] \arrow[d, "f_0"'] & R_1 \arrow[r, "h_1"] \arrow[d, "f_1"'] & R_2 \arrow[r, "h_2"] \arrow[d, "f_2"'] & ... \arrow[r, "h_{n-1}"] & R_n \arrow[r, "h_n"] \arrow[d, "f_n"'] & R_{n+1} \arrow[r, "h_{n+1}"] \arrow[d, "f_{n+1}"'] & ... \\
S_0 \arrow[r, "l_0"] & S_1 \arrow[r, "l_1"] & S_2 \arrow[r, "l_2"] & ... \arrow[r, "l_{n-1}"] & S_n \arrow[r, "l_n"] & S_{n+1} \arrow[r, "l_{n+1}"] & ...
\end{tikzcd}$$

In fact, since $R_0 \cong \mathbb{F}_2 \cong S_0$ and $f(1) = 1$, then $f_0 : R_0 \to S_0$ is the unique abelian group isomorphism and $f_1 \circ h_0 = l_0 \circ f_0$. If $n \geq 1$, for all $a_n \in R_n$ holds

$$\begin{aligned} f_{n+1} \circ h_n(a_n) &= f_{n+1} \circ (*_{1n}(\top_1, a_n)) = f_1(\top_1) *_{1n} f_n(a_n) \\ &= \top_1 *_{1n} f_n(a_n) = l_n(f_n(a_n)) = l_n \circ f_n(a_n). \end{aligned}$$

ex1

Example 4.4.2.

a - *Let F be a field of characteristic not 2. The main actors here are WF, the Witt ring of F and IF, the fundamental ideal of WF. Is well know that I^nF, the n-th power of IF is additively generated by n-fold Pfister forms over F. Now, let $R_0 = WF/IF \cong \mathbb{F}_2$ and $R_n = I^nF/I^{n+1}F$. Finally, let $h_n = \_ \otimes \langle 1, 1\rangle$, $n \geq 1$. With these prescriptions we have an inductive graded ring R associated to F: $W_*(F)$, the graded Witt ring of the field F.*

b - *The previous example still works if we change the Witt ring of a field F for the Witt ring of a (formally real) special group G.*

c - *An inductive graded ring can be seen as a graded F_2-algebra R with $R_0 = F_2$ and a distinguished element T_1 in R_1.*

There is an alternative definition for Igr with a first-order theoretic flavor. It is a technical framework that allows achieving some model-theoretic results.

Before define it, we need some preparation. First of all, we set up the language. Here, we will work with the poli-sorted framework (as established in chapter 5 of [1]), which means the following:

Let S be a set (of sorts). For each $s \in S$ assume a countable set Var_s of **variables of sort** s (with the convention if $s \neq t$ then $\mathrm{Var}_s \cap \mathrm{Var}_t = \emptyset$). For each sort $s \in S$ an equality symbol $=_s$ (or just $=$); the connectives $\neg, \wedge, \vee, \to$ (not, and, or, implies); the quantifiers $\forall, \exists$ (for all, there exists).

A **finitary S-sorted language (or signature)** is a set $\mathcal{L} = (\mathcal{C}, \mathcal{F}, \mathcal{R})$ where:

i - $\mathcal{C}$ is the set of constant symbols. For each $c \in \mathcal{C}$ we assign an element $s \in S$, the sort of c;

ii - $\mathcal{F}$ is the set of functional symbols. For each $f \in \mathcal{F}$ we assign elements $s, s_1, ..., s_n \in S$, we say that f has arity $s_1 \times ... \times s_n$ and s is the value sort of f; and we use the notation $f : s_1 \times ... \times s_n \to s$.

iii - $\mathcal{R}$ is the set of relation symbols. $c \in \mathcal{C}$ we assign elements $s_1, ..., s_n \in S$, the arity of R; and we say that R has arity $s_1 \times ... \times s_n$.

A **$\mathcal{L}$-structure** $\mathcal{M}$ is, in this sense, prescribed by the following data:

i- The **domain or universe** of $\mathcal{M}$, which is an S-sorted set $|\mathcal{M}| := (M_s)_{s\in S}$.

ii- For each constant symbol $c \in \mathcal{C}$ of arity s, an element $c^{\mathcal{M}} \in M_s$.

iii- For each functional symbol $f \in \mathcal{F}$, $f : s_1 \times ... \times s_n \to s$, a function $f^{\mathcal{M}} : M_{s_1} \times ... \times M_{s_n} \to M_s$.

iv- For each relation symbol $R \in \mathcal{R}$ of arity $s_1 \times ... \times s_n$ a relation, i.e. a subset $R^{\mathcal{M}} \subseteq M_{s_1} \times ... \times M_{s_n}$.

A **$\mathcal{L}$-morphism** $\varphi : \mathcal{M} \to \mathcal{N}$ is a sequence of functions $\varphi = (\varphi_s)_s : |\mathcal{M}| \to |\mathcal{N}|$ such that

i - for all $c \in \mathcal{C}$ of arity s, $\varphi_s(c^{\mathcal{M}}) = c^{\mathcal{N}}$;

ii - for all $f : s_1 \times ... \times s_n \to s$, if $(a_1, ..., a_n) \in: M_{s_1} \times ... \times M_{s_n}$, then $\varphi_s(f^{\mathcal{M}}(a_1, ..., a_n)) = f^{\mathcal{N}}(\varphi_{s_1}(a_1), ..., \varphi_{s_n}(a_n))$;

iii - for all R of arity $s_1 \times ... \times s_n$, if $(a_1, ..., a_n) \in R^{\mathcal{M}}$ then $(\varphi(a_1), ..., \varphi(a_n)) \in R^{\mathcal{N}}$.

The category of $\mathcal{L}$-structures and $\mathcal{L}$-morphism in the poli-sorted language $\mathcal{L}$ will be denoted by $\mathrm{Str}_s(\mathcal{L})$.

The terms, formulas, occurrence and free variables definitions for the poli-sorted case are similar to the usual (single-sorted) first order ones. For example, the terms are defined as follows:

i - variables $x \in \mathrm{Var}_s$ and constants $c \in C_s$ are terms of value sort s;

ii - if $\vec{s} = \langle s_1, ..., s_n, s \rangle \in S^{n+1}$, $f \in \mathcal{F}$ with $f : s_1 \times ... \times s_n \to s$, and $\tau_1, ..., \tau_n$ are terms of value sorts $s_1, ..., s_n$ respectively, then $f(\tau_1, ..., \tau_n)$ is a term of sort s.

As usual, we may write $\tau : s$ to indicate that the term τ has value sort s.

For the formulas:

i - if $x, y \in \mathrm{Var}_s$ then $x = y$ is a formula; if $\vec{s} = \langle s_1, ..., s_n \rangle \in S^n$, $R \in \mathcal{R}$ of arity $s_1 \times ... \times s_n$ and $\tau_1, ..., \tau_n$ are terms of sort $s_1, ..., s_n$ respectively, then $R(\tau_1, ..., \tau_n)$ is a formula. These are the **atomic formulas**.

ii - If φ_1, φ_2 are formulas, then $\neg\varphi_1$, $\varphi_1 \wedge \varphi_2$, $\varphi_1 \vee \varphi_2$ and $\varphi_1 \to \varphi_2$ are formulas.

iii - If φ is a formula and $x \in \mathrm{Var}_s$ $(s \in S)$, then $\forall x\varphi$ and $\exists x\varphi$ are formulas.

In our particular case, the set of sorts will be just $\mathbb{N}$. Then, for each $n, m \geq 0$, we set the following data:

i - $0_n, \top_n$ are constant symbols of arity n. We use $0_0 = 0$ and $\top_0 = 1$.

ii - $+_n : n \times n \to n$ is a binary operation symbol.

iii - $h_n : n \to (n+1)$ and $*_{n,m} : n \times m \to (n+m)$ are functional symbols.

The **(first order) language of inductive graded rings** $\mathcal{L}_{igr}$ is just the following language (in the poli-sorted sense):

$$\mathcal{L}_{igr} := \{0_n, \top_n, +_n, h_n, *_{nm} : n, m \geq 0\}.$$

The **(first order) theory of inductive graded rings** $T(\mathcal{L}_{igr})$ is the $\mathcal{L}_{igr}$-theory axiomatized by the following $\mathcal{L}_{igr}$-sentences, where we use $\cdot_n : 0 \times n \to n$ as an abbreviation for $*_{0n}$:

i - For $n \geq 0$, sentences saying that "$+_n, 0_n, \top_n$ induces a pointed left $\mathbb{F}_2$-module":

$$\begin{aligned}
&\forall\, x : n \forall\, y : n \forall\, z : n((x +_n y) +_n z = x +_n (y +_n z)) \\
&\forall\, x : n(x +_n 0_n = x) \\
&\forall\, x : n \forall\, y : n(x +_n y = y +_n x) \\
&\forall\, x : n(x +_n x = 0_n) \\
&\forall\, x : n(1 \cdot_n x = x) \\
&\forall\, x : n \forall\, y : n \forall\, a : 0(a \cdot_n (x +_n y) = a \cdot_n x +_n a \cdot_n y) \\
&\forall\, x : n \forall\, a : 0 \forall\, b : 0((a +_0 b) \cdot_n x = a \cdot_n x +_n b \cdot_n x)
\end{aligned}$$

ii - For $n \geq 0$, sentences saying that "h_n is a pointed $\mathbb{F}_2$-morphism":

$$\begin{aligned}&\forall\, x : n \forall\, y : n(h_n(x +_n y) = h_n(x) +_{n+1} h_n(y))\\&\forall\, x : n \forall\, a : 0(h_n(a \cdot_n x) = a \cdot_n h_n(x))\\&h_n(\top_n) = \top_{n+1}\end{aligned}$$

iii - Sentences saying that "$R_0 \cong \mathbb{F}_2$":

$$\begin{aligned}&0_0 \neq \top_0\\&\forall\, x : n(x = 0_0 \vee x = \top_0)\end{aligned}$$

iv - Using the abbreviation $*_{n,m}(x, y) = x *_{n,m} y$, we write for $n, m \geq 0$ sentences saying that "$*_{n,m}$ is a biadditive function compatible with h_n":

$$\begin{aligned}&\forall\, x : n \forall\, y : n \forall\, z : m(((x +_n y) *_{nm} z) = (x *_{mn} z +_{n+m} y *_{nm} z))\\&\forall\, x : n \forall\, y : m \forall\, z : m((x *_{mn} (y +_m z)) = (x *_{nm} y +_{n+m} x *_{nm} z))\\&\forall\, x : n \forall\, y : m(h_{n+m}(x *_{nm} y) = h_n(x) *_{nm} h_m(y))\end{aligned}$$

v - Sentences describing "the induced ring with product induced by $*_{n,m}$, $n, m \geq 0$":

$$\begin{aligned}&\forall\, x : n \forall\, y : m \forall\, z : p((x *_{n,m} y) *_{(m+n),p} z = x *_{n,(m+p)} (y *_{m,p} z))\\&\forall\, x : n \forall\, y : m(x *_{n,m} y = y *_{m,n} x)\end{aligned}$$

vi - For $n \geq 1$, sentences saying that "$h_n = \top_1 *_{1n} \_$":

$$\forall\, x : n(h_n(x) = \top_1 *_{1n} x)$$

Now we are in a position to define another version of Igr:

igr3

Definition 4.4.3 (Inductive Graded Rings Second Version)**.** *An **inductive graded ring** (or **(Igr)** for short) is a model for $T(\mathcal{L}_{igr})$, or in other words, a $\mathcal{L}_{igr}$-structure $\mathcal{R}$ such that $\mathcal{R} \models_{\mathcal{L}_{igr}} T(\mathcal{L}_{igr})$. We denote by Igr$_2$ the category of $\mathcal{L}_{igr}$-structures and $\mathcal{L}_{igr}$-morphisms.*

Again, after some straightforward calculations we can check:

Theorem 4.4.4. *The categories Igr, Igr$_2$ are equivalent.*

igr-re

Remark 4.4.5. *Following a well-known procedure, it is possible to correspond theories on poly-sorted first-order languages with theories on traditional (single-sorted) first-order languages in such a way that the corresponding categories of models are equivalent. This allows a useful interchanging between model-theoretic results, in both directions. In particular, in the following, we will freely interchange the three notions of Igr indicated in this section.*

4.5 Interchanging K-theories

We finalize this chapter with an use of Igr's to interchanging the three K-theory notions presented before in a functorial fashion. Lets first, look more carefully at theorem 4.5.1. We make the following distinctions between K-theories:

$$\begin{aligned} K &\text{ will denote the Milnor's K-Theory,} \\ K^{dm} &\text{ will denote the Dickmann-Miraglia's K-Theory,} \\ K^{mult} &\text{ will denote the K-Theory of Hyperfields.} \end{aligned}$$

Of course, we need the following theorem:

km1

Theorem 4.5.1.

a - *Let F be a field. Then $k_*^{mil}F$ (the reduced Milnor K-theory) is an inductive graded ring.*

b - *Let G be a special group. Then $k_*^{dm}G$ (the Dickmann-Miraglia K-theory of G) is an inductive graded ring.*

c - *Let F be a hyperfield. Then $k_*^{mult}F$ (our reduced K-theory) is an inductive graded ring.*

Proof. Item (a) is the content of Lemma 9.11 in [28], and item (b) is the content of Lemma 9.12 in [28]. We prove item (c) and items (a) and (b) will proceed by the same argument.

Let $k_*^{mult}F = (k_0F, k_1F, ..., k_nF, ...)$ be the reduced K-theory of a hyperfield F. Let $\top_0 = 1$ and for each $n \geq 1$, we set $\top_n = l(-1)^n$ as the distinguished element of $m-n$. For each $n \geq 0$, let $\theta_n : \prod_{j=1}^{n} K_1^{mult}F \to \otimes_{j=1}^{n+1} K_{n+1}^{mult}F$ given by the rule

$$\theta_n(\rho(a_1), ..., \rho(a_n)) := \rho(-1)\rho(a_1)...\rho(a_n).$$

We have for each $i \in \{1, ..., n\}$ and each $a_1, ..., a_n, b_i \in F^*$ that

$$\begin{aligned} &\theta_n(\rho(a_1), ...\rho(a_i) + \rho(b_i), ..., \rho(a_n)) = \theta_n(\rho(a_1), ...\rho(a_ib_i), ..., \rho(a_n)) := \\ &\rho(-1)\rho(a_1)...\rho(a_ib_i)...\rho(a_n) = \rho(-1)\rho(a_1)...[\rho(a_i) + \rho(b_i)]...\rho(a_n) = \\ &\rho(-1)\rho(a_1)...\rho(a_i)...\rho(a_n) + \rho(-1)\rho(a_1)...\rho(b_i)...\rho(a_n) = \\ &\theta_n(\rho(a_1), ..., \rho(a_i), ..., \rho(a_n)) + \theta_n(\rho(a_1)...\rho(b_i)...\rho(a_n)), \end{aligned}$$

then θ_n is multilinear. By the universal property of tensor product, we have a group homomorphism $\tilde{\theta}_n : K_n^{mult}F \to K_{n+1}^{mult}F$ given by the rule[2]

$$\tilde{\theta}_n(\rho(a_1)...\rho(a_n)) = \rho(-1)\rho(a_1)...\rho(a_n).$$

In order to make distinctions between reduced and non-reduced K-theories, we punctually denote an element in $k_n^{mult}F := K_n^{mult}F/2K_n^{mult}F$ by $\tilde{\rho}(a_1)...\tilde{\rho}(a_n)$. Lets also denote the canonical projection by $\pi_n : K_n^{mult}F \to k_n^{mult}F$. We define $\omega_n : k_n^{mult}F \to k_{n+1}^{mult}F$ by the following rule (on generators): for $a_1, ..., a_n \in \dot{F}$,

$$\omega_n(\tilde{\rho}(a_1)...\tilde{\rho}(a_n)) = \tilde{\rho}(-1)\tilde{\rho}(a_1)...\tilde{\rho}(a_n).$$

In fact, if $\rho(a_1)...\rho(b_n) - \rho(b_1)...\rho(b_n) \in 2K_n^{mult}F$ then

$$\rho(-1)\rho(a_1)...\rho(b_n) - \rho(-1)\rho(b_1)...\rho(b_n) = \rho(-1)[\rho(a_1)...\rho(b_n) - \rho(b_1)...\rho(b_n)] \in 2K_{n+1}^{mult}F,$$

[2] Remember that we are using the simplified notation for elements in $K_n^{mult}F$ (and all other K-theories), which is $\rho(a_1)...\rho(a_n) := \rho(a_1) \otimes ... \otimes \rho(a_n)$.

which proves that ω_n is in fact a group homomorphism making the following diagram commute

$$\begin{tikzcd} K_n^{mult}F \arrow[r, "\tilde{\theta}_n"] \arrow[d, "\pi_n"'] & K_{n+1}^{mult}F \arrow[d, "\pi_{n+1}"] \\ k_n^{mult}F \arrow[r, "\omega_n"'] & k_{n+1}^{mult}F \end{tikzcd}$$

With these rules, we already have the properties (i)-(iv) of Definition 4.4.1 holding in k_*F, remaining only property (v). Note that $\omega_s^t = \tilde{\rho}(-1)^{t-s}$ for $0 \leq s < t$.

Now let $m, n, p, q \in \mathbb{N}$, $p \geq n$, $q \geq m$ and consider $x \in k_n^{mult}F$ and $y \in k_m^{mult}F$. Note that $\omega_n^p(x) = \tilde{\rho}(-1)^{p-n} \cdot x$ and $\omega_m^q(y) = \tilde{\rho}(-1)^{q-m} \cdot y$. Then

$$\omega_n^p(x) \cdot \omega_m^q(y) = (\tilde{\rho}(-1)^{p-n} \cdot x)(\tilde{\rho}(-1)^{q-m} \cdot y) = \tilde{\rho}(-1)^{p-n+q-m} \cdot (x \cdot y) = \omega_{n-m}^{p+q}(x),$$

completing the proof. □

Using this Theorem (in addition with the argument of Lemma 3.3 in [30]) we obtain the following.

km2

Corollary 4.5.2. *We have a functor and $k : Field_2 \to Igr$ induced by K-theory and Milnor's reduced K-theory.*

km3

Corollary 4.5.3. *We have a functor $k^{mult} : MField_2 \to Igr$ induced by our reduced K-theory.*

km4

Theorem 4.5.4 (Theorem 2.5 in [29]). *Let F be a field. The functor $G : Field_2 \to SG$ provides a functor $k_*^{dm} : Field_2 \to Igr$ (the special group K-theory functor) given on the objects by $k_*^{dm}(F) : k_*^{dm}(G(F))$ and on the morphisms $f : F \to K$ by $k_*^{dm}(f) := G(f)_*$ (in the sense of Lemma 3.3 of [30]). Moreover, this functor commutes with the functors G and k, i.e, for all $F \in Field$, $k_*^{dm}(G(F)) \cong k_*(F)$.*

km5

Theorem 4.5.5. *Let G be a special group. The equivalence of categories $M : SG \to SMF$ induces a functor $k_*^{mult} : SG \to Igr$ given on the objects by $k_*^{mult}(G) := k_*^{mult}(M(G))$ and on the morphisms $f : G \to H$ by $k_*^{mult}(f) := k_*^{mult}(M(f))$. Moreover, this functor commutes with M and k^{dm}, i.e, for all $G \in SG$, $k_*^{mult}(M(G)) \cong k_*^{dm}(G)$.*

Proof. The only part requiring proof is that for all $G \in SG$, $k_*^{mult}(M(G)) \cong k_*^{dm}(G)$. The very first observation is that: since G is an exponent 2 group, the reduced and non-reduced K^{mult}-theory of $M(G)$ coincide.

Following the argument of Theorem 2.5 in [29], it is enough to show the following two statements:

i - For all $a, b \in G$, if $b \in 1 - a$ in $M(G)$ then $\lambda(b)\lambda(a) = 0$;

ii - For all $a, b \in G$, if $b \in D_G(1, a)$ then $\rho(b)\rho(a) = 0$.

For (i), if $b \in 1 - a$ in $M(G)$ then $b \in D_G(1, -a)$ and then, $\lambda(b)\lambda(-a) = 0$. Hence

$$\lambda(b)^2 = \lambda(b)\lambda(-a) = \lambda(b)\lambda(a) + \lambda(b)\lambda(-1).$$

Since $\lambda(b)\lambda(-1) = \lambda(b)^2$, we get $\lambda(b)\lambda(a) = 0$.

For (ii) we just use the same argument: if $b \in D_G(1,a)$ then $b \in 1+a$ in $M(G)$ and then, $\rho(b)\rho(-a) = 0$. Hence

$$\rho(b)^2 = \rho(b)\rho(-a) = \rho(b)\rho(a) + \rho(b)\rho(-1).$$

Since $\rho(b)\rho(-1) = \rho(b)^2$, we get $\rho(b)\rho(a) = 0$. □

Combining Theorems 4.5.1, 4.5.4, 4.5.5, 4.3.6 and Corollaries 4.5.2 and 4.5.3 we obtain the following Theorem, that unify in some sense all three K-theories:

res0

Theorem 4.5.6 (Interchanging K-theories Formulas)**.** *Let $F \in Field_2$. Then*

$$k^{mil}(F) \cong k^{dm}(G(F)) \cong k^{mult}(M(G(F))).$$

If F is formally real and T is a preordering of F, then

$$k^{dm}(G_T(F)) \cong k^{mult}(M(G_T(F))).$$

Moreover, since $M(G(F)) \cong F/_m\dot{F}^2$ and $M(G_T(F)) \cong F/_mT^*$, we get

$$k^{mil}(F) \cong k^{dm}(G(F)) \cong k^{mult}(F/_m\dot{F}^2) \text{ and}$$
$$k^{dm}(G_T(F)) \cong k^{mult}(F/_mT^*).$$

res1

Corollary 4.5.7. *Let F be a field. Then*

$$k^{mil}(F) \cong k^{mult}(F/_m\dot{F}^2).$$

Proof. Using the previous Corollary, we already have

$$k^{mil}(F) \cong k^{dm}(G(F)) \cong k^{mult}(M(G(F))).$$

Now, is enough to observe that $M(G(F)) \cong F/_m\dot{F}^2$. □

Combining Theorem 4.5.6, Corollary 4.5.7 and Theorem 4.3.6 we get the following Corollaries.

res2

Corollary 4.5.8. *Let F be a formally real field and T be a preordering. Then we have a surjective map*

$$k^{mil}(F) \to k^{mult}(F/_mT^*).$$

res3

Corollary 4.5.9. *Let G be a pre-special group and $H \subseteq G$ be a subgroup of G. Let $M(G)$ be the pre-special multifield associated to G and $M(H) = H \cup \{0\} \subseteq M(G)$. Then*

$$G/H \cong M(G)/_mM(H)^*.$$

Moreover, $M(H) \subseteq M(G)$ is a preordering if and only if H is saturated.

res4

Corollary 4.5.10. *Let G be a special group and H be a saturated subgroup. Then we have a surjective map*

$$k^{dm}(G) \to k^{mult}(G/_mH) \cong k^{dm}(G/H).$$

Chapter 5

Inductive Graded Rings: A Deeper Look at Marshall's Signature Conjecture

Theorem 4.5.6 gives a hint that the category of Igr is a good abstract environment for studying questions of "quadratic flavour". So a better understanding of Igr's is at least desirable and this is the main purpose of this Chapter.

We develop the general properties valid for Igr's and the main results here are Theorem 5.5.4, providing an adjunction between the categories of pre-special groups and (a subcategory of) inductive graded rings. We also characterize the Special and Weak Marshall Conjecture in the context of inductive graded rings (Section 5.6).

5.1 Some Categorical Facts

In order to easy the presentation, in this section there are some categorical results concerning adjunctions. Mostly are based on [8], but the reader could also consult [44].

3.1.1borceux

Definition 5.1.1 (3.1.1 of [8]). *Let $F : \mathcal{A} \to \mathcal{B}$ be a functor and B an object of $\mathcal{B}$. A **reflection** of B along F is a pair (R_B, η_B) where*

1. *R_B is an object of A and $\eta_B : B \to F(R_B)$ is a morphism of $\mathcal{B}$.*
2. *If $A \in \mathcal{A}$ is another object and $b : B \to F(A)$ is a morphism of $\mathcal{B}$, there exists a unique morphism $a : R_B \to A$ in $\mathcal{A}$ such that $F(a) \circ \eta_B = b$.*

3.1.2borceux

Proposition 5.1.2 (3.1.2 of [8]). *Let $F : \mathcal{A} \to \mathcal{B}$ be a functor and B an object of $\mathcal{B}$. When the reflection of B along F exists, it is unique up to isomorphism.*

3.1.4borceux

Definition 5.1.3 (3.1.4 of [8]). *A functor $R : \mathcal{B} \to A$ is **left adjoint** to the functor $F : \mathcal{A} \to \mathcal{B}$ when there exists a natural transformation*

$$\eta : 1_{\mathcal{B}} \Rightarrow F \circ R$$

such that for every $B \in \mathcal{B}$, $(R(B), \eta_B)$ is a reflection of B along F.

3.1.5borceux

Theorem 5.1.4 (3.1.5 of [8]). *Consider two functors $F : \mathcal{A} \to \mathcal{B}$ and $G : \mathcal{B} \to \mathcal{A}$. The following conditions are equivalent.*

1. *G is left adjoint of F.*

2. *There exist a natural transformation $\eta : 1_{\mathcal{B}} \Rightarrow F \circ G$ and $\varepsilon : G \to F \Rightarrow 1_{\mathcal{A}}$ such that*

$$(F * \varepsilon) \circ (\eta * F) = 1_F,\ (\varepsilon * G) \circ (G * \eta) = 1_G.$$

3. *There exist bijections*
$$\theta_{AB} : \mathcal{A}(G(B), A) \cong \mathcal{B}(B, F(A))$$
for every objects A and B, and those bijections are natural both in A and B.

4. *F is right adjoint of G.*

3.2.2borceux

Proposition 5.1.5 (3.2.2 of [8])**.** *If the functor $F : \mathcal{A} \to \mathcal{B}$ has a left adjoint then F preserves all limits which turn out to exist in $\mathcal{A}$.*

3.4.1borceux

Proposition 5.1.6 (3.4.1 of [8])**.** *Consider two functors $F : \mathcal{A} \to \mathcal{B}$, $G : \mathcal{B} \to \mathcal{A}$ with G left adjoint to F with $\eta : 1_{\mathcal{B}} \Rightarrow F \circ G$ and $\varepsilon : G \circ F \Rightarrow 1_{\mathcal{A}}$ the two corresponding natural transformations. The following conditions are equivalent.*

1. *F is full and faithfull.*

2. *ε is an isomorphism.*

Under these conditions, $\eta * F$ and $G * \eta$ are isomorphisms as well.

3.4.3borceux

Proposition 5.1.7 (3.4.3 of [8])**.** *Given a functor $F : \mathcal{A} \to \mathcal{B}$, the following conditions are equivalent:*

1. *F is full and faithfull and has a full and faithfull left adjoint G.*

2. *F has a left adjoint G and the two canonical natural transformations of the adjunction $\eta : 1_{\mathcal{B}} \Rightarrow F \circ G$ and $\varepsilon : G \to F \Rightarrow 1_{\mathcal{A}}$ are isomorphisms.*

3. *There exists a functor $G : \mathcal{B} \to \mathcal{A}$ and two arbitrary natural isomorphisms $1_{\mathcal{B}} \cong F \circ G$, $G \circ F \cong 1_{\mathcal{A}}$.*

4. *F is full and faithfull and each object $B \in \mathcal{B}$ is isomorphic to an object of the form $F(A)$, for some $A \in \mathcal{A}$.*

5. *The dual condition of (1).*

6. *The dual condition of (2).*

3.4.4borceux

Definition 5.1.8 (3.4.4 of [8])**.** *The categories $\mathcal{A}, \mathcal{B}$ are **equivalent** if there exist a functor $F : \mathcal{A} \to \mathcal{B}$ satisfying the conditions of Proposition 5.1.7.*

5.2 The First Properties of Igr

In this section we discuss the theory of Igr's. Constructions like products, limits, colimits, ideals, quotients, kernel and image are not new and are obtained in a very straightforward manner (basically, putting those structures available for rings in a "coordinatewise" fashion), then in order to gain speed, we will present these facts leaving more detailed proofs to the reader.

Denote: $p\mathbb{F}_2 - mod$ the category of pointed $\mathbb{F}_2$-modules, Ring the category of commutative rings with unity and morphism that preserves these units and Ring_2 the full subcategory of the associative $\mathbb{F}_2$-algebras. We have a functorial correspondence $\mathrm{Ring}_2 \to \mathrm{Igr}$, given by the following diagram:

$$\begin{tikzcd} A \arrow[d, "f"'] & \mapsto & \mathbb{F}_2 \arrow[r, "!"] \arrow[d, "id"'] & A \arrow[r, "id"] \arrow[d, "f"'] & A \arrow[r, "id"] \arrow[d, "f"'] & \dots \arrow[r, "id"] & A \arrow[r, "id"] \arrow[d, "f"'] & \dots \\ B & & \mathbb{F}_2 \arrow[r, "!"] & B \arrow[r, "id"] & B \arrow[r, "id"] & \dots \arrow[r, "id"] & B \arrow[r, "id"] & \dots \end{tikzcd}$$

Here A is a $p\mathbb{F}_2 - mod$ where $\top_n = 1, n \geq 1$ and $\top_0 = 1 \in \mathbb{F}_2$.

trivialigr

Definition 5.2.1. *The **trivial graded ring functor** $\mathbb{T} : Ring_2 \to Igr$ is the functor defined for $f : A \to B$ by $T(A)_0 := \mathbb{F}_2$, $T(f)_0 := id_{\mathbb{F}_2}$ and for all $n \geq 1$ we set $T(A)_n = A$ and $T(f)_n := f$.*

f2alg

Definition 5.2.2. *We define the **associated $\mathbb{F}_2$-algebra functor** $\mathbb{A} : Igr \to Ring_2$ is the functor defined for $f : R \to S$ by*

$$\mathbb{A}(R) := R_{\mathbb{A}} = \varinjlim_{n \geq 0} R_n \text{ and } \mathbb{A}(f) = f_{\mathbb{A}} := \varinjlim_{n \geq 0} f_n.$$

More explicitly, $\mathbb{A}(R) = (R_{\mathbb{A}}, 0, 1, +_{\mathbb{A}}, \cdot)$, where

i - $R_{\mathbb{A}} = \varinjlim_{n \geq 0} R_n$,

ii - $0 = [(0, 0)]$ and $1 = [(1, 0)]$,

iii - given $[(a_n, n)], [(b_m, m)] \in R_{\mathbb{A}}$ and setting $d \geq m, n$ we have

$$[(a_n, n)] + [(b_m, m)] = [(h_{nd}(a_n) + h_{md}(b_m), d)]$$

iv - given $[(a_n, n)], [(b_m, m)] \in R_{\mathbb{A}}$, we have

$$[(a_n, n)] \cdot [(b_m, m)] = [(a_n *_{nm} b_m, n + m)].$$

propadj1

Proposition 5.2.3.

i - The functor $\mathbb{A}$ is the left adjunct to $\mathbb{T}$.

ii - The functor $\mathbb{T}$ is full and faithful.

iii - The composite functor $\mathbb{A} \circ \mathbb{T}$ is naturally isomorphic to the functor 1_{Ring_2}.

Proof. Let $R \in Igr$. We have

$$\mathbb{T}(\mathbb{A}(R)) = \mathbb{T}\left(\varinjlim_{m \geq 0} R_m\right).$$

In other words, for all $n \geq 1$

$$\mathbb{T}\left(\varinjlim_{m \geq 0} R_m\right)_n := \varinjlim_{m \geq 0} R_m.$$

Then, for all $n \geq 1$ we have a canonical embedding

$$\eta(R)_n : R_n \to \varinjlim_{m\geq 0} R_m = \mathbb{T}\left(\varinjlim_{m\geq 0} R_m\right)_n ,$$

providing a morphism

$$\eta(R) : R \to \varinjlim_{m\geq 0} R_m = \mathbb{T}\left(\varinjlim_{m\geq 0} R_m\right).$$

For $f \in \mathrm{Igr}(R, S)$, taking $n \geq 1$ we have a commutative diagram

$$\begin{tikzcd} R_n \arrow[r, "f_n"] \arrow[d, "\eta(R)_n"'] & S_n \arrow[d, "\eta(S)_n"] \\ \varinjlim_{m\geq 0} R_m \arrow[r, "\varinjlim_{m\geq 0} f_m"'] & \varinjlim_{m\geq 0} S_m \end{tikzcd}$$

with the convention that $\eta(R)_0 = id_{\mathbb{F}_2}$. Then it is legitimate the definition of a natural transformation $\eta : 1_{\mathrm{Igr}} \to \mathbb{T} \circ \mathbb{A}$ given by the rule $R \mapsto \eta(R)$.

Now let $A \in Ring_2$ and $g \in Ring_2(R, \mathbb{T}(A))$. Then for each $n \geq 0$, there is a morphism $g_n : R_n \to \mathbb{T}(A)_n = A$ and by the universal property of inductive limit we get a morphism

$$\varinjlim_{m\geq 0} g_n : \varinjlim_{m\geq 0} R_m \to A.$$

In fact, $\varinjlim_{m\geq 0} g_n = \mathbb{A}(g)$.

Now, using the fact that $\eta(R)_n$ is the morphism induced by the inductive limit we have for all $n \geq 0$ the following commutative diagram

$$\begin{tikzcd} R_n \arrow[r, "\eta(B)_n"] \arrow[dr, "g_n"'] & \varinjlim_{m\geq 0} R_m \arrow[d, "\varinjlim_{m\geq 0} g_n"] \\ & A \end{tikzcd}$$

In other words, $\eta(B)_n$ is the canonical morphism commuting the diagram

$$\begin{tikzcd}
R_n \arrow[r, "\eta(B)_n"] \arrow[dr, "g_n"'] & \mathbb{T}(\mathbb{A}(R)) \arrow[d, "\mathbb{T}(\mathbb{A}(g_n))"] \\
 & \mathbb{T}(A)
\end{tikzcd}$$

and hence, $\mathbb{A}$ is the left adjoint of $\mathbb{T}$, proving item (i). By the very definition of $\mathbb{A}$ and $\mathbb{T}$ we get item (iii), and using Proposition 5.1.5 we get item (ii). $\square$

Using Proposition 5.1.5 (and its dual version) we get the following Corollary.

Corollary 5.2.4.

i - $\mathbb{T} : Ring_2 \to Igr$ *preserves all projective limits.*

ii - *If* I *is such that Igr is* I*-inductively complete then for* $\{A_i\}_{i\in I}$ *in Igr we have*

$$\varinjlim_{i\in I} A_i \cong \mathbb{A}\left(\varinjlim_{i\in I} \mathbb{T}(A_i)\right).$$

iii - $\mathbb{F}_2 \in Ring_2$ *is the initial object in* $Ring_2$.

iv - $0 \in Ring_2$ *is the terminal object in* $Ring_2$.

v - $\mathbb{T}(\mathbb{F}_2)$ *is the initial object in Igr.*

vi - $\mathbb{T}(0)$ *is the terminal object in Igr.*

Now we discuss (essentially) the limits and colimits in Igr. Fix a non-empty set I and let $\{(R_i, \top_i, h_i)\}_{i\in I}$ be a family of Igr's. We start with the construction of the Igr-product

$$R = \prod_{i\in I} R_i.$$

For this, we define $R_0 \cong \mathbb{F}_2$ and for all $n \geq 1$, we define

$$R_n := \prod_{i\in I}(R_i)_n \text{ and } \top_n := \prod_{i\in I}(\top_i)_n.$$

In the sequel, we define $h_0 : \mathbb{F}_2 \to R_1$ as the only possible morphism and for $n \geq 1$, we define $h_n : R_n \to R_{n+1}$ by

$$h_n := \prod_{i\in I}(h_i)_n.$$

`boohull-df`

Definition 5.2.5.

i- *The* **space of orderings**, X_R, *of the Igr* R, *is the set of Igr-morphisms* $Igr(R, \mathbb{T}(\mathbb{F}_2)$. *By the Proposition 5.2.3.(i), we have a natural bijection* $Igr(R, \mathbb{T}(\mathbb{F}_2) \cong Ring_2(\mathbb{A}(R), \mathbb{F}_2)$, *thus considering the discrete topologies on the* $\mathbb{F}_2$*-algebras* $\mathbb{A}(R), \mathbb{F}_2)$ *and transporting the boolean topology in* $Ring_2(\mathbb{A}(R), \mathbb{F}_2)$, *we obtain a boolean topology on the space of orderings* $X_R = Igr(R, \mathbb{T}(\mathbb{F}_2))$.

ii- *The* **boolean hull**, $B(R)$, *of the Igr* R, *is the boolean ring canonically associated to the space of orderings of* R *by Stone duality:* $B(R) := \mathcal{C}(X_R, \mathbb{F}_2)$.

iii- *A Igr* R *is called* **formally real** *if* $X_R \neq \emptyset$ *(or, equivalently, if* $B(R) \neq 0$*).*

fixigr1

Proposition 5.2.6. *Let* I *be a non-empty set and* $\{(R_i, h_i)\}_{i \in I}$ *be a family of Igr's. Then*

$$R = \prod_{i \in I} R_i$$

with the above rules is an Igr. Moreover it is the product in the category Igr.

Proof. Using Definition 4.4.1 is straightforward to verify that $(R, \top_n, h_n)$ is an Igr. Note that for each $i \in I$, we have an epimorphism $\pi_i : R \to R_i$ given by the following rules: for each $n \geq 0$ and each $(x_i)_{i \in I} \in R_n$, we define

$$(\pi_i)_n((x_i)_{i \in I}) := x_i.$$

Now, let $(Q, \{q_i\}_{i \in I})$ be another pair with Q being an Igr and $q_i : Q \to R_i$ being a morphism for each $i \in I$. Given $i \in I$ and $n \geq 0$, since $R_n := \prod_{i \in I}(R_i)_n$ is the product in the category of pointed $\mathbb{F}_2$-modules, we have an unique morphism $(q)_n : (Q)_n \to (R)_n$ such that $(\pi_i)_n \circ (q)_n = (q_i)_n$. Set $q_n := ((q_i)_{i \in I})_n$. By construction, q is the unique Igr-morphism such that $\pi_i \circ q = q_i$, completing the proof that R is in fact the product in the category Igr. □

Proposition 5.2.7.

i- *Let* R *be an Igr and let* $X \subseteq R = \bigoplus_{n \in \mathbb{N}} R_n$. *Then there exists the* **inductive graded subring generated by** X *(notation :* $[X] \overset{i_X}{\hookrightarrow} R$*): this is the least inductive graded subring of* R *such that* $\forall n \in \mathbb{N}$, $X \cap R_n \subseteq [X]_n$.

ii- *Let* $\mathcal{I}$ *be a small category and* $\mathcal{R} : \mathcal{R} \to Igr$ *be a diagram. Then there exists* $\varprojlim_{i \in \mathcal{I}} \mathcal{R}_i$ *in the category* Igr.

Proof.

i- It is enough consider S_X , the $\mathbb{F}_2$-subalgebra of $(\bigoplus_{n \in \mathbb{N}} R_n, *)$ generated by $X \cup \{\top_1\} \subseteq \bigoplus_{n \in \mathbb{N}} R_n$ and set $\forall n \in \mathbb{N}$, $[X]_n := s_x \cap R_n$.

ii- Just define $\varprojlim_{i \in \mathcal{I}} \mathcal{R}_i$ as the inductive graded subring of $\prod_{i \in obj(\mathcal{I})} \mathcal{R}_i$ generated by $X_D = \bigoplus_{n \in \mathbb{N}} X_n$ and $X_n := \varprojlim_{i \in \mathcal{I}} (\mathcal{R}_i)_n$ (projective limit of pointed $\mathbb{F}_2$-algebras).

□

Now we construct the Igr-tensor product of a finite family of Igr's, $\{R_i : i \in I\}$

$$R = \bigotimes_{i \in I} R_i.$$

For this, we define $R_0 \cong \mathbb{F}_2$ and for all $n \geq 1$, we define

$$R_n := \bigotimes_{i \in I} (R_i)_n,$$

$$(\otimes_{i\in I} a_i) *_{n,k} (\otimes_{i\in I} b_i) := \otimes_{i\in I}(a_i *^i_{n,k} b_i)$$

$$\text{and } \top_n := \otimes_{i\in I}(\top_i)_n.$$

In particular, if $I = \emptyset$, then $R_n = \{0\}, n \geq 1$. In the sequel, we define $h_0 : \mathbb{F}_2 \to R_1$ as the only possible morphism and for $n \geq 1$, we define $h_n : R_n \to R_{n+1}$ by

$$h_n := \bigotimes_{i\in I} (h_i)_n.$$

In other words, for a generator $\bigotimes_{i\in I} x_i \in R_n$, we have

$$h_n\left(\otimes_{i\in I} x_i\right) := \bigotimes_{i\in I} (h_i)_n(x_i).$$

`fixigr2`

Proposition 5.2.8. *Let I be a finite set and $\{(R_i, h_i)\}_{i\in I}$ be a family of Igr's. Then*

$$R = \bigotimes_{i\in I} R_i$$

with the above rules is an Igr. Moreover it is the coproduct in the category Igr.

Now suppose that $(I, \leq)$ is an upward directed poset and that $((R_i, h_i), \varphi_{ij})_{i\leq j\in I}$ is an inductive system of Igr's. We define the inductive limit

$$R = \varinjlim_{i\in I} R_i$$

by the following: for all $n \geq 0$ define

$$R_n := \varinjlim_{i\in I} (R_i)_n.$$

Note that

$$R_0 := \varinjlim_{i\in I} (R_i)_0 \cong \varinjlim_{i\in I} \mathbb{F}_2 \cong \mathbb{F}_2.$$

In the sequel, for $n \geq 1$ we define $h_n : R_n \to R_{n+1}$ by

$$h_n := \varinjlim_{i\in I} (h_i)_n.$$

`fixigr4`

Proposition 5.2.9. *Let $(I, \leq)$ is an upward directed poset and $((R_i, h_i), \varphi_{ij})_{i\in I}$ be a directed family of Igr's. Then*

$$R = \varinjlim_{i\in I} R_i$$

with the above rules is an Igr. Moreover, it is the inductive limit in the category Igr.

Proposition 5.2.10. *The general coproduct (general tensor product) of a family $\{R_i : i \in I\}$ in* *the category Igr is given by the combination of constructions:*

$$\bigotimes_{i\in I} R_i := \varinjlim_{I'\in P_{fin}(I)} \bigotimes_{i\in I'} R_i.$$

After discussing directed inductive colimits and coproducts, we will deal with ideals, quotients, and coequalizers.

Definition 5.2.11. *Given $R \in Igr$ and $(J_n)_{n\geq 0}$ where $J_n \subseteq R_n$ for all $n \geq 0$. We say that J is a* ***graded ideal*** *of R where*

$$J := \bigoplus_{n\geq 0} J_n \subseteq \bigoplus_{n\geq 0} R_n$$

is an ideal of $(R, *)$.

In particular, for all $n \geq 0$, $J_n \subseteq R_n$ is a graded $\mathbb{F}_2$-submodule of $(R_n, +_n, 0_n)$. For each $X \subseteq R$, there exists the ideal generated by X, denoted by $\langle X\rangle$. It is the smaller graded ideal of R such that for all $n \geq 0$, $(X \cap R_n) \subseteq [X]_n$. For this, just consider $\langle X\rangle$, the ideal of $(R, *)$ generated by $X \subseteq R$ and define $\langle X\rangle_n := \langle X\rangle \cap R_n$.

Definition 5.2.12. *Let R, S be Igr's and $f : R \to S$ be a morphism. We define the* ***kernel*** *of f, notation $Ker(f)$ by*

$$Ker(f)_n := \{x \in R_n : f_n(x) = 0\}$$

and ***image*** *of f, notation $Im(f)$ by*

$$Im(f)_n := \{f_n(x) \in S_n : x \in R_n\}.$$

Of course, $\mathrm{Ker}(f) \subseteq R$ is an ideal and $\mathrm{Im}(f) \subseteq S$ is an Igr.

Given $R \in$ Igr and $J = (J_n)_{n\geq 0}$ a graded ideal of R, we define $R/J \in$ Igr, the **quotient inductive graded ring of R by J**: for all $n \geq 0$, $(R/J)_n := R_n/J_n$, where the distinguished element is $\top_n +_n J_n$. We have a canonical projection $q_J : R \to R/J$, "coordinatewise surjective" and therefore, an Igr-epimorphism.

Proposition 5.2.13 (Homomorphism Theorem)**.** *Let R, S be Igr's and $f : R \to S$ be a morphism. Then there exist an unique monomorphism $\overline{f} : R/Ker(f) \to S$ commuting the following diagram:*

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "q"'] & S \\ R/Ker(f) \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

where q is the canonical projection. In particular $R/Ker(f) \cong Im(f)$.

Proposition 5.2.14. *Let $R \underset{g}{\overset{f}{\rightrightarrows}} S$ be Igr-morphisms and consider $q_J : S \to S/J$ the quotient morphism where $J := \langle X\rangle$ is the graded ideal generated by $X_n := \{f_n(a) - g_n(a) : a \in R_n\}, nzin\mathbb{N}$. Then q_J is the coequalizer of f, g.*

Proposition 5.2.15. *Given $R, S \in Igr$ and $f \in Igr(R, S)$.*

i - *f is a Igr-monomorphism whenever for all $n \geq 0$ $f_n : R_n \to S_n$ is a monomorphism of pointed $\mathbb{F}_2$-modules iff for all $n \geq 0$, $f_n : R_n \to S_n$ is an injective homomorphism of pointed $\mathbb{F}_2$-modules.*

ii - *f is a Igr-epimorphism whenever for all $n \geq 0$ $f_n : R_n \to S_n$ is a epimorphism of pointed $\mathbb{F}_2$-modules iff for all $n \geq 0$, $f_n : R_n \to S_n$ is a surjective homomorphism of pointed $\mathbb{F}_2$-modules.*

iii - *f is a Igr-isomorphism iff for all $n \geq 0$ $f_n : R_n \to S_n$ is a isomorphism of pointed $\mathbb{F}_2$-modules iff for all $n \geq 0$, $f_n : R_n \to S_n$ is a bijective homomorphism of pointed $\mathbb{F}_2$-modules.*

Definition 5.2.16. *We denote Igr_{fin} the full subcategory of Igr such that*

$$Obj(Igr_{fin}) = \{R \in Obj(Igr) : |R_n| < \omega \text{ for all } n \geq 1\}.$$

Remark 5.2.17. *Of course,*

$$\left\{ R \in Obj(Igr) : \left| \bigoplus_{n \geq 1} R_n \right| < \omega \right\} \neq Obj(Igr_{fin}),$$

for example, in 4.4.2(a), if F is a Euclidian field (for instance, any real closed field), then $\bigoplus\limits_{n \in \mathbb{N}} I^n F / I^{n+1} F \cong \mathbb{F}_2[x]$, thus the graded Witt ring of F (see definition 5.4.9) $W_*(F) \in Obj(Igr_{fin})$ but $\mathbb{F}_2[x]$ is not finite.

5.3 Relevant subcategories of Igr

The aim of this Section is to define subcategories of Igr that mimetize the following two central aspects of K-theories:

1. The K-theory graded ring is "generated" by K_1;

2. The K-theory graded ring is defined by some convenient quotient of a graded tensor algebra.

Our desired category will be the intersection of two subcategories. The first one is obtained after we define the **graded subring generated by the level 1** functor

$$\mathbb{1} : \text{Igr} \to \text{Igr}.$$

We define it as follow: for an object $R = ((R_n)_{n \geq 0}, (h_n)_{n \geq 0}, *_{nm})$,

i - $\mathbb{1}(R)_0 := R_0 \cong \mathbb{F}_2$,

ii - $\mathbb{1}(R)_1 := R_1$,

iii - for $n \geq 2$,

$$\mathbb{1}(R)_n := \{x \in R_n : x = \sum_{j=1}^{r} a_{1j} *_{11} ... *_{11} a_{nj},$$
$$\text{with } a_{ij} \in R_1,\ 1 \leq i \leq n,\ 1 \leq j \leq r \text{ for some } r \geq 1\}.$$

Note that for all $n \geq 2$, R_n is generated by the expressions of type

$$d_1 *_{11} d_2 *_{11} ... *_{11} d_n,\ d_i \in R_1,\ i = 1, ..., n.$$

Of course, $\mathbb{1}(R)$ provides an inclusion $\iota_{\mathbb{1}(R)} : \mathbb{1}(R) \to R$ in the obvious way.

On the morphisms, for $f \in \mathrm{Igr}(R,S)$, we define $\mathbb{1}(f) \in \mathrm{Igr}(\mathbb{1}(R), \mathbb{1}(S))$ by the restriction $\mathbb{1}(f) = f\restriction_{\mathbb{1}(R)}$. In other words, $\mathbb{1}(f)$ is the only Igr-morphisms that makes the following diagram commute:

$$\begin{tikzcd}
\mathbb{1}(R) \arrow[r, "\iota_{\mathbb{1}(R)}"] \arrow[d, "\mathbb{1}(f)"'] & R \arrow[d, "f"] \\
\mathbb{1}(S) \arrow[r, "\iota_{\mathbb{1}(S)}"'] & S
\end{tikzcd}$$

level1

Definition 5.3.1. *We denote $Igr_{\mathbb{1}}$ the full subcategory of Igr such that*

$$Obj(Igr_{\mathbb{1}}) = \{R \in Igr : \iota_{\mathbb{1}(R)} : \mathbb{1}(R) \to R \text{ is an isomorphism}\}.$$

Example 5.3.2.

i - If A is a $\mathbb{F}_2$-algebra, then $\mathbb{T}(A) \in obj(Igr_{\mathbb{1}})$.

ii - If F is an hyperbolic hyperfield, then $k_*(F) \in obj(Igr_{\mathbb{1}})$.

iii - If F is a special hyperfield (equivalently, $G = F \setminus \{0\}$ is a special group), then the graduate Witt ring of F (definition 5.4.9) $W_*(F) \in obj(Igr_{\mathbb{1}})$.

iv - If F is a field with $char(F) \neq 2$, then, by a known result of Vladimir Voevodski,

$$\mathcal{H}^*(Gal(F^s|F), \{\pm 1\}) \in obj(Igr_{\mathbb{1}}).$$

Proposition 5.3.3.

i - For each $R \in Igr$ we have that $\iota_{\mathbb{1}(\mathbb{1}(R))} : \mathbb{1}(\mathbb{1}(R)) \to \mathbb{1}(R)$ is the identity arrow.

ii - $\mathbb{1} \circ \mathbb{1} = \mathbb{1}$.

iii - The functor $\mathbb{1} : Igr \to Igr_{\mathbb{1}}$ is the right adjoint of the inclusion functor $j_{\mathbb{1}} : Igr_{\mathbb{1}} \to Igr$.

iv - $j_{\mathbb{1}} : Igr_{\mathbb{1}} \to Igr$ creates inductive limits and to obtain the projective limits in $Igr_{\mathbb{1}}$ is sufficient restrict the projective limits obtained in Igr:

$$\varprojlim_{i\in I} R_i \cong \left(\varprojlim_{i\in I} j_{\mathbb{1}}(R_i)\right)_{\mathbb{1}} \xrightarrow{\varprojlim_{i\in I} j_{\mathbb{1}}(R_i)} \varprojlim_{i\in I} j_{\mathbb{1}}(R_i).$$

Proof. Similar to Proposition 5.2.3. □

Now we define the second subcategory. We define the **quotient graded ring functor**

$$\mathcal{Q} : \mathrm{Igr} \to \mathrm{Igr}$$

as follow: for a object $R = ((R_n)_{n\geq 0}, (h_n)_{n\geq 0}, *_{nm})$, $\mathcal{Q}(R) := R/T$, where $T = (T_n)_{n\geq 0}$ is the ideal generated by $\{(\top_1 +_1 a) *_{11} a \in R_2 : a \in R_1\}$. More explicit, i - $T_0 := \{0_0\} \subseteq R_0$,

ii - $T_1 := \{0_1\} \subseteq R_1$,

iii - for $n \geq 2$, $T_n \subseteq R_n$ is the pointed $\mathbb{F}_2$-submodule generated by

$$\{x \in R_n : x = y_l *_{l1} (\top_1 +_1 a_1) *_{11} a_1 *_{1r} z_r, \\ \text{with } a_1 \in R_1,\ y_l \in R_l,\ z_r \in R_r,\ l+r = n-2\}.$$

Of course, $\mathcal{Q}(R)$ provides a projection $\pi_R : R \to \mathcal{Q}(R)$ in the obvious way.

On the morphisms, for $f \in \mathrm{Igr}(R,S)$, we define $\mathcal{Q}(f) \in \mathrm{Igr}(\mathcal{Q}(R),\mathcal{Q}(S))$ by the only Igr-morphisms that makes the following diagram commute:

$$\begin{tikzcd} R \arrow[r, "\pi_R"] \arrow[d, "f"'] & \mathcal{Q}(R) \arrow[d, "\mathcal{Q}(f)"] \\ S \arrow[r, "\pi_S"'] & \mathcal{Q}(S) \end{tikzcd}$$

quotop

Definition 5.3.4. *We denote Igr_h the full subcategory of Igr such that*

$$Obj(Igr_h) = \{R \in Igr : \pi_R : R \to \mathcal{Q}(R) \text{ is an isomorphism}\}.$$

Remark 5.3.5. *Note that $R \in obj(Igr_h)$ iff for each $a \in R_1$, $a *_{11} \top_1 = a *_{11} a \in R_2$. Each R satisfying this condition is, in some sense, "hyperbolic" (see Proposition 5.5.2): this is the motivation of the index "h".*

Example 5.3.6. *i- Let A be a $\mathbb{F}_2$-algebra. Then $\mathbb{T}(A) \in obj(Igr_h)$ iff A is a boolean ring (i.e., $\forall a \in A, a^2 = a$).*

ii- If F is an hyperbolic hyperfield, then $k_*(F) \in obj(Igr_h)$.

iii- If F is a special hyperfield (equivalently, $G = F \setminus \{0\}$ is a special group), then $W_*(F) \in obj(Igr_h)$.

iv- If F is a field with $char(F) \neq 2$, then $\mathcal{H}^*(Gal(F^s|F), \{\pm 1\}) \in obj(Igr_h)$.

Proposition 5.3.7.

i - For each $R \in Igr$ we have that $\pi_{\mathcal{Q}(R)} : \mathcal{Q}(R) \to \mathcal{Q}(\mathcal{Q}(R))$ is an isomorphism.

ii - $\mathcal{Q} \circ \mathcal{Q} = \mathcal{Q}$.

iii - The functor $\mathcal{Q} : Igr \to Igr_h$ is the left adjoint of the inclusion functor $j_q : Igr_{\mathcal{Q}} \to Igr$.

iv - $j_q : Igr_h \to Igr$ creates projective limits and to obtain the inductive limits in Igr_h is sufficient restrict the inductive limits obtained in Igr:

$$\varinjlim_{i \in I} j_q(R_i) \xrightarrow{\varinjlim_{i\in I} j_q(R_i)} \left(\varinjlim_{i \in I} j_q(R_i)\right)_{\mathcal{Q}} \cong \varinjlim_{i \in I} R_i.$$

Moreover, $j_q : Igr_h \to Igr$ creates filtered inductive limits and quotients by graded ideals.

Are examples of inductive graded rings in Igr_+: (i) $\mathbb{T}(A)$, where A is a boolean ring; (ii) $k_*(F)$, where F is an hyperbolic hyperfield; (iii) $W_*(F)$, where F is an special hyperfield; (iv) $\mathcal{H}^*(Gal(F^s|F), \{\pm 1\})$, where F is a field with $char(F) \neq 2$.

igr+

Definition 5.3.8 (The Category Igr_+)**.** *We denote by Igr_+ the full subcategory of Igr such that*

$$Obj(Igr_+) = Obj(Igr_{\mathbb{1}}) \cap Obj(Igr_h).$$

We denote by $j_+ : Igr_+ \to Igr$ the inclusion functor.

Remark 5.3.9. *i- Note that the notion of an Igr, R, be in the subcategory Igr_h can be axiomatized by a first-order (finitary) sentence in L, the polysorted language for Igr's described in the previous Chapter: $(\forall a : 1, a *_{11} a = \top_1 *_{11} a)$. On the other hand, the concepts $R \in Igr_{\mathbb{1}}$ and $R \in Igr_+$ are axiomatized by $L_{\omega_1,\omega}$-sentences.*

ii- Note that the subcategory $Igr_+ \hookrightarrow Igr$ is closed by filtered inductive limits.

In order to think of an object in Igr_+ as a graded ring of "K-theoretic type", we make the following convention.

igrlog

Definition 5.3.10 (Exponential and Logarithm of an Igr)**.** *Let $R \in Igr_+$ and write R_1 **multiplicatively** by $(\Gamma(R), \cdot, 1, -1)$, i.e, fix an isomorphism $e_R : R_1 \to \Gamma(R)$ in order that $e_R(\top) = -1$ and $e_R(a + b) = a \cdot b$. Such isomorphism e_R is called **exponential** of R and $l_R = e_R^{-1}$ is called **logarithm** of R. In this sense, we can write $R_1 = \{l(a) : a \in \Gamma(R)\}$. We also denote $l(a) *_{11} l(b)$ simply by $l(a)l(b)$, $a, b \in \Gamma(R)$. We drop the superscript and write just e, l when the context allows it.*

Using Definitions 5.3.8, 5.3.10 (and of course, Definitions 5.3.1 and 5.3.4 with an argument similar to the used in Lemma 4.3.2) we have the following properties.

igr_+first

Lemma 5.3.11 (First Properties)**.** *Let $R \in Igr_+$.*

i - $l(1) = 0$.

ii - For all $n \geq 1$, $\eta \in R_n$ is generated by $l(a_1)...l(a_n)$ with $a_1, ..., a_n \in \Gamma(R)$.

iii - $l(a)l(-a) = 0$ and $l(a)l(a) = l(-1)l(a)$ for all $a \in \Gamma(R)$.

iv - $l(a)l(b) = l(b)l(a)$ for all $a, b \in \Gamma(R)$.

v - For every $a_1, ..., a_n \in \Gamma(R)$ and every permutation $\sigma \in S_n$,

$$l(a_1)...l(a_i)...l(a_n) = sgn(\sigma)l(a_{\sigma 1})...l(a_{\sigma n}) \text{ in } R_n.$$

vi - For all $\xi \in R_n$, $\eta \in R_n$,

$$\xi\eta = \eta\xi.$$

vii - For all $n \geq 1$,

$$h_n(l(a_1)...l(a_n)) = l(-1)l(a_1)...l(a_n).$$

igr_+prop

Proposition 5.3.12. *Let $R \in Igr_+$*

i- *For each* $n \in \mathbb{N}$ *and each* $x \in R_n$, $x *_{n,n} x = \top_n *_{n,n} x \in R_{2n}$.

ii- $\mathbb{A}(R) = \varinjlim_{n\in\mathbb{N}} R_n$ *is a boolean ring (or, equivalently,* $\mathbb{T}(\mathbb{A}(R)) \in Igr_+$*).*

Proof.

i- The property is clear if $n = 0$. If $n \geq 1$, then the property can be verified by induction on the number of generators $k \geq 1, x = \sum_{i=1}^{k} a_{1,i} *_{1,1} a_{2,i} *_{1,1} \cdots *_{1,1} a_{n,i} \in R_n$: if $k = 1$, then note that

$$\begin{aligned} x *_{n,n} x &= (a_1 * a_2 * \cdots * a_n) * (a_1 * a_2 * \cdots * a_n) \\ &= (a_1 * a_1) * (a_2 * a_2) * \cdots (a_n * a_n) = (\top_1 * a_1) * (\top_1 * a_2) * \cdots * (\top_1 * a_n) \\ &= (\top_n) * (a_1 * a_2 * \cdots * a_n); \end{aligned}$$

if $k > 1$, write $x = y + z$, where $y, z \in R_n$ are have $< k$ generator and then, by induction,

$$\begin{aligned} x *_{n,n} x = (y+z) *_{n,n} (y+z) &= y *_{n,n} y + y *_{n,n} z + z *_{n,n} y + z *_{n,n} z \\ &= y *_{n,n} y + z *_{n,n} z = \top_n *_{n,n} y + \top_n *_{n,n} z \\ &= \top_n *_{n,n} (y+z) = \top_n *_{n,n} x \end{aligned}$$

ii- This follows directly from item (i) and the definition of the ring structure in $\mathbb{A}(R) = \varinjlim_{n\in\mathbb{N}} R_n$.

□

By the previous Proposition and the universal property of the boolean hull of an Igr (Definition 5.2.5.(ii)), we obtain:

igr+co

Corollary 5.3.13. *Let* $R \in Igr_+$*. Then:*

i- $X_{\mathbb{T}(\mathbb{A}(R))} \approx X_R$.

ii- $\mathbb{A}(R) \cong B(R)$.

Lemma 5.3.14.

i - *Given* $R \in Igr_{\mathbb{1}}$, $S \in Igr$ *and* $f : S \to j_{\mathbb{1}}(R)$, *we have:* f *is coordinatewise surjective iff* $f_1 : S_1 \to R_1$ *is a surjective morphism of pointed* $\mathbb{F}_2$*-modules.*

ii - *Given* $R \in Igr_{\mathbb{1}}$, $S \in Igr$ *and* $f, h \in Igr(j_{\mathbb{1}}(R), S)$, *we have* $f = h$ *if and only if* $f_1 = h_1$.

Let $R, S \in$ Igr. The inclusion function $\iota_R : \mathbb{1}(R) \to R$ and projection function $\pi_R : R \to \mathcal{Q}(R)$ induces respective natural transformations $\iota : \mathbb{1} \Rightarrow 1_{Igr}$ and $\pi : 1_{Igr} \Rightarrow \mathcal{Q}$. Moreover, we have a natural transformation $can : \mathcal{Q}\mathbb{1} \Rightarrow \mathbb{1}\mathcal{Q}$ given by the rule $can_n(l(a_1)...l(a_n)) := l(a_1)...l(a_n)$, $n \geq 1$. (can_n is well defined and is an isomorphism basically because both $\mathcal{Q}\mathbb{1}(R)$ and $\mathbb{1}\mathcal{Q}(R)$ are generated in level 1 by R_1 and both graded rings satisfies the relation $l(a)l(-a) = 0$).

We have another immediate consequence of the previous results (and adjunctions):

Lemma 5.3.15.

i - *For all* $R \in Igr_h$, $\mathbb{1}(R) \in Igr_+$ *and* can_R *is an isomorphism.*

ii - *For all* $R \in Igr_{\mathbb{1}}$, $\mathcal{Q}(R) \in Igr_+$ *and* can_R *is an isomorphism.*

iii - To get projective limits in Igr_+ is enough to restrict the projective limits obtained in Igr:

$$\varprojlim_{i\in I} R_i \cong \mathbb{1}\left(\varprojlim_{i\in I} j_+(R_i)\right).$$

iv - To get inductive limits in Igr_+ is enough to restrict the inductive limits obtained in Igr:

$$\varinjlim_{i\in I} R_i \cong \mathcal{Q}\left(\varinjlim_{i\in I} j_+(R_i)\right).$$

5.4 Examples and Constructions of Quadratic Interest

Definition 5.4.1. *A **filtered ring** is a tuple $A = (A, (J_n)_{n\geq 0}, +, \cdot, 0, 1)$ where:*

i - $(A, +, \cdot, 0, 1)$ is a commutative ring with unit.

ii - $J_0 = A$ and for all $n \geq 1$, $J_n \subseteq A$ is an ideal.

iii - For all $n, m \geq 0$, $n \leq m \Rightarrow J_n \supseteq J_m$.

iv - For all $n, m \geq 0$, $J_n \cdot J_m \subseteq J_{n+m}$.

v - $J_0/J_1 \cong \mathbb{F}_2$ (then $2 = 1 + 1 \in J_1$).

vi - For all $n \geq 0$, J_n/J_{n+1} is a group of exponent 2 (then $2 \cdot J_n \subseteq J_{n+1}$ and $2^n \in J_n$).

*A **morphism** $f : A \to A'$ of filtered rings is a ring homomorphism such that $f(J_n) \subseteq J'_n$. The category of filtered rings will be denoted by FRing.*

gradfilt

Definition 5.4.2. *We define the **inductive graded ring associated functor***

$$Grad : FRing \to Igr$$

for $f : FRing(A, B)$ as follow: $Grad(A) := ((Grad(A)_n)_{n\geq 0}, (t_n)_{n\geq 0}, *) \in Igr$ is the igr where

i - For all $n \geq 0$, $Grad(A)_n := (J_n/J_{n+1}, +_n, 0_n, \top_n)$ is the exponent 2 group with distinguished element $\top_n := 2^n + J_{n+1}$.

ii - For all $n \geq 0$, $t_n : Grad(A)_n \to Grad(A)_{n+1}$ is defined by $t_n := 2 \cdot \_$, i.e,

$$\text{For all } a + J_{n+1} \in J_n/J_{n+1},\ t_n(a + J_{n+1}) := 2 \cdot a + J_{n+2} \in J_{n+1}/J_{n+2}.$$

Observe that $t_n(\top_n) = \top_{n+1}$, i.e, t_n is a morphism of pointed $\mathbb{F}_2$-modules.

iii - For all $n, m \geq 0$ the biadditive function $*_{nm} : Grad(A)_n \times Grad(A)_m \to Grad(A)_{n+m}$ is defined by the rule

$$(a_n + J_{n+1}) *_{mn} (b_m + J_{m+1}) = a_n \cdot b_m + J_{n+m+1} \in J_{n+m}/J_{n+m+1}.$$

The group $A_g := \bigoplus_{n\geq 0} Grad(A)_n$ of exponent 2 and the induced application $* : A_g \times A_g \to A_g$ are such that $(A_g, *)$ is a commutative ring with unit $\top_1 = (2 + J_2) \in J_1/J_2$.

iv - For all $n \geq 1$, $t_n = \top_1 *_{1n} \_$.

The morphism $Grad(f) \in Igr(Grad(A), Grad(A'))$ is defined by the following rules: for all $n \geq 0$, $f_n : Grad(A)_n \to Grad(A')_n$ is given by

$$f_n(a + J_{n+1}) := f_n(a) + J'_{n+1}.$$

Note that f_n a homomorphism of $\mathbb{F}_2$-pointed modules and $\bigoplus_{n\geq 0} f_n : (A_g, *) \to (A'_g, *)$ is a homomorphism of graded rings with unit.

igrcont

Definition 5.4.3. *The **functor of graded ring of continuous functions** over a space X*

$$\mathcal{C}(X, \_) : Igr \to Igr$$

is the functor defined for $f : R \to S$ by

i - $\mathcal{C}(X, R)_0 := R_0 \cong \mathbb{F}_2$,

ii - for all $n \geq 1$, $\mathcal{C}(X, R)_n := \mathcal{C}(X, R_n)$ as a pointed $\mathbb{F}_2$-module,

iii - for all $n, m \geq 0$, $*^X_{nm} : \mathcal{C}(X, R_n) \times \mathcal{C}(X, R_m) \to \mathcal{C}(X, R_{n+m})$ is given by $(\alpha_n, \beta_m) \mapsto \alpha_n *^X_{nm} \beta_m$, where for $x \in X$,

$$\alpha_n *^X_{nm} \beta_m(x) = \alpha_n(x) *_{nm} \beta_m(x) \in R_{n+m}.$$

iv - $\mathcal{C}(X, f)_0 := f_0$ as an homomorphism of pointed $\mathbb{F}_2$-modules $R_0 \to S_0$.

v - for all $n \geq 1$, $\mathcal{C}(X, f)_n := \mathcal{C}(X, f_n) := f_n \circ \_ \in p\mathbb{F}_2 - mod(\mathcal{C}(X, R_n), \mathcal{C}(X, S_n))$.

Remark 5.4.4. *Let X be a topological space and let $R \in Igr_{\mathbb{1}}$. Note that if X is compact or $R \in Igr_{fin}$, then $\mathcal{C}(X, R) \in Igr_{\mathbb{1}}$.*

sgfilt

Definition 5.4.5. *We define the **continuous function filtered ring functor***

$$\mathcal{C} : SG \to FRing$$

as follow: first, consider the functor $\mathcal{C}(X_\_, \mathbb{Z}) : SG \to Ring$, composition of the (contravariant) functors "associated ordering space" $X_\_ : SG \to Top^{op}$ and "continuous functions in $\mathbb{Z}$ ring" $\mathcal{C}(\_, \mathbb{Z}) : Top^{op} \to Ring$ (here $\mathbb{Z}$ is endowed with the discrete topology).

Now we define the functor $\mathcal{C} : SG \to FRing$: given a special group $G \in SG$, we define

$$\mathcal{C}(G) := (R(G), (J_n(G))_{n\geq 0}, +, \cdot, 0, 1)$$

where

i - $(R(G), +, \cdot, 0, 1)$ is the subring of $\mathcal{C}(X_G, \mathbb{Z})$ of continuous functions of constant parity, i.e, $R(G) := J_0(G) \xrightarrow{i_0(G)} \mathcal{C}(X_G, \mathbb{Z})$ is the image of the monomorphism of rings with unit

$$j_0(G) : \mathcal{C}(X_G, 2\mathbb{Z}) \cup \mathcal{C}(X_G, 2\mathbb{Z} + 1) \to \mathcal{C}(X_G, \mathbb{Z}).$$

ii - For all $n \geq 1$, $J_n(G) \xrightarrow{i_n(G)} J_0(G)$ is the ideal of $R(G)$ (and also of $\mathcal{C}(X_G, \mathbb{Z})$) that is the image of the monomorphism of abelian groups

$$j_n(G) : \mathcal{C}(X_G, 2^n\mathbb{Z}) \to \mathcal{C}(X_G, 2\mathbb{Z}) \cup \mathcal{C}(X_G, 2\mathbb{Z} + 1).$$

We also have $J_0(G)/J_1(G) \cong \mathbb{F}_2$ *and for all* $n, m \geq 0$*:*

a - *If* $n \geq m$ *then* $J_n(G) \supseteq J_m(G)$*;*

b - $J_n(G) \cdot J_m(G) \subseteq J_{n+m}(G)$*;*

c - $2J_n(G) = J_{n+1}(G) \Rightarrow J_n(G)/J_{n+1}(G)$ *is an exponent 2 group.*

On the morphisms, for $f \in SG(G, G')$*, we define* $\mathcal{C}(f) \in FRing(\mathcal{C}(G), \mathcal{C}(G'))$ *by*

$$\mathcal{C}(f)(h) = \mathcal{C}(X_f, \mathbb{Z})(h)$$

for $h \in \mathcal{C}(G)$*.* $\mathcal{C}(f)$ *is well-defined because* $\mathcal{C}(f) \in Ring(\mathcal{C}(G), \mathcal{C}(G'))$ *and for all* $n \geq 0$*,*

$$\mathcal{C}(f)(J_n(G)) \subseteq J_n(G').$$

Definition 5.4.6. *We define the* ***continuous function graded ring functor*** *by*

$$Grad \circ \mathcal{C} : SG \to Igr.$$

For convenience, we describe this functor now: given $G \in \mathrm{SG}$,

$$Grad(\mathcal{C}(G)) := ((Grad(\mathcal{C}(G))_n)_{n \geq 0}, (t_n)_{n \geq 0}, \cdot)$$

where:

i - $Grad(\mathcal{C}(G))_n := (J_n(G)/J_{n+1}(G), \cdot, 0 \cdot J_{n+1}(G), 2^n J_{n+1}(G))$, where $2 \in \mathcal{C}(X_G, \mathbb{Z})$ is the constant function of value $2 \in 2\mathbb{Z} \subseteq \mathbb{Z}$.

ii - For all $n \geq 0$, $J_n(G)/J_{n+1}(G) \xrightarrow{t_2 = 2 \cdot \_} J_{n+1}(G)/J_{n+2}(G)$.

iii - For all $n, m \geq 0$, $*_{nm} : J_n(G)/J_{n+1}(G) \times J_m(G)/J_{m+1}(G) \to J_{n+m}(G)/J_{n+m+1}(G)$ is given by
$$(h_n + J_{n+1}(G)) *_{nm} (k_m + J_{m+1}(G)) = h_n k_m + J_{n+m+1}(G).$$

On the morphisms, given $f \in SG(G, G')$, we have that

$$Grad(\mathcal{C}(f)) = (Grad(\mathcal{C}(f))_n)_{n \geq 0} \in \mathrm{Igr}(Grad(\mathcal{C}(G), Grad(\mathcal{C}(G')),$$

where for all $n \geq 0$, $Grad(\mathcal{C}(f))_n : Grad(\mathcal{C}(G))_n \to Grad(\mathcal{C}(G'))_n$ is such that

$$Grad(\mathcal{C}(f))_n(h + J_{n+1}(G)) = \mathcal{C}(f)(h) + J'_{n+1}(G').$$

Proposition 5.4.7.

a - *There is a natural isomorphism* $\theta : Grad \circ \mathcal{C} \xrightarrow{\cong} \mathbb{T} \circ \mathcal{C}(X_{\_}, \mathbb{F}_2)$*. In particular, for all* $G \in SG$*,* $Grad(\mathcal{C}(G)) \in Igr_+$*.*

b - *For all* $0 < n \leq m < \omega$*,* $2^{m-n} \cdot \_ : J_n(G)/J_{n+1}(G) \to J_m/J_{m+1}(G)$ *is an isomorphism of groups of exponent 2.*

c - *For all* $n \geq 1$*, there is an isomorphism of groups of exponent 2*

$$\theta_n(G) : J_n(G)/J_{n+1}(G) \xrightarrow{\cong} \mathcal{C}(X_G, \mathbb{F}_2),$$

given by the rule

$$\theta_n(h + J_n(G))(\sigma) := h_n(\sigma)/2^n \in \mathcal{C}(X_G, \mathbb{Z}/2\mathbb{Z}).$$

d - *For all* $0 < n \leq m < \omega$ *the following diagram commute:*

$$\begin{tikzcd}
J_n(G)/J_{n+1}(G) \arrow[rr, "2^{m-n}\cdot_"] \arrow[dr, "\theta_n(G)"'] & & J_m(G)/J_{m+1}(G) \arrow[dl, "\theta_m(G)"] \\
& \mathcal{C}(X_G, \mathbb{F}_2) &
\end{tikzcd}$$

filtered Witt ring functor

Definition 5.4.8. *We define the* ***filtered Witt ring functor***

$$\mathcal{W} : SG \to FRing$$

for $f \in SG(G, H)$ *as follow: given a special group* $G \in SG$*, we define*

$$\mathcal{W}(G) := (W(G), I^n(G)_{n\geq 0}, \oplus, \otimes, \langle\rangle, \langle 1\rangle)$$

where for all $n \geq 0$*,* $I^n(G)$ *is the n-th power of the fundamental ideal*

$$I(G) := \{\varphi \in W(G) : \dim_2(\varphi) = 0\}.$$

We define $\mathcal{W}(f) \in FRing(\mathcal{W}(G), \mathcal{W}(H))$ *by the rule* $\mathcal{W}(f)(\varphi) := f \star \varphi$*.*

$\mathcal{W}(G)$ is a filtered commutative ring with unit because:

i - $(W(G), \oplus, \otimes, \langle\rangle, \langle 1\rangle) \in$ Ring.

ii - For all $n \geq 0$, $I^n(G) \subseteq W(G)$ is an ideal.

iii - For all $n, m \geq 0$, $n \leq m \Rightarrow I^n(G) \supseteq I^m(G)$.

iv - For all $n, m \geq 0$, $I^n(G) \otimes I(G) \subseteq I^{n+m}(G)$.

v - $I^0(G) := W(G)$.

vi - $I^0(G)/I^1(G) \cong \mathbb{F}_2$.

vii - For all $n \geq 0$, $(I^n(G)/I^{n+1}(G), \oplus, \langle\rangle)$ is a group of exponent 2 with distinguished element $2^n + I^{n+1}(G)$, where $2^n = \otimes_{i<n}\langle 1, 1\rangle$.

graded Witt ring functor

Definition 5.4.9. *We define the* ***graded Witt ring*** *functor*

$$Grad \circ \mathcal{W} : SG \to Igr.$$

We register, again, the following result:

Proposition 5.4.10. *For each* $G \in SG$ *we have* $Grad(\mathcal{W}(G)) \in Igr_+$*.*

For each commutative ring with unit A, we have

$$t(A) = \{a \in A : \text{ exists } n \geq 0 \text{ with } n \cdot a = 0\} \subseteq A$$

is an ideal (the torsion ideal of A). The association $A \mapsto A/t(A)$ is the component on the objects of an endofunctor of Ring.

For each $G \in SG$ we have a ring homomorphism with unit $\mathrm{sgn}_G : W(G) \to \mathcal{C}(X_G, \mathbb{Z})$ given by the rule

$$\mathrm{sgn}_G(\langle a_0, ..., a_{n-1}\rangle)(\sigma) := \sum_{i=0}^{n-1} \sigma(a_i).$$

The Pfister Local-Global principle says that sgn_G induces a monomorphism

$$\mathrm{rsgn}_G : W(G)/t(W(G)) \to \mathcal{C}(X_G, \mathbb{Z}).$$

For each $G \in SG$ we have $\mathrm{sgn}_G(W(G)) \subseteq \mathcal{C}(X_G, 2\mathbb{Z}) \cup \mathcal{C}(X_G, 2\mathbb{Z}+1)$ (since the signatures of classes of forms has the same parity of its dimension) and for all $n \geq 1$, $\mathrm{sgn}_G(I^n(G)) \subseteq \mathcal{C}(X_G, 2^n\mathbb{Z})$ (since $I^n(G)$ is the abelian subgroup of $W(G)$ generated by classes of Pfister forms of dimension 2^n).

$\mathrm{sgn} : \mathcal{W} \to \mathcal{C}$ (respectively $\mathrm{rsgn} : \mathcal{W}/t(\mathcal{W}) \to \mathcal{C}$) is the natural transformation between functors

$$SG \overset{\mathcal{W}}{\underset{\mathcal{C}}{\rightrightarrows}} \text{FRing}$$

that provide natural transformations between functors $SG \rightrightarrows \text{Igr}$:

$$\text{Grad} \cdot \text{sgn} : \text{Grad} \circ \mathcal{W} \to \text{Grad} \circ \mathcal{C}, \text{ respectively}$$
$$\text{Grad} \cdot \text{rsgn} : \text{Grad} \circ (\mathcal{W}/t(\mathcal{W})) \to \text{Grad} \circ \mathcal{C}.$$

Remember that [MC] ([LC]) and [WMC] ([WLC]) are conjectures about these natural transformations.

$\mathcal{C}$ is a particular case of $\mathcal{W}$ in the following sense: $\mathcal{C} : SG \to \text{FRing}$ is naturally isomorphic to the composition of functors $SG \xrightarrow{\gamma\circ\beta} SG \xrightarrow{\mathcal{W}} \text{FRing}$.

5.5 The adjunction between PSG and $\mathbf{Igr}_h$

By the very definition of the K-theory of hyperfields (with the notations in Theorem 4.3.3) we define the following functor.

Definition 5.5.1 (K-theories Functors). *With the notations of Theorem 4.3.3 we have a functors $k : \mathcal{HMF} \to Igr_+$, $k : \mathcal{PSMF} \to Igr_+$ induced by the reduced K-theory for hyperfields.*

Now, let $R \in \text{Igr}_h$. We define a hyperfield $(\Gamma(R), +, -\cdot, 0, 1)$ by the following: firstly, fix an exponential isomorphism $e_R : (R_1, +_1, 0_1, \top_1) \to (G(R), \cdot, 1, -1)$ (in agreement with Definition 5.3.10). This isomorphism makes, for example, an element $a *_{11} (\top_1 + b) \in R_2$, $a, b \in R_1$ take the form $(l_R(x)) *_{11} (l_R((-1) \cdot y)) \in R_2$, $x, y \in G(R)$. By an abuse of notation, we simply write $l_R(x)l_R(-y) \in R_2$, $x, y \in G(R)$. In this sense, an element in Q_2 has the form $l_R(x)l_R(-x)$, $x \in \Gamma(R)$, and we can extend this terminology for all Q_n, $n \geq 2$ (see Definition 5.3.4, and Lemma 5.3.11).

Now, let $\Gamma(R) := G(R) \cup \{0\}$ and for $a, b \in \Gamma(R)$ we define

$$
\begin{aligned}
-a &:= (-1) \cdot a, \\
a \cdot 0 = 0 \cdot a &:= 0, \\
a + 0 = 0 + a &= \{a\}, \\
a + (-a) &= \Gamma(R), \\
&\text{for } a, b \neq 0, a \neq -b \text{ define} \\
a + b &:= \{c \in \Gamma(R) : \text{there exist } d \in G(R) \text{ such that} \\
&\quad a \cdot b = c \cdot d \in G(R) \text{ and } l_R(a)l_R(b) = l_R(c)l_R(d) \in R_2\}.
\end{aligned} \tag{5.1}
$$

gammahyper

prespechf

Proposition 5.5.2. *With the above rules,* $(\Gamma(R), +, -\cdot, 0, 1)$ *is a pre-special hyperfield.*

Proof. We will verify the conditions of Definition 1.2.7. Note that by the definition of multivalued sum once we proof that $\Gamma(R)$ is an hyperfield, it will be hyperbolic. In order to prove that $(\Gamma(R), +, -\cdot, 0, 1)$ is a multigroup we follow the steps below. Here we use freely the properties in Lemma 5.3.11.

i - Commutativity and $(a \in b + 0) \Leftrightarrow (a = b)$ are direct consequence of the definition of multi-valuated sum and the fact that $l_R(a)l_R(b) = l_R(b)l_R(a)$.

ii - We will prove that if $c \in a + b$, then $a \in c - b$ and $b \in c - a$.

If $a = 0$ (or $b = 0$) or $a = -b$, then $c \in a + b$ means $c = a$ or $c \in a - a$. In both cases we get $a \in c - b$ and $b \in c - a$.

Now suppose $a, b \neq 0$ with $a \neq -b$. Let $c \in a + b$. Then $a \cdot b = c \cdot d$ and $l_R(a)l_R(b) = l_R(c)l_R(d) \in R_2$ for some $d \in G(R)$. Since $G(R)$ is a multiplicative group of exponent 2, we have $a \cdot d = b \cdot c$ (and hence $a \cdot (-d) = c \cdot (-b)$). Note that

$$
\begin{aligned}
l_R(a)l_R(-d) &= l_R(a)l_R(-abc) = l_R(a)l_R(bc) = l_R(a)l_R(b) + l_R(a)l_R(c) \\
&= l_R(c)l_R(d) + l_R(a)l_R(c) = l_R(c)l_R(d) + l_R(c)l_R(a) = l_R(c)l_R(ad).
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
l_R(b)l_R(-c) &= l_R(b)l_R(-abd) = l_R(b)l_R(ad) = l_R(b)l_R(a) + l_R(b)l_R(d) \\
&= l_R(a)l_R(b) + l_R(b)l_R(d) = l_R(c)l_R(d) + l_R(b)l_R(d) \\
&= l_R(bc)l_R(d) = l_R(ad)l_R(d).
\end{aligned}
$$

Then

$$
\begin{aligned}
l_R(a)l_R(-d) - l_R(b)l_R(-c) &= l_R(c)l_R(ad) - l_R(ad)l_R(d) = \\
&= l_R(c)l_R(ad) - l_R(d)l_R(ad) = l_R(-cd)l_R(ad).
\end{aligned}
$$

But

$$
\begin{aligned}
l_R(-cd)l_R(ad) &= l_R(-cd)l_R(a) + l_R(-cd)l_R(d) = \\
&= l_R(-cd)l_R(a) + l_R(c)l_R(d) = l_R(a)l_R(-cd) + l_R(a)l_R(b) \\
&= l_R(a)l_R(-bcd) = l_R(a)l_R(-a) = 0.
\end{aligned}
$$

Then

$$l_R(a)l_R(-d) = l_R(b)l_R(-c),$$

proving that $a \in b - c$. Similarly we prove that $b \in -c + a$.

iii - Since $(G(R), \cdot, 1)$ is an abelian group, we conclude that $(\Gamma(R), \cdot, 1)$ is a commutative monoid. Beyond this, every nonzero element $a \in \Gamma(R)$ is such that $a^2 = 1$.

iv - $a \cdot 0 = 0$ for all $a \in \Gamma(R)$ is direct from definition.

v - For the distributive property, let $a, b, d \in \Gamma(R)$ and consider $x \in d(a + b)$. We need to prove that

$$x \in d \cdot a + d \cdot b. \tag{*}$$

It is the case if $0 \in \{a, b, d\}$ or if $b = -a$. Now suppose $a, b, d \neq 0$ with $b \neq -a$. Then there exist $y \in G(R)$ such that $x = dy$ and $y \in a + b$. Moreover, there exist some $z \in G(R)$ such that $y \cdot z = a \cdot b$ and $l_R(y)l_R(z) = l_R(a)l_R(b)$.

If $0 \in \{a, b, d\}$ or if $b = -a$ there is nothing to prove. Now suppose $a, b, d \neq 0$ with $b \neq -a$. Therefore $(dy) \cdot (dz) = (da) \cdot (db)$ and

$$\begin{aligned}
l_R(dy)l_R(dz) &= l_R(d)l_R(d) + l_R(d)l_R(z) + l_R(d)l_R(y) + l_R(y)l_R(z) \\
&= l_R(d)l_R(d) + l_R(d)[l_R(z) + l_R(y)] + l_R(y)l_R(z) \\
&= l_R(d)l_R(d) + l_R(d)l_R(yz) + l_R(y)l_R(z) \\
&= l_R(d)l_R(d) + l_R(d)l_R(ab) + l_R(a)l_R(b) \\
&= l_R(d)l_R(d) + l_R(d)l_R(a) + l_R(d)l_R(b) + l_R(a)l_R(b) \\
&= l_R(da)l_R(db),
\end{aligned}$$

so $l_R(dy)l_R(dz) = l_R(da)l_R(db)$. Hence we have $x = dy \in d \cdot a + d \cdot b$.

vi - Using distributivity we have that for all $a, b, c, d \in \Gamma(R)$

$$d[(a + b) + c] = (da + db) + dc \text{ and } d[a + (b + c)] = da + (db + dc).$$

In fact, if $x \in (a + b) + c$, then $x \in y + c$ for $y \in a + b$. Hence

$$dx \in dy + dc \subseteq d(a + b) + dc = (da + db) + dc.$$

Conversely, if $z \in (da + db) + dc$, then $z = w + dc$, for some $w \in da + db = d(a + b)$. But in this case, $w = dt$ for some $t \in a + b$. Then

$$z \in dt + dc = d[t + c] \subseteq d[(a + b) + c].$$

Similarly we prove that $d[a + (b + c)] = da + (db + dc)$.

vii - Let $a \in \Gamma(R)$ and $x, y \in 1 - a$. If $a = 0$ or $a = 1$ then we automatically have $x \cdot y \in 1 - a$, so let $a \neq 0$ and $a \neq 1$. Then $x, y \in G(R)$ and there exist $p, q \in \Gamma(R)$ such that

$$\begin{aligned}
x \cdot p = 1 \cdot a &\text{ and } l_R(x)l_R(p) = l_R(1)l_R(a) = 0 \\
y \cdot q = 1 \cdot a &\text{ and } l_R(y)l_R(q) = l_R(1)l_R(a) = 0.
\end{aligned}$$

Then $(xy) \cdot (pqa) = 1 \cdot a$ and

$$\begin{aligned} l_R(xy)l_R(pqa) &= l_R(xy)l_R(p) + l_R(xy)l_R(q) + l_R(xy)l_R(a) \\ &= l_R(y)l_R(p) + l_R(x)l_R(q) + l_R(x)l_R(a) + l_R(y)l_R(a) \\ &= l_R(y)l_R(pa) + l_R(x)l_R(qa) \\ &= l_R(y)l_R(x) + l_R(x)l_R(y) = 0. \end{aligned}$$

Then $xy \in 1-a$, proving that $(1-a)(1-a) \subseteq (1-a)$. In particular, since $1 \in 1-a$, we have $(1-a)(1-a) = (1-a)$.

viii - Finally, to prove associativity, we use Theorem 2.2.8. Let $\langle a,b\rangle \equiv \langle c,d\rangle$ the relation defined for $a,b,c,d \in \Gamma(R) \setminus \{0\}$ by

$$\langle a,b\rangle \equiv \langle c,d\rangle \text{ iff } ab = cd \text{ and } l_R(a)l_R(b) = l_R(c)l_R(d).$$

For $0 \notin \{a,b,c,d\}$, $a \neq -b$ and $ab = cd$, we have

$$a+b = c+d \text{ iff } \langle a,b\rangle \equiv \langle c,d\rangle.$$

Using items (i)-(vii) we get that $(\Gamma(R)\setminus\{0\}, \equiv, 1, -1)$ is a pre-special group. Then by Theorem 2.2.8 we have that $M(\Gamma(R) \setminus \{0\}) \cong \Gamma(R)$ is a pre-special hyperfield, and in particular, $(\Gamma(R)$ is associative.

□

Definition 5.5.3. *With the notations of Proposition 5.5.2 we have a functor $\Gamma : Igr_+ \to PSMF$ defined by the following rules: for $R \in Igr_+$, $\Gamma(R)$ is the special hyperfield obtained in Proposition 5.5.2 and for $f \in Igr_+(R,S)$, $\Gamma(f) : \Gamma(R) \to \Gamma(S)$ is the unique morphism such that the following diagram commute*

$$\begin{tikzcd} R \arrow[r, "e_R"] \arrow[d, "f_1"'] & \Gamma(R) \arrow[d, dotted, "\Gamma(f)"] \\ S \arrow[r, "e_S"'] & \Gamma(S) \end{tikzcd}$$

In other words, for $x \in R$ we have

$$\Gamma(f)(x) = (e_S \circ f_1 \circ l_R)(x) = e_S(f_1(l_R(x))).$$

psgadj

Theorem 5.5.4. *The functor $k : \mathcal{PSMF} \to Igr_+$ is the left adjoint of $\Gamma : Igr_+ \to \mathcal{PSMF}$. The unity of the adjoint is the natural transformation $\phi : 1_{\mathcal{PSMF}} \to \Gamma \circ k$ defined for $F \in \mathcal{PSMF}$ by $\phi_F = e_{k(F)} \circ \rho_F$.*

Proof. We show that for all $f \in \mathcal{PSMF}(F, \Gamma(R))$ there is an unique $f^\sharp : \mathrm{Igr}_+(k(F), R)$ such that $\Gamma(f^\sharp) \circ \phi_F = f$. Note that $\phi_F = e_{k(F)} \circ \rho_F$ is a group isomorphism (because $e_{k(F)}$ and ρ_F are group isomorphisms).

Let $f_0^\sharp : 1_{\mathbb{F}_2} : \mathbb{F}_2 \to \mathbb{F}_2$ and $f_1^\sharp := l_R \circ f \circ (\phi_F)^{-1} \circ e_{k(F)} : k_1(F) \to R_1$. For $n \geq 2$, define

$h_n : \prod_{i=1}^n k_1(F) \to R_n$ by the rule

$$h_n(\rho(a_1), ..., \rho(a_n)) := l_R(f(a_1)) * ... * l_R(f(a_n)).$$

We have that h_n is multilinear and by the Universal Property of tensor products we have an induced morphism $\bigotimes_{i=1}^n k_n(F) \to R_n$ defined on the generators by

$$h_n(\rho(a_1) \otimes ... \otimes \rho(a_n)) := l_R(f(a_1)) * ... * l_R(f(a_n)).$$

Now let $\eta \in Q_n(F)$. Suppose without loss of generalities that $\eta = \rho(a_1) \otimes ... \otimes \rho(a_n)$ with $a_1 \in 1 - a_2$. Then $f(a_1) \in 1 - f(a_2)$ which imply $l_R(f(a_1)) \in 1 - l_R(f(a_2))$. Since $R_n \in \mathrm{Igr}_+$,

$$h_n(\eta) := h_n(\rho(a_1) \otimes ... \otimes \rho(a_n)) = l_R(f(a_1)) * ... * l_R(f(a_n)) = 0 \in R_n.$$

Then h_n factors through Q_n, and we have an induced morphism $\overline{h}_n : k_n(F) \to R_n$. We set $f_n^\sharp := \overline{h}_n$. In other words, $f_n^\sharp$ is defined on the generators by

$$f_n^\sharp(\rho(a_1)...\rho(a_n)) := l_R(f(a_1)) * ... * l_R(f(a_n)).$$

Finally, we have

$$\begin{aligned}
\Gamma(f^\sharp) \circ \phi_F &= [e_R \circ (f_1^\sharp) \circ e_{k(F)}^{-1}] \circ [e_{k(F)} \circ \rho_F] = e_R \circ (f_1^\sharp) \circ \rho_F \\
&= e_R \circ [l_R \circ f \circ (\phi_F)^{-1} \circ e_{k(F)}] \circ \rho_F \\
&= f \circ (\phi_F)^{-1} \circ [e_{k(F)} \circ \rho_F] \\
&= f \circ (\phi_F)^{-1} \circ \phi_F = f.
\end{aligned}$$

For the unicity, let $u, v \in \mathrm{Igr}_+(k(F), R)$ such that $\Gamma(u) \circ \phi_F = \Gamma(v) \circ \phi_F$. Since ϕ_F is an isomorphism we have $u_1 = v_1$ and since $k(F) \in \mathrm{Igr}_+$ we have $u = v$. □

As we have already seen in Theorem 5.5.4, there natural transformation $\phi_F : F \to \Gamma(k(F))$ is a group isomorphism. Now let $a, c, d \in F$ with $a \in c + d$. Then $\phi_F(a) \in \phi_F(c) + \phi_F(d)$, i.e, ϕ_F is a morphism of hyperfields. In fact, if $0 \in \{a, c, d\}$ there is nothing to prove. Let $0 \notin \{a, c, d\}$. To prove that $\phi_F(a) \in \phi_F(c) + \phi_F(d)$ we need to show that $\rho_F(a)\rho_F(acd) = \rho_F(c)\rho_F(d)$. In fact, from $a \in c + d$ we get $ac \in 1 + ad$, and then $\rho_F(ac)\rho_F(ad) = 0$. Moreover

$$\begin{aligned}
\rho_F(a)\rho_F(acd) + \rho_F(c)\rho_F(d) &= \rho_F(a)\rho_F(acd) + \rho_F(c)\rho_F(d) + \rho_F(ac)\rho_F(ad) \\
&= \rho_F(a)\rho_F(ac) + \rho_F(a)\rho_F(d) + \rho_F(c)\rho_F(d) + \rho_F(ac)\rho_F(ad) \\
&= [\rho_F(a)\rho_F(ac) + \rho_F(ac)\rho_F(ad)] + [\rho_F(a)\rho_F(d) + \rho_F(c)\rho_F(d)] \\
&= \rho_F(d)\rho_F(ac) + \rho_F(d)\rho_F(ac) = 0,
\end{aligned}$$

proving that $\phi_F(a) \in \phi_F(c) + \phi_F(d)$. Unfortunately we do not now if or where ϕ_F is a strong morphism. Then we propose the following definition.

`kstable-def`

Definition 5.5.5 (The k stability)**.** *Let F be a pre-special hyperfield. We say that F is **k-stable** if $\phi_F : F \to \Gamma(F(G))$ is a full morphism. Alternatively, F is k-stable if for all $a, b, c, d \in \dot{F}$, if $ab = cd$ then*

$$\rho_F(a)\rho_f(b) = \rho_F(c)\rho_F(d) \textit{ imply } ac \in 1 + cd.$$

Proposition 5.5.6. *Every PSG G has a k-stable hull $G_{(k)}$ that satisfies the corresponding universal* *property . This is just given by*

$$G_{(k)} = \varinjlim_{n\in\mathbb{N}} (\Gamma \circ k)^n(G).$$

Thus the inclusion functor $PSG_{(k)} \hookrightarrow PSG$ has a left adjoint $(k) : PSG \to PSG_{(k)}$.

We emphasize that if G is $AP(3)$ special group, then G is k-stable. In particular, every reduced special group is k-stable, and if F is a field of characteristic not 2, then $G(F)$ is also k-stable.

In the next Chapter, it is established the Arason-Pfister Hauptsatz (Theorem 6.3.2) for **every special group** G, (i.e., G satisfies $AP(n)$ for each $n \in \mathbb{N}$.)

Proposition 5.5.7.

i - For each $G \in SG$, $\Gamma(s_G) : \Gamma(\mathcal{K}(G)) \to \Gamma(Grad(\mathcal{W}(G)))$ is a PSG-isomorphism.

ii - For each $G \in \mathcal{RSG}$, $\kappa_G : G \to \Gamma(\mathcal{K}(G))$ is a PSG-isomorphism.

iii - For each $G \in \mathcal{RSG}$, $\omega_G : G \to \Gamma(Grad(\mathcal{W}(G)))$ is a PSG-isomorphism.

Proposition 5.5.8. *Let G be a PSG. Are equivalent:*

i - $G \in \mathcal{PSG}_{fin}$.

ii - $\mathcal{K}(G) \in Igr_{fin}$.

Proposition 5.5.9. *Let G be a SG. Are equivalent:*

i - $G \in SG_{fin}$.

ii - $\mathcal{K}(G) \in Igr_{fin}$.

iii - $(Grad \circ \mathcal{W})(G) \in Igr_{fin}$.

Proposition 5.5.10. *The canonical arrow*

$$can : \varinjlim_{i\in I} \mathcal{K}(G_i) \to \mathcal{K}\left(\varinjlim_{i\in I} G_i\right)$$

is an Igr_+-isomorphism as long as the I-colimits above exists.

Proposition 5.5.11. *The canonical arrow*

$$can : \mathcal{K}\left(\varprojlim_{i\in I} G_i\right) \to \varprojlim_{i\in I} \mathcal{K}(G_i)$$

is an Igr_+-morphism pointwise surjective, as long as the I-colimits above exists.

Remark 5.5.12. *In [27] there is an interesting analysis identifying the boolean hull of a special group G (or special hyperfield $F = G \cup \{0\}$) with the boolean hull of the inductive graded rings $k_*(F), W_*(F) \in Igr_+$ (see the above Corollary 5.3.13). It could be interesting to compare the space of orderings of $R \in Igr_h$ and of $\Gamma(R) \in \mathcal{PSMF}$.*

5.6 Igr and Marshall's Conjecture

igrmarshall

Using the Boolean hull functor, M. Dickmann and F. Miraglia provide an encoding of Marshall's signature conjecture ([MC]) for reduced special groups by the condition

$$\langle 1,1\rangle \otimes - : I^n(G)/I^{n+1}(G) \to I^{n+1}(G)/I^{n+2}(G)$$

to be injective, for each $n \in \mathbb{N}$. In fact they introduce the notion of a [SMC] reduced special group:

$$l(-1) \otimes - : k_n(G) \to k_{n+1}(G)$$

is injective, for each $n \in \mathbb{N}$. They establish that, [SMC] imply [MC], for every reduced special group G. Moreover (see 5.1 and 5.4 in [30]):

- The inductive limit of [SMC] groups is [SMC].
- The finite product of [SMC] groups is [SMC].
- $G(F)$ is [SMC], for every Pythagorean field F (with $(char(F) \neq 2)$.

Proposition 5.6.1.

i - $s : k \to Grad \circ \mathcal{W}$ is a "surjective" natural transformation, where for each $G \in SG$ and all $n \geq 1$, $s_n(G) : K_n(G) \to I^n(G)/I^{n+1}(G)$ is given by the rule

$$s_n(G)\left(\sum_{i=0}^{s-1} l(g_{1,i}) \otimes ... \otimes l(g_{n,i}) + \mathcal{Q}_n(G)\right) := \overline{\bigotimes}_{i=0}^{s-1} [\langle 1, -g_{1,i}\rangle]\overline{\otimes}...\overline{\otimes}[\langle 1, -g_{n,i}\rangle]\overline{\otimes} I^{n+1}(G).$$

ii - $r : Grad \circ \mathcal{W} \to k$ is a natural transformation, where for each $G \in SG$ and all $n \geq 1$, $r^n_G : I^n(G)/I^{n+2}(G) \to k_{2n-1}(G)$ is given by the rule

$$r_n(G)\left(\overline{\bigotimes}_{i=0}^{s-1} [\langle 1, -g_{1,i}\rangle]\overline{\otimes}...\overline{\otimes}[\langle 1, -g_{n,i}\rangle]\overline{\otimes} I^{n+1}(G)\right) :=$$
$$\sum_{i=0}^{s-1} l(-1)^{2^{n-1}-n} l(g_{1,i}) \otimes ... \otimes l(g_{n,i}) + \mathcal{Q}_{2n-1}(G)$$

iii - For all $n \geq 1$, $r_n(G) \circ s_n(G) = l(-1)^{2^{n-1}-n}\overline{\otimes}\_$.

iv - We have an isomorphism of pointed $\mathbb{F}_2$-modules: $s^1_G : k_1(G) \xrightarrow{\cong} I^1(G)/I^2(G)$, $s^2_G : k_2(G) \xrightarrow{\cong} I^2(G)/I^3(G)$.

v - If G is [SMC] Then $s_G : k(G) \to Grad \circ \mathcal{W}(G)$ is an isomorphism.

We finish this chapter considering a general setting for "Marshall's conjectures", that includes the previous case of the Igr's $W_*(F), k_*(F)$ for special hyperfields F.

Let $R \in Igr_+$. The ideal, $nil(R)$, in the ring $\bigoplus_{n \in \mathbb{N}} R_n$, formed by all of its nilpotent elements, determines $N(R)$ a Igr-ideal of R, where $(N(R))_n := nil(R) \cap R_n$, $\forall n \in \mathbb{N}$. Note that, by Proposition 5.3.12, $(nil(R))_n = \{a \in R_n : \exists k \in \mathbb{N} \setminus \{0\}(\top_{kn} *_{kn,n} a = 0_{(k+1)n})\}$, $\forall n \in \mathbb{N}$.

Remark 5.6.2. *Let $\rho : \mathbb{N} \to \mathbb{N}$ be an increasing function and define $(N_\rho(R))_n = \{a \in R_n : \exists k \in \mathbb{N}(\top_{\rho(n)} *_{\rho(n),n} a = 0_{\rho(n)+n})\}$, $\forall n \in \mathbb{N}$. Then $(N_\rho(R))_n$ is a subgroup of R_n and, since $\rho(n+k) \geq \rho(n)$, we have $(N_\rho(R))_n *_{n,k} R_k \subseteq (N_\rho(R))_{n+k}$. Summing up, $((N_\rho(R))_n)_{n\in\mathbb{N}}$ is an Igr-ideal.*

The following result is straightforward consequence of the Definitions and 5.2.3, 5.3.13.

Proposition 5.6.3. *For each $R \in Igr_+$ are equivalent:*

i - For all $n \leq m \in \mathbb{N}$, $ker(h_{nm}) = \{0_n\} \in R_n$.

ii - The canonical morphism $R \to \mathbb{T}(\mathbb{A}(R))$ is pointwise injective.

iii - There exists a boolean ring B and a pointwise injective Igr-morphism $R \to \mathbb{T}(B)$.

Moreover, if $R \in Igr_{fin}$, these are equivalent to

iv - $N(R) \cong \mathbb{T}(0) \in Igr$.

Motivated by item (i), we use the abbreviation $MC(R)$ to say that R satisfies one (and hence all) of the above conditions.

In the following, we fix a category of L-structures $\mathcal{A}$ that is closed under directed inductive limits and a functor $F_* : \mathcal{A} \to Igr_+$ be a functor that preserves directed inductive limits. Examples of such kind of functors are $k_* : \mathcal{HMF} \to Igr_+$ and $W_* : \mathcal{HMF} \to Igr_+$, since such hyperfields can be conveniently described in the first-order relational language for multirings and it is closed under directed inductive limits. Related examples are the functors $k_* : SG \to Igr_+$ and $W_* : SG \to Igr_+$; note that SG is a full subcategory of $L_{SG} - Str$ that is closed under directed inductive limits **and** under arbitrary products.

Proposition 5.6.4. *If $(I, \leq)$ is an upward directed poset and $\Gamma : (I, \leq) \to \mathcal{A}$ is such that: $MC(F_*(\Gamma(i)))$, for all $i \in I$, then $MC(F_*(\varinjlim_{i\in I} \Gamma(i)))$.*

Proof. The hypothesis on F_* and the fact that the directed inductive limits in Igr_+ are pointwise, give us immediately that the mappings $h_n : F_n(\varinjlim_{i\in I} \Gamma(i)) \to F_{n+1}(\varinjlim_{i\in I} \Gamma(i))$ are isomorphic to the injective maps $\varinjlim_{i\in I} h_n^i : \varinjlim_{i\in I} F_n(\Gamma(i)) \to \varinjlim_{i\in I} F_{n+1}(\Gamma(i))$, for each $n \in \mathbb{N}$. Therefore it holds

$$MC(F_*(\varinjlim_{i\in I} \Gamma(i)))$$

. □

Corollary 5.6.5. *Let $F \subseteq P(I)$ be a filter and let $\{M_i : i \in I\}$ be a family of (non-empty) L-structures in $\mathcal{A}$. Suppose that $\mathcal{A}$ is closed under products and suppose that holds $MC(F_*(\prod_{i\in J} M_i))$, for each $J \in F$. Then holds $MC(F_*(\prod_{i\in J} M_i/F))$.*

Proof. This follows from the preceding result since, by a well-known model-theoretic result due to D. Ellerman ([34]), any reduced product of a family of (non-empty) L-structures, $\{M_i : i \in I\}$, module a filter $F \subseteq P(I)$, is canonically isomorphic to an upward directed inductive limit, $\varinjlim_{J\in F}(\prod_{i\in J} M_i) \cong (\prod_{i\in I} M_i)/F$. □

Proposition 5.6.6. *Let $F_* : \mathcal{A} \to Igr_+$ preserves pure embeddings. More precisely, if $M, M' \in \mathcal{A}$ and $j : M \to M'$ is a pure L-embedding, then $F_*(j) : F_*(M) \to F_*(M')$ is a pure morphism of Igr's (described in the first-order polysorted language for Igr's).*

Proof. This follows from the well known characterization result:

Fact: Let L' be a first-order language and $f : A \to B$ be an L'-homomorphism. Then are equivalent

- $f : A \to B$ is a pure L'-embedding.
- There exists an elementary L'-embedding $e : A \to C$ and a L'-homomorphism $h : B \to C$, such that $e = h \circ f$.
- There exists an ultrapower A^I/U and a L'-homomorphism $g : B \to A^I/U$, such that $\delta_A^{(I,U)} = g \circ f$, where $\delta_A^{(I,U)} : A \to A^I/U$ is the diagonal (elementary) L'-embedding.

Since the morphism $j : M \to M'$ is a pure embedding, by the Fact there exists an ultrapower M^I/U and a L-homomorphism $g : M' \to M^I/U$, such that $\delta^M_{(I,U)} = g \circ j$, where $\delta_M^{(I,U)} : M \to M^I/U$ is the diagonal (elementary) L-embedding.

Since we have a canonical isomorphism $can : \varinjlim_{J \in U} M^J \overset{\cong}{\to} M^I/U$, applying the functor F_*, we obtain $F_*(M^I/U) \cong F_*(\varinjlim_{J\in U} M^J) \cong \varinjlim_{J\in U} F^*(M^J) \to \varinjlim_{J\in U}(F^*(M))^J \cong (F_*(M))^I/U$.

Keeping track, we obtain that the above morphism $t : F_*(M^I/U) \to (F_*(M))^I/U$ establishes a comparison between $F_*(\delta^M_{(I,U)}) : F_*(M) \to F_*(M^I/U)$ and $\delta^{F_*(M)}_{(I,U)}) : F_*(M) \to F_*(M)^I/U$

$$\delta^{F_*(M)}_{(I,U)}) = t \circ F_*(\delta^M_{(I,U)}).$$

Since $F_*(\delta^M_{(I,U)}) = F_*(g) \circ F_*(j)$, combining the equations we obtain

$$\delta^{F_*(M)}_{(I,U)}) = t \circ F_*(g) \circ F_*(j).$$

Applying again the Fact, we conclude that $F_*(j) : F_*(M) \to F_*(M')$ is a pure morphism of Igr's. $\square$

Corollary 5.6.7. *For each $n \in \mathbb{N}$, the functor $F_n : \mathcal{A} \to p\mathbb{F}_2 - mod$ preserves pure embeddings. More precisely, if $M, M' \in \mathcal{A}$ and $j : M \to M'$ is a pure L-embedding, then $F_n(j) : F_n(M) \to k_n(M')$ is a pure morphism of pointed $\mathbb{F}_2$-modules (described in the first-order single sorted language adequate). In particular $F_n(j) : F_n(M) \to F_n(M')$ is an injective morphism of pointed $\mathbb{F}_2$-modules.*

Corollary 5.6.8. *Let $M, M' \in \mathcal{A}$ and $j : M \to M'$ is a pure L-embedding. If $MC(F_*(M'))$, then $MC(F_*(M))$.*

Proof. This follows directly from the previous Corollary. Indeed, suppose that holds $MC(F_*(M'))$. Since $h'_n : F_n(M') \to F_{n+1}(M')$ and $F_n(j) : F_n(M) \to F_n(M')$ are injective morphisms, then, by a diagram chase, $h_n : F_n(M) \to F_{n+1}(M)$ is an injective morphism too, thus holds $MC(F_*(M))$.

$$\begin{tikzcd}
F_nM \arrow[r, "h_n"] \arrow[d, "F_n(j)"'] & F_{n+1}M \arrow[d, "F_{n+1}(j)"] \\
F_n(M') \arrow[r, "h'_n"'] & F_{n+1}(M')
\end{tikzcd}$$

□

Chapter 6

Quadratic Extensions of Special Groups, Hauptsatz and Consequences

In this Chapter we develop the theory of quadratic extensions for hyperfields/superfields, through the development of results concerning the superrings of polynomials, envisaging some applications to algebraic theory of quadratic forms and Real Algebraic Geometry. The main results here are the Arason-Pfister Hauptsatz for **all** special groups (Theorem 6.3.2) and its consequences.

The use of hyperfields/hyperrings/multirings in connection with Real Algebraic Geometry started 15 years ago, in [47].

The significance of these multivalued methods - as addition of roots to a superfield (Theorem 3.5.4) and Marshall's quotient of a superring (Theorem 6.1.5)-to (univalent) Commutative Algebra is indicated by applying these results to algebraic theory of quadratic forms: (i) obtaining new relevant constructions in the category of special groups (or its equivalent category special hyperfields, as in Theorems 6.2.6, 6.2.12; (ii) extending to <u>all</u> special hyperfields the validity of the Arason-Pfister Hauptsatz (Theorem 6.3.2)- a positive answer ([7]) to a question posed by Milnor in a classical paper of 1970 ([52], [7])- and established by Dickmann-Miraglia to the realm of *reduced* special groups (or its equivalent category real reduced hyperfields) in 2000 ([28]); and applied that to obtain interesting properties of graded rings associated to special hyperfields ([30], [18]).

Throughout this Chapter, all superrings will be considered associative.

6.1 Marshall's Quotient of Superfields

quotient-section

In the realm of multirings, the notion of the so called "Marshall's quotient", introduced in [47] and further developed in [24], is a quotient multiring defined for pair (A, S) where A is a multiring and $S \subseteq A$ is a multiplicative subset: given $a, b \in A$,

$$a \approx_S b \text{ iff there are } x, y \in S \text{ such that } ax = by.$$

Now we introduce the following:

Definition 6.1.1. *Let A be a superring and $S \subseteq A$. The set S is called* ***Marshall's coherent*** *if it is multiplicative ($1 \in S$ and $S \cdot S \subseteq S$) and given $x, a \in A$ with $x \in as$ for some $s \in S$, there are $P, Q \subseteq S$ such that $xP = aQ$. We say that S is* ***nontrivial Marshall's coherent*** *if $0 \notin S$.*

Let A be a superring with $S \subseteq A$ Marshall's coherent. For $a, b \in A$, define

$$a \sim_S b \text{ iff there are non-empty subsets } X, Y \subseteq S \text{ with } aX = bY.$$

Fact 6.1.2. *If A is a multiring viewed as a superring, then every multiplicative subset $S \subseteq A$ is Marshall's coherent and the above quotient notion coincides with the original Marshall's quotient, i.e. $\approx_S = \sim_S$.*

Lemma 6.1.3.

i - For $a, b \in A$, the following are equivalent:

a) $a \sim b$.

b) There exists $s, t \in S$ such that $as \cap bt \neq \emptyset$.

c) There are $s, t, p, q \in S$ with $a(st) = b(pq)$.

ii - The relation $\sim$ is an equivalence relation.

Proof. we only need to deal with the case S nontrivial.

i - The implication $c) \Rightarrow a)$ is straightforward. For $a) \Rightarrow b)$, let $X, Y \subseteq S$ such that $aX = bY$. Then there are $s \in X$ and $t \in Y$ such that $as \cap bt \neq \emptyset$. On the other hand, for $b) \Rightarrow c)$, let $x \in as \cap bt$. Thus, by Marshall's coherence, there are $M, N, P, Q \subseteq S$ such that $xM = aP$ and $xN = bQ$. Therefore,
$$a(PN) = x(MN) = b(QM).$$

ii - Let $a, b, c \in A$.

- Since $a \cdot \{1\} = a \cdot \{1\}$ and $1 \in S$, we have $a \sim a$.
- If $a \sim b$, then $aX = bY$ for some $X, Y \subseteq S$. So $bY = aX$ and $b \sim a$.
- Let $a \sim b$ and $b \sim c$. Then $aX = bY$ and $bZ = cW$ for some $X, Y, Z, W \subseteq S$. Hence
$$a(XZ) = b(YZ) = c(WY)$$
and so $a \sim c$.

□

Now, let $A/_m S$ be the set of equivalence classes of $\sim$. We want to prescribe a superring structure for $A/_m S$.

For $a \in A$, let $[a]$ be the equivalence class of a in $A/_m S$. Define for $[a], [b] \in A/_m S$ the congruence relations:

$[c] \in [a] + [b]$ iff there exist $c', a', b' \in A$ with $c' \in a' + b'$ and $c' \sim c, a' \sim a, b' \sim b$.

$[c] \in [a][b]$ iff there exist $c', a', b' \in A$ with $c' \in a' \cdot b'$ and $c' \sim c, a' \sim a, b' \sim b$.

$[-a] := -[a]$.

lemsum1

Lemma 6.1.4. *Let A be a superring and $S \subseteq A$ a Marshall's coherent subset. Let $a, b, c \in A$.*

i - $[c] \in [a] + [b]$ iff there is $s \in S$ such that $cs \subseteq aS + bS$.

ii - $[c] \in [a] \cdot [b]$ iff there is $s \in S$ such that $cs \subseteq abS$.

Proof. we only need to deal with the case S nontrivial.

i - ($\Rightarrow$): Let $c', a', b' \in A$ such that $c' \in a' + b'$ and $c' \sim c, a' \sim a, b' \sim b$. Then

$$c'X' = cX, a'Y' = aY, b'Z' = bZ \text{ for some } X, Y, Z, X', Y', Z' \subseteq S$$

and so

$$c(XY'Z') = c'(X'Y'Z') \in a'(X'Y'Z') + b'(X'Y'Z') = a(X'YZ') + b(X'Y'Z) \subseteq aS + bS.$$

Therefore, for any $s \in XY'Z' \subseteq S$, we have $cs \subseteq aS + bS$.
($\Leftarrow$): By hypothesis, there is $c' \in cs \cap at + bv$ for some $t, v \in S$. Therefore there exists $a' \in at$ and $b' \in bv$ with $c' \in a' + b'$. Lastly, Marshall's coherence implies that $c' \sim c, a' \sim a$ and $b' \sim b$.

ii - ($\Rightarrow$): Let $c', a', b' \in A$ such that $c' \in a' \cdot b'$ and $c' \sim c, a' \sim a, b' \sim b$. Then

$$c'X' = cX, a'Y' = aY, b'Z' = bZ \text{ for some } X, Y, Z, X', Y', Z' \subseteq S$$

and so

$$c(XY'Z') = c'(X'Y'Z') \in a'(X'Y'Z')b'(X'Y'Z') = a(X'YZ')b(X'Y'Z) \subseteq bcS.$$

Therefore, for any $s \in XY'Z' \subseteq S$, we have $cs \subseteq abS$.

□

marshallquo-teo

Theorem 6.1.5. *Let A be a superring and $S \subseteq A$ a Marshall's coherent subset.*

i - The structure $(A/_m S, +, \cdot, -, [0], [1])$ is a superring.

ii - The projection map $\pi\colon A \to A/_m S$ is a universal morphism satisfying $\pi(S) = \{1\}$, that is, given a morphism $f\colon A \to B$ with $f(S) = \{1\}$, there is an unique morphism $\overline{f}\colon A/_m S \to B$ such that $f = \overline{f} \circ \pi$. In other words, for every morphism $f : A \to B$ such that $f[S] = \{1\}$, there exist a unique morphism $\tilde{f} : A/_m S \to B$ such that the following diagram commute:

$$\begin{tikzcd} A \arrow[r, "\pi"] \arrow[dr, "f"'] & A/_m S \arrow[d, "!\tilde{f}"] \\ & B \end{tikzcd}$$

where $\pi : A \to A/_m S$ is the canonical projection $\pi(a) = \overline{a}$.

Proof. we only need to deal with the case S nontrivial.

i - Firstly, we prove that $A/_m S$ is a superring.

- $(A/_m S, +, -, [0])$ is a multigroup.
The commutativity of $+$ is straightforward. Let $a, b, c \in A$.
  - $[c] \in [a] + [b] \Rightarrow -[a] \in -[b] + [c]$.
  Let $c', a', b' \in A$ with $c' \in a' + b'$ and $c' \sim c, a' \sim a, b' \sim b$. Then $-a' \in -c' + b'$ and so $-[a] \in -[b] + [c]$.

- $[a] + [0] = \{[a]\}$.
  Let $[x] \in [a] + [0]$. Then there is $s \in S$ such that $xs \subseteq aS$. So, by Marshall's coherence, $[x] = [a]$.
- $([a] + [b]) + [c] \subseteq [a] + ([b] + [c])$.
  Let $[x] \in [y] + [c]$, with $[y] \in [a] + [b]$. Then there are $s, t \in S$ such that $xs \subseteq yS + cS, yt \subseteq aS + bS$. Thus

$$xst \subseteq (aS + bS) + cS \subseteq aS + (bS + cS).$$

  It follows by Marshall's coherence that $[x] \in [a] + [l], [l] \in [b] + [c]$.

- $(A/_mS, \cdot, [1])$ is a multimonoid.
  The commutativity of $\cdot$ is straightforward too. So let $a, b, c \in A$.
  - $([a] \cdot [b]) \cdot [c] \subseteq [a] \cdot ([b] \cdot [c])$.
    Let $[x] \in [y] \cdot [c]$ with $[y] \in [a][b]$. Then there are $s, t \in S$ such that $xs \subseteq ycS, yt \subseteq abS$. Thus

$$xst \subseteq (ab)cS \subseteq a(bc)S$$

    and by Marshall's coherence $[x] \in [a][l], [l] \in [b][c]$.
  - $[a] \cdot [1] = \{[a]\}$.
    Let $[x] \in [a] \cdot [1]$. Then there is $s \in S$ with $xs \subseteq aS$. By Marshall's coherence $[x] = [a]$.

The verification of axioms iii, iv and v of Definition 3.1.1 are straightforward.

ii - It follows immediately from Marshall's quotient definition that $\pi\colon A \to A/_mS$ is a morphism satisfying $\pi(S) = \{1\}$. Now let $f\colon A \to B$ be a morphism with $f(S) = \{1\}$. Note that if $a \sim b$, then $as = bt$ for some $s, t \in S$ and so for any $x \in as \cap bt$ we have $f(x) \in f(as) \cap f(bt) \subseteq \{f(a)\} \cap \{f(b)\}$. Thus $f(a) = f(b)$. Then we can define $\overline{f}\colon A/_mS \to B$ by $\overline{f}([a]) = f(a)$. Since the multioperations are defined by congruence relations, we have that $\overline{f}$ is a superring morphism.

□

As an immediate consequence, note that if S, T are Marshall coherent subsets of A and $S \subseteq T$, then we have a canonical surjective morphism of superrings:

$$A/_mS \twoheadrightarrow A/_mT.$$

Corollary 6.1.6. *Let A be a superring and $S \subseteq A$ be a non-trivial Marshall coherent subset of A.*

i - If A is full then $A/_mS$ is full.

ii - If A is a superdomain then $A/_mS$ is a superdomain.

iii - If A is a superfield then $A/_mS$ is a superfield.

qext1

Theorem 6.1.7. *Let A be a superdomain and $S \subseteq A \setminus \{0\}$ such that $1 \in S$, $0 \notin S$, $S \cdot S \subseteq S$ and $A^2 \setminus \{0\} \subseteq S$. Then S is a Marshall coherent subset of S. Moreover $A/_mS$ is a hyperfield, i.e, for all $[a], [b] \in A/_mS$, $[a][b]$ is a singleton set.*

Proof. Let $a \in A$, $s \in S$ and $x \in as$. Suppose without loss of generality that $x \neq 0$ (because if $x = 0$ then $a = 0$ because A is a superdomain). Then $xa \subseteq a^2 s \subseteq S$ and since

$$x(xa) = ax^2 \text{ with } xa \text{ and } x^2 \text{ contained in } S,$$

we have that S is a Marshall coherent subset. Now let $[c], [d] \in [a].[b] \neq \emptyset$. Then $cs_1 \subseteq abS$ and $ds_2 \subseteq abS$ for some $s_1, s_2 \in S$ (see Lemma 6.1.4).

If $c = 0$ or $d = 0$ then $0 \in abS$ which imply $a = 0$ or $b = 0$ and $[a][b] = \{[0]\}$. Let $c, d \neq 0$. Then

$$cds_1s_2 \subseteq a^2b^2S \cdot S \subseteq S.$$

Using this fact we get

$$c(cds_1s_2) = d(c^2s_1s_2) \text{ with } cds_1s_2 \text{ and } c^2s_1s_2 \text{ contained in } S.$$

Moreover $c \sim d$, thus $[a].[b]$ is a singleton.

We already know that $A/_mS$ is a superdomain. To show that $A/_mS$ is a superfield, it suffices to note that for each $a \in A$ such that $[a] \neq [0]$, $[1] \in [a].[a]$, or, equivalently, there is $s \in S$ such that $1s \subseteq aS.aS$, but $a^2 \in S$ and $1.a^2 \subseteq (a.1).(a.1)$. Thus $A/_mS$ is superfield with single-valued products, i.e., $A/_mS$ is an hyperfield. □

From Theorem 6.1.7, we have many examples of Marshall coherent sets for superdomains A (of course, after removing zero):

- the squares
$$A^2 := \bigcup_{a \in A} a^2;$$
- the sum of squares
$$\sum A^2 := \bigcup_{a_1, \ldots, a_n \in A,\, n \in \mathbb{N}} a_1^2 + a_2^2 + \ldots + a_n^2;$$
- preorderings, that are subsets $T \subseteq A$ with $T + T \subseteq T$, $T \cdot T \subseteq T$ and $A^2 \subseteq T$.

6.2 Special Hyperfields and Quadratic Extensions

quadrapre-krasner

Theorem 6.2.1. *Let F be a hyperbolic hyperfield such that $1 + 1 = \{0, 1\}$ and $1 = -1$. Then $F \cong \{0, 1\}$ (the Krasner hyperfield). In particular, F is a DM-hyperfield.*

Proof. Just observe that
$$F = 1 - 1 = 1 + 1 = \{0, 1\}.$$
□

Throughout this section we establish the following notation: Let G be a formally real pre-special group and F its special multifield associated. In particular, if $\alpha \in F$, $\alpha \neq 0, 1$, the polynomial $f(X) \in F[X]$, $f(X) = X^2 - \alpha$ has no roots in F (basically because $\alpha^2 = 1$ for all $\alpha \in F^*$).

Then, let $\omega \in \overline{F}$, such that $0 \in f(\omega)$ (i.e, $0 \in \omega^2 - \alpha$) and $\mathrm{Irr}(F, \omega) = f$. Note that this imply

$\alpha = \omega^2$. Next, consider the superfield extension $F(\omega) = F(\mathrm{Irr}(F,\omega))$ and let

$$S_F(\omega) = (F(\omega))/_m(F(\omega)^2 \setminus \{0\})$$
$$S_F^{red}(\omega) = (F(\omega))/_m(\sum F(\omega)^2 \setminus \{0\})$$

We denote $\omega = \sqrt{\alpha}$.

prop1

Proposition 6.2.2. *Let F be a formally real special hyperfield and $S_F(\omega)$ as above.*

a - Let $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n \in F$. Then

$$(a_1 + b_1\omega)^2 + (a_2 + b_2\omega)^2 + ... + (a_n + b_n\omega)^2 \subseteq (1 + \alpha) + 2[a_1b_1 + a_2b_2 + ... + a_nb_n]\omega,$$

where $2X := X + X$.

b - $\sum F(\omega)^2 \setminus \{0\} = (1 + \alpha) + F \cdot \omega$.

c - Denote $(2)F = \bigcup\{x + x : x \in F\}$. Then

$$F(\omega)^2 = (1 + \alpha) + (2)F \cdot \omega.$$

d - $F(\omega)^2 = \sum F(\omega)^2$ iff $(2)F = F$.

e - $-1 \notin \sum F(\omega)^2$ iff $-1 \notin 1 + \alpha$.

f - $\omega \notin F(\omega)^2$.

g - The morphism $F \to S_F(\omega)$ is full and not injective.

h - If $-1 \notin 1+\alpha$ and $a, b \in a+b$ for all $a, b \in \dot{F}$ then $S_F(\omega)$ is a real reduced hyperfield (and then, a reduced special group).

Proof.

a - In fact, if $n = 2$, then

$$\begin{aligned}(a_1 + b_1\omega)^2 + (a_2 + b_2\omega)^2 &= a_1^2 + a_1b_1\omega + a_1b_1\omega + b_1^2\omega^2 + a_2^2 + a_2b_2\omega + a_2b_2\omega + b_2^2\omega^2 \\ &= 1 + [a_1b_1 + a_1b_1]\omega + \alpha + 1 + [a_2b_2 + a_2b_2]\omega + \alpha \\ &= [1 + \alpha + 1 + \alpha] + [a_1b_1 + a_1b_1 + a_2b_2 + a_2b_2]\omega \\ &\subseteq (1 + \alpha) + 2[a_1b_1 + a_2b_2]\omega.\end{aligned}$$

Here, we use the fact $1 + \alpha + 1 + \alpha = (1 + \alpha)(1 + \alpha) \subseteq 1 + \alpha$.

Now, suppose true for n and let $a_1, a_2, ..., a_n, a_{n+1}, b_1, b_2, ..., b_n, b_{n+1} \in F$.

$$\begin{aligned}&(a_1 + b_1\omega)^2 + (a_2 + b_2\omega)^2 + ... + (a_n + b_n\omega)^2 + (a_{n+1} + b_{n+1}\omega)^2 \\ &= [(a_1 + b_1\omega)^2 + (a_2 + b_2\omega)^2 + ... + (a_n + b_n\omega)^2] + (a_{n+1} + b_{n+1}\omega)^2 \\ &= (1 + \alpha) + 2[a_1b_1 + ... + a_nb_n]\omega + 1 + 2a_{n+1}b_{n+1}\omega + \alpha \\ &= (1 + \alpha) + 2[a_1b_1 + ... + a_nb_n + a_{n+1}b_{n+1}]\omega,\end{aligned}$$

as desired.

b - Using the previous item, we get

$$(1-\omega)^2+(1+\omega)^2=(1+\alpha)+2[1-1]\omega=(1+\alpha)+F\cdot\omega.$$

Moreover, $(1+\alpha)+F\cdot\omega\subseteq\sum S_F(\omega)^2\setminus\{0\}$, completing the proof.

c - Let $a,b\in F$. Then

$$(a+b\omega)^2=a^2+ab\omega+ab\omega+b^2\omega^2=(1+\alpha)+2ab\omega.$$

Then $F(\omega)^2\subseteq(1+\alpha)+(2)F\cdot\omega$. Conversely, let $t\in(1+\alpha)+(2)F\cdot\omega$. Then $t\in(1+\alpha)+2a\omega$ for some $a\in F$. Since

$$(1+\alpha)+2a\omega=(1+a\omega)^2,$$

we get $t\in(1+a\omega)^2\subseteq F(\omega)^2$, completing the proof.

d - Just use items (a), (b) and (c).

e - If $-1\in F(\omega)^2$, then $-1\in x+2z\omega$ for some $x\in 1+\alpha$ and $z\in F$. If $z=0$ then $-1=1+\alpha$, contradiction. If $z\neq 0$, then

$$0\in 1-1\subseteq 1+x+2z\omega\subseteq 1+1+\alpha+2z\omega.$$

Then $0\in y+z\omega$ for some $y\in 1+1+\alpha$, and then, $0\in ev(g(X),\omega)$, for $g(X)=y+zX$, contradicting the fact that $f(X)=X^2-\alpha=\mathrm{Irr}(F,\omega)$.

f - Just use the same argument of item (d).

g - Let $t\in a+b$ for some $t\in x+2y\omega$, with $y\neq 0$. Then

$$-b\in a-t\subseteq a-x-2y\omega,$$

and then,

$$0\in b-b\subseteq b+a-x-2y\omega.$$

Therefore exists some $d\in b+a-x$ such that $0\in d-2y\omega$, which imply that $0\in ev(g(X),\omega)$ for $g(X)=d-zX$ for some $z\in 2y$ with $z\neq 0$, contradiction. This morphism is not injective because if $a\in 1+\alpha$ then $[a]=[1]$ in $S_F(\omega)$.

h - If $a,b\in a+b$ for all $a,b\in\dot{F}$, then $(2)F=F$. Hence $F(\omega)^2=\sum F(\omega)^2$, which imply $S_F(\omega)$ real reduced $(1+1=\{1\})$.

$\square$

Remark 6.2.3. *It is not an easy task to find the description of $S_F(\omega)$ in the language/theory of special groups. Also, it is not clear if such description provides an advantage in terms of comprehension of the following results.*

If $\varphi=\langle a_1,...,a_n\rangle$ is a form on F, we denote the form $[\varphi]$ on $S_F(\omega)$ simply by $[\varphi]:=\langle[a_1],...,[a_n]\rangle$. We say that $[\varphi]$ **is the equivalence class of** φ **in** $S_F(\omega)$. Of course, if $\varphi=\varphi_1\oplus\varphi_2$ (or $\varphi=\varphi_1\otimes\varphi_2$) then $[\varphi]=[\varphi_1]\oplus[\varphi_2]$ (or $[\varphi]=[\varphi_1]\otimes[\varphi_2]$). We have the following useful consequences of Proposition 6.2.2 (which we will use freely):

Remark 6.2.4.

a - If $\varphi \equiv \psi$ on F then $[\varphi] \equiv [\psi]$ on $S_F(\omega)$;

b - if φ is isotropic on F then $[\varphi]$ is isotropic on $S_F(\omega)$;

c - if $[\varphi]$ is anisotropic on $S_F(\omega)$ then if φ is anisotropic on F.

Definition 6.2.5 (Rooted Superfield). *A superfield F is* ***rooted*** *if*

$$\{a, b\} \subseteq a + b \text{ for all } a, b \in F \setminus \{0\}.$$

teo150

Theorem 6.2.6. *Let F be a formally real pre-special hyperfield and $\omega \in \overline{F} \setminus F$ be a root of $f(X) = X^2 - \alpha \in F[X]$. Suppose that $-1 \notin 1 + \alpha$. Then $S_F(\omega)$ is a formally real pre-special hyperfield. Moreover if F is rooted then $S_F(\omega) = S_F^{red}(\omega)$, and in particular, $S_F(\omega)$ is a real reduced hyperfield.*

Proof. We already know (using Theorem 6.1.7 and item (e) of Proposition 6.2.2) that $S_F(\omega)$ is a formally real pre-special hyperfield. If F is rooted, then by item (h) of Proposition 6.2.2 we have the desired. □

exquad1

Example 6.2.7 (Quadratic Field Extensions and Quadratic Hyperfield Extensions). *Let F be a formally real field and $p \in F^*$ such that $x^2 - p$ has no roots in F. Consider $K = F(\sqrt{p})$. Of course, we have two special multifields (and special groups) $G(K) := K/_m(K^2)^*$ and $G_{red}(K) = K/_m(\sum K^2)^*$. Note that if $a + b\sqrt{p} \in \dot{K}$, then*

$$(a + b\sqrt{p})^2 = a^2 + pb^2 + 2ab\sqrt{p} \in D_F(\langle 1, p\rangle) + \sqrt{p} \cdot F,$$

where $D_F(\langle 1, p\rangle)$ is the usual set of representatives of the F-quadratic form $\langle 1, p\rangle$:

$$D_F(\langle 1, p\rangle) := \{x^2 + y^2 p : x, y \in \dot{F}\}.$$

In other words,

$$K^2 \setminus \{0\} \subseteq D_F(\langle 1, p\rangle) + \sqrt{p} \cdot F.$$

Moreover,

$$\begin{aligned}(a + b\sqrt{p})^2 + (c + d\sqrt{p})^2 &= (a^2 + pb^2 + 2pab\sqrt{p}) + (c^2 + pd^2 + 2cd\sqrt{p}) \\ &= (a^2 + pb^2 + c^2 + pd^2) + 2(ab + cd)\sqrt{p}.\end{aligned}$$

Using the fact that $D_F(\langle 1, p\rangle) \cdot D_F(\langle 1, p\rangle) \subseteq D_F(\langle 1, p\rangle)$ and for $a, b, c, d \neq 0$,

$$a^2 + pb^2 + c^2 + pd^2 \in D_F(\langle 1, p, 1, p\rangle) = D_F(\langle 1, p\rangle \otimes \langle 1, p\rangle) = D_F(\langle 1, p\rangle) \cdot D_F(\langle 1, p\rangle),$$

we conclude by induction (and a case analysis involving $0 \in \{a, b, c, d\}$) that

$$\sum K^2 \setminus \{0\} \subseteq D_F(\langle 1, p\rangle) + \sqrt{p} \cdot F.$$

So, let $Q_p := D_K(\langle 1, p\rangle) + \sqrt{p} \cdot F$. Then $Q_p \cdot Q_p$ is a multiplicative set containing $\sum K^2$. Define $G_{\sqrt{p}}(K) := K/_m Q_p$. Then $G_{\sqrt{p}}(K)$ is a reduced special group such that

$$G(K) \twoheadrightarrow G_{red}(K) \twoheadrightarrow G_{\sqrt{p}}(K). \qquad (*)$$

Moreover,

$$G_{\sqrt{p}}(K) \cong S_{K/_m(K^2)^*}(\sqrt{p}),$$

*i.e, the hyperfield of Theorem 6.2.6. We say that K is p-**special** if $G_{\sqrt{p}}(K) \cong G_{red}(K)$.*

exquad2

Example 6.2.8 (The Special Group of a quadratic extension)**.** *Let F be a formally real field and $p \in F^*$ such that $x^2 - p$ has no roots in F. Consider $K = F(\sqrt{p})$. Using the calculations of Example 6.2.7 we have*

$$\begin{aligned}\dot{K}^2 &= D_F(1,p) + \{x^2 + yb^2 + z\sqrt{p} : x, y \neq \dot{F} \text{ and } z = (x+y)^2 - (x^2+y^2)\} \\ &= \{x^2 + yb^2 + z\sqrt{p} : x, y \neq F \text{ are not both 0 and } z = (x+y)^2 - (x^2+y^2)\}.\end{aligned}$$

In this sense, for $a, b, c, d \in \dot{K}$, what means $\langle a, b\rangle \equiv_K \langle c, d\rangle$ in terms of the isometry relation on F?

By Lemma 1.5(a) of [28] we have

$$\langle a, b\rangle \equiv_K \langle c, d\rangle \text{ iff } ab = cd \text{ and } ac \in D_K(1, cd).$$

Lets first understand what means $\beta \in D_K(1,\alpha)$ for $\alpha, \beta \in \dot{K}$. By definition,

$$\beta \in D_K(1,\alpha) \text{ iff } \beta = x^2 + \alpha y^2,\ x, y \in \dot{K}.$$

Write $\alpha = \alpha_1 + \alpha_2\sqrt{p}$, $\beta = \beta_1 + \beta_2\sqrt{p}$, $x = x_1 + x_2\sqrt{p}$ and $y = y_1 + y_2\sqrt{p}$. Then

$$\begin{aligned}\beta &= x^2 + \alpha y^2 \Leftrightarrow \\ \beta_1 + \beta_2\sqrt{p} &= (x_1 + x_2\sqrt{p})^2 + (\alpha_1 + \alpha_2\sqrt{p})(y_1 + y_2\sqrt{p})^2 \Leftrightarrow \\ \beta_1 + \beta_2\sqrt{p} &= (x_1^2 + px_2^2 + 2x_1x_2\sqrt{p}) + (\alpha_1 + \alpha_2\sqrt{p})(y_1^2 + py_2^2 + 2y_1y_2\sqrt{p}) \Leftrightarrow \\ \beta_1 + \beta_2\sqrt{p} &= (x_1^2 + px_2^2 + \alpha_1y_1^2 + \alpha_1py_2^2 + 2p\alpha_2y_1y_2) + (2x_1x_2 + 2\alpha_1y_1y_2 + \alpha_2y_1^2 + \alpha_2py_2^2)\sqrt{p} \\ &\Leftrightarrow \begin{cases}\beta_1 = x_1^2 + px_2^2 + \alpha_1y_1^2 + \alpha_1py_2^2 + 2p\alpha_2y_1y_2 \\ \beta_2 = 2x_1x_2 + 2\alpha_1y_1y_2 + \alpha_2y_1^2 + \alpha_2py_2^2\end{cases} \\ &\Leftrightarrow \begin{cases}\beta_1 + \beta_2 = (x_1+x_2)^2 + (\alpha_1 + \alpha_2p)(y_1+y_2)^2 + (p-1)(x_2^2 + \alpha_1y_2^2 - \alpha_2y_1^2) \\ \beta_1 - \beta_2 = (x_1-x_2)^2 + (\alpha_1 - \alpha_2p)(y_1-y_2)^2 + (p-1)(x_2^2 + \alpha_1y_2^2 + \alpha_2y_1^2)\end{cases}\end{aligned}$$

Then

$$\beta = x^2 + ay^2 \Leftrightarrow \begin{cases}\beta_1 + \beta_2 = (x_1+x_2)^2 + (a_1 + a_2p)(y_1+y_2)^2 + (p-1)(x_2^2 + a_1y_2^2 - a_2y_1^2) \\ \beta_1 - \beta_2 = (x_1-x_2)^2 + (a_1 - a_2p)(y_1-y_2)^2 + (p-1)(x_2^2 + a_1y_2^2 + a_2y_1^2)\end{cases} \tag{6.1}$$

eqkrep1

For the discriminant part, let $a, b, c, d \in \dot{K}$ with $a = a_1 + a_2\sqrt{p}$, $b = b_1 + b_2\sqrt{p}$, $c = c_1 + c_2\sqrt{p}$

and $d = d_1 + d_2\sqrt{p}$ *for suitable* $a_i, b_i, c_i, d_i \in F$ $(i = 1, 2)$*. We have*

$$\begin{aligned}
ab = cd &\Leftrightarrow (a_1 + a_2\sqrt{p})(b_1 + b_2\sqrt{p}) = (c_1 + c_2\sqrt{p})(d_1 + d_2\sqrt{p}) \\
&\Leftrightarrow (a_1b_1 + pa_2b_2) + (a_1b_2 + a_2b_1)\sqrt{p} = (c_1d_1 + pc_2d_2) + (c_1d_2 + c_2d_1)\sqrt{p} \\
&\Leftrightarrow \begin{cases} a_1b_1 + pa_2b_2 = c_1d_1 + pc_2d_2 \\ a_1b_2 + a_2b_1 = c_1d_2 + c_2d_1 \end{cases} \\
&\Leftrightarrow \begin{cases} (a_1b_1 + pa_2b_2) + (a_1b_2 + a_2b_1) = (c_1d_1 + pc_2d_2) + (c_1d_2 + c_2d_1) \\ (a_1b_1 + pa_2b_2) - (a_1b_2 + a_2b_1) = (c_1d_1 + pc_2d_2) - (c_1d_2 + c_2d_1) \end{cases} \\
&\Leftrightarrow \begin{cases} (a_1 + a_2)(b_1 + b_2) + (p-1)a_2b_2 = (c_1 + c_2)(d_1 + d_2) + (p-1)c_2d_2 \\ (a_1 - a_2)(b_1 - b_2) + (p-1)a_2b_2 = (c_1 - c_2)(d_1 - d_2) + (p-1)c_2d_2 \end{cases}
\end{aligned}$$

Then

$$ab = cd \Leftrightarrow \begin{cases} (a_1 + a_2)(b_1 + b_2) + (p-1)a_2b_2 = (c_1 + c_2)(d_1 + d_2) + (p-1)c_2d_2 \\ (a_1 - a_2)(b_1 - b_2) + (p-1)a_2b_2 = (c_1 - c_2)(d_1 - d_2) + (p-1)c_2d_2 \end{cases} \qquad \text{eqkrep2} \quad (6.2)$$

Now, since $ac = (a_1c_1 + pa_2c_2) + (a_1c_2 + a_2c_1)\sqrt{p}$ *and* $ad = (a_1d_1 + pa_2d_2) + (a_1c_2 + a_2d_1)\sqrt{p}$*, using Equations 6.1 and 6.2 (with* $\beta = ac$ *and* $\alpha = ad$ *in Equation 6.1), we have the following characterization:*

$\langle a, b\rangle \equiv_K \langle c, d\rangle$ *if and only if there exists* $x_1, x_2, y_1, y_2 \in F$ *such that* $(x_1, x_2), (y_1, y_2) \neq (0, 0)$ *and*

$$\begin{cases}
(a_1 + a_2)(b_1 + b_2) + (p-1)a_2b_2 = (c_1 + c_2)(d_1 + d_2) + (p-1)c_2d_2 \\
(a_1 - a_2)(b_1 - b_2) + (p-1)a_2b_2 = (c_1 - c_2)(d_1 - d_2) + (p-1)c_2d_2 \\
(a_1 + a_2)(c_1 + c_2) + (p-1)a_2c_2 = (x_1 + x_2)^2 + [p(a_1 + a_2)(d_1 + d_2) - (p-1)a_1d_1](y_1 + y_2)^2 \\
\qquad\qquad + (p-1)[x_2^2 + (a_1d_1 + pa_2d_2)y_2^2 - (a_1c_2 + a_2d_1)y_1^2] \\
(a_1 - a_2)(c_1 - c_2) + (p-1)a_2c_2 = (x_1 - x_2)^2 + [p(a_1 - a_2)(d_1 - d_2) - (p-1)a_1d_1](y_1 - y_2)^2 \\
\qquad\qquad + (p-1)[x_2^2 + (a_1d_1 + pa_2d_2)y_2^2 + (a_1c_2 + a_2d_1)y_1^2]
\end{cases}$$

Manipulating Equation 6.2 we get a very similar system to describe when $\overline{a} = \overline{b}$ *in* $K/_m\dot{K}^2$*,* $a, b \in K$*.*

In the sequel, we want to iterate de construction $S_F(\omega)$. Let $\alpha, \beta \in \dot{F} \setminus \{-1\}$. The properties of Proposition 6.2.2 are valid if we change F by $S_F(\sqrt{\alpha})(\sqrt{\beta})$ (or $S_F(\sqrt{\beta})(\sqrt{\alpha})$).

sext1

Theorem 6.2.9. *Let* F *be a special hyperfield and* $\alpha, \beta \in \dot{F} \setminus \{\pm 1\}$*. Then*

$$S_{S_F(\sqrt{\alpha})}(\sqrt{\beta}) \cong S_{S_F(\sqrt{\beta})}(\sqrt{\alpha}).$$

Proof. We already know that

$$F(\sqrt{\alpha})(\sqrt{\beta}) \cong F(\sqrt{\beta})(\sqrt{\alpha})$$

and

$$F(\sqrt{\alpha})(\sqrt{\beta}) = F + F\sqrt{\alpha} + F\sqrt{\beta} + F\sqrt{\alpha}\sqrt{\beta}.$$

Let $\varphi : F(\sqrt{\alpha})(\sqrt{\beta}) \to F(\sqrt{\beta})(\sqrt{\alpha})$ be an isomorphism and denote $q_1 : F(\sqrt{\alpha})(\sqrt{\beta}) \to S_F(\sqrt{\alpha})(\sqrt{\beta})$ and $q_2 : F(\sqrt{\beta})(\sqrt{\alpha}) \to S_F(\sqrt{\beta})(\sqrt{\alpha})$ the natural projections. For instance, q_1 is given by the rule

$$q_1(a_0 + a_1\sqrt{\alpha} + a_2\sqrt{\beta} + a_3\sqrt{\alpha}\sqrt{\beta}) := [a_0 + a_1\sqrt{\alpha}] + [a_2 + a_3\sqrt{\alpha}]\sqrt{\beta} \in S_F(\sqrt{\alpha})(\sqrt{\beta}).$$

Similarly for q_2.

Now, let $\pi_1 : S_F(\sqrt{\alpha})(\sqrt{\beta}) \to S_{S_F(\sqrt{\alpha})}(\sqrt{\beta})$ and $\pi_2 : S_F(\sqrt{\beta})(\sqrt{\alpha}) \to S_{S_F(\sqrt{\beta})}(\sqrt{\alpha})$ be the quotient morphisms. Since $\varphi[F(\sqrt{\alpha})(\sqrt{\beta})^2] = F(\sqrt{\beta})(\sqrt{\alpha})^2$ and $q_2[F(\sqrt{\beta})(\sqrt{\alpha})^2] \subseteq (S_F(\sqrt{\beta})(\sqrt{\alpha}))^2$, we have that $\pi_2 \circ q_2 \circ \varphi : F(\sqrt{\alpha})(\sqrt{\beta}) \to S_{S_F(\sqrt{\beta})}(\sqrt{\alpha})$ is a morphism such that

$$\pi_2 \circ q_2 \circ \varphi[F(\sqrt{\alpha})(\sqrt{\beta})] = \{1\}.$$

By the universal property there is an unique morphism $\varphi_{\alpha\beta} : S_{S_F(\sqrt{\alpha})}(\sqrt{\beta}) \to S_{S_F(\sqrt{\beta})}(\sqrt{\alpha})$. Using the same argument, there is an unique morphism $\varphi_{\beta\alpha} : S_{S_F(\sqrt{\beta})}(\sqrt{\alpha}) \to S_{S_F(\sqrt{\alpha})}(\sqrt{\beta})$. The universal property forces $\varphi_{\alpha\beta} \circ \varphi_{\beta\alpha} = id$ and $\varphi_{\beta\alpha} \circ \varphi_{\alpha\beta} = id$. □

With Theorem 6.2.9 we are able to properly iterate the construction $S_F(\omega)$. For $a_1, ..., a_n \in \dot{F}$, we define recursively:

$$S_{F(\sqrt{a_1},\sqrt{a_2})} := S_{S_F(\sqrt{a_1})}(\sqrt{a_2});$$
$$S_{F(\sqrt{a_1},...,\sqrt{a_{n+1}})} := S_{S_F(\sqrt{a_1},...,\sqrt{a_n})}(\sqrt{a_{n+1}}).$$

cor333

Corollary 6.2.10. *Let F be a special hyperfield, $\alpha_1, \alpha_2, ..., \alpha_n \in \dot{F}$, and $\sigma \in S_n$. Then*

$$S_{F(\sqrt{a_1},...,\sqrt{a_n})} \cong S_{F(\sqrt{a_{\sigma(1)}},...,\sqrt{a_{\sigma(n)}})}.$$

It is important to comprehend the distinction between $S_{F(\sqrt{a_1},...,\sqrt{a_n})}(\sqrt{a_{n+1}})$ and $S_{F(\sqrt{a_1},...,\sqrt{a_{n+1}})}$: $S_{F(\sqrt{a_1},...,\sqrt{a_n})}(\sqrt{a_{n+1}})$ is an algebraic extension of $S_{F(\sqrt{a_1},...,\sqrt{a_n})}$ from which $\sqrt{a_{n+1}}$ is algebraic. On the other hand,

$$S_{F(\sqrt{a_1},...,\sqrt{a_{n+1}})} := S_{F(\sqrt{a_1},...,\sqrt{a_n})}(\sqrt{a_{n+1}})/_m((S_{F(\sqrt{a_1},...,\sqrt{a_n})}(\sqrt{a_{n+1}}))^2 \setminus \{0\}).$$

We want to describe the isometry relation $\equiv_{S_F(\omega)}$ in $S_F(\omega)$ in terms of isometry relation $\equiv_F$ in F. We begin this investigation with some general results.

iso0

Theorem 6.2.11. *Let $a, b \in F$. Then $[a] = [b]$ in $S_F(\omega)$ iff there is $s, t \in 1 + \alpha$ with $as = bt$ (or $a = bst$).*

Proof. ($\Rightarrow$) Suppose that $[a] = [b]$ in $S_F(\omega)$. Then there exist $X, Y \subseteq F(\omega)^2 \setminus \{0\}$ with $aX = bY$. Let $r_1 + s_1\omega \in X$, with $r \in 1 + \alpha$. Then

$$a(r_1 + s_1\omega) = ar_1 + as_1\omega \in bY,$$

and there exist $r_2 + s_2\omega \in Y$ with

$$\emptyset \neq (ar_1 + as_1\omega) \cap (b(r_2 + s_2\omega)).$$

But $b(r_2 + s_2\omega) = \{br_2 + bs_2\omega\}$. Then $ar_1 + as_1\omega = br_2 + bs_2\omega$, which imply $ar_1 = br_2$ and $as_1 = bs_2$.

($\Leftarrow$) Immediate since $1 + \alpha \subseteq F(\omega)^2 \setminus \{0\}$. □

teo32

Theorem 6.2.12. *Let $a, b \in F$. Then $[a] = [b]$ in $S_{F(\sqrt{a_1},...,\sqrt{a_n})}$ iff there is $s, t \in D_F(\langle\langle \alpha_1, \alpha_2, ..., \alpha_n \rangle\rangle)$* [1] *such that $as = bt$ (or $a = bst$ or even $ab \in D_F(\langle\langle \alpha_1, \alpha_2, ..., \alpha_n \rangle\rangle)$).*

[1] Here $\langle\langle \alpha_1, \alpha_2, ..., \alpha_n \rangle\rangle$ denotes the Pfister form $\langle 1, \alpha_1 \rangle \otimes \langle 1, \alpha_2 \rangle \otimes ... \otimes \langle 1, \alpha_n \rangle$.

Proof. Since $S_{F(\sqrt{a_1},...,\sqrt{a_n})}$ is a real reduced hyperfield and in $S_{F(\sqrt{a_1},...,\sqrt{a_n})}$, $\{[\alpha_1],...,[\alpha_n]\}=\{[1]\}$ we only need to prove $(\Rightarrow)$.

Let $a,b\in F$. If $[a]=[b]$ in $S_{F(\sqrt{\alpha_1},\sqrt{\alpha_2})}=S_{S_{F(\sqrt{\alpha_1})}}(\sqrt{\alpha_2})$, then by Theorem 6.2.11 (changing F by $S_{F(\sqrt{\alpha_1})}$) we have $[ab]\in[1]+[\alpha_2]$ (in $S_{F(\sqrt{\alpha_1})}$). Then there exist $s\in 1+\alpha_1$ such that

$$abs\in(1+\alpha_1)+\alpha_2(1+\alpha_1)=D_F(\langle 1,\alpha_1,\alpha_2,\alpha_1\alpha_2\rangle)=D_F(\langle\langle\alpha_1,\alpha_2\rangle\rangle).$$

This means $abs\in D_F(\langle\langle\alpha_1,\alpha_2\rangle\rangle)$.

Now suppose the desired valid for n. By induction hypothesis $[a]=[b]$ in

$$S_{F(\sqrt{a_1},...,\sqrt{a_{n+1}})}\cong S_{(S_F(\sqrt{a_1}))(\sqrt{a_2},...,\sqrt{a_{n+1}})}{}^{2}$$

iff

$$[ab]\in D_{S_F(\sqrt{a_1})}(\langle\langle[\alpha_2],[\alpha_2],...,[\alpha_n]\rangle\rangle).$$

This imply

$$ab\in D_F(\langle\langle\alpha_2,\alpha_2,...,\alpha_n\rangle\rangle)\cdot(1+\alpha_1)\subseteq D_F(\langle\langle\alpha_1,\alpha_2,...,\alpha_{n+1}\rangle\rangle).$$

□

cor33

Corollary 6.2.13. *Let F be a special hyperfield and $\alpha_1,\alpha_2,...,\alpha_n\in\dot F\setminus\{\pm1\}$. Then $S_{F(\sqrt{a_1},...,\sqrt{a_n})}$ is formally real iff $-1\notin D_F(\langle\langle\alpha_1,\alpha_2,...,\alpha_n\rangle\rangle)$.*

Proof. Since $S_{F(\sqrt{a_1},...,\sqrt{a_n})}$ is a real reduced hyperfield, we have $S_{F(\sqrt{a_1},...,\sqrt{a_n})}$ formally real iff $[1]\neq[-1]$, which by Theorem 6.2.12 occurs iff $-1\notin D(\langle\langle\alpha_1,\alpha_2,...,\alpha_n\rangle\rangle)$. □

iso2

Theorem 6.2.14. *Let $a,b,c,d\in\dot F$. Then $\langle[a],[b]\rangle\equiv_{S_F(\omega)}\langle[c],[d]\rangle$ iff $\langle ar,bs\rangle\equiv_F\langle c,dt\rangle$ for some $r,s,t\in 1+\alpha$.*

Proof. $(\Rightarrow)$ Let $\langle[a],[b]\rangle\equiv_{S_F(\omega)}\langle[c],[d]\rangle$. Then $[a][b]=[c][d]$ and $[a][c]\in 1+[c][d]$. Hence, there are $v,w\in 1+\alpha$ and $x\in S=F(\omega)^2\setminus\{0\}$ with $abv=cdw$ (or $abvw=cd$) and $acx\in S+cdS$. Write $x=x_1+x_2\omega$. We have

$$avwcx_1x\in vx_1(S+cdS)\subseteq vx_1S+cdvx_1S\subseteq S+cdS.$$

Then

$$avwcx_1(x_1+x_2\omega)\in(y_1+y_2\omega)+cd(z_1+z_2\omega)$$

for some $y_1,z_1\in 1+\alpha$ and $y_2,z_2\in F$. This means

$$avwc+avwcx_1x_2\omega\in(y_1+cdz_1)+(y_2+cdz_2)\omega,$$

and then, $avwc\in y_1+cdz_1$ and $avwcx_1x_2\in y_2+cdz_2$. Then $avwcy_1\in 1+cdy_1z_1$ or equivalently, $(avwy_1)c\in 1+c(dy_1z_1)$. Therefore $(avwy_1)(bz_1)=c(dy_1z_1)$ with $(avwy_1)c\in 1+c(dy_1z_1)$, which means $\langle avwy_1,bz_1\rangle\equiv_F\langle c,dy_1z_1\rangle$. Putting $r=vwy_1$, $s=z_1$ and $t=y_1z_1$ we get the desired.

$(\Leftarrow)$ Immediate. □

Then for all $a,b,c,d\in\dot F$ are equivalent:

i- $\langle[a],[b]\rangle\equiv_{S_F(\omega)}\langle[c],[d]\rangle$;

ii- $\langle ar,bs\rangle\equiv_F\langle ct,d\rangle$ for some $r,s,t\in 1+\alpha$.

[2]We are doing a convenient use of Corollary 6.2.10.

iii- $\langle ar, bs\rangle \equiv_F \langle c, dt\rangle$ for some $r, s, t \in 1+\alpha$.

iv- $\langle a, br\rangle \equiv_F \langle cs, dt\rangle$ for some $r, s, t \in 1+\alpha$.

v- $\langle ar, b\rangle \equiv_F \langle cs, dt\rangle$ for some $r, s, t \in 1+\alpha$.

6.3 Expanding the Arason-Pfister Hauptsatz and consequences

Hauptsatz-section

As an application of the former developed results, we reserve this section to expand one of the more emblematic questions/results in algebraic theory of quadratic forms: the so-called Arason Pfister Hauptsatz (APH).

In the sequel we present a brief historic of APH.

In [52], a 1970 paper of John Milnor seminal to the algebraic theory of quadratic forms over fields, the author poses two questions concerning the class of fields of characteristic $\neq 2$ (positively solved in the paper in many instances). One of the question was concerning the so called "Milnor's conjectures for the graded cohomology ring and for the graded Witt ring" that Voevodsky et al. solved around 2000. The other question asked if for every such field F, the intersection $\bigcap_{n\in\mathbb{N}} I^n(F)$ contains only $0 \in W(F)$, where $I^n(F)$ is the n-th power of the fundamental ideal $I(F)$ of the Witt ring of F ($I(F) = \{$even dimensional anisotropic forms over $F\}$).

In the subsequent year, J. Arason and A. Pfister solved this question as an immediate corollary of the nowadays called "Arason-Pfister Hauptsatz" (APH):

([7])*Let $\phi \neq \emptyset$ be an anisotropic form. If $\phi \in I^n(F)$, then $dim(\phi) \geq 2^n$.*

The theory of special groups, an abstract (first-order) theory of quadratic forms developed by Dickmann-Miraglia since the middle of the 1990s, allows a functorial encoding of the algebraic theory of quadratic forms of fields (with char $\neq 2$). In [28], Dickmann-Miraglia, restated the APH to the setting of special groups and, employing boolean theoretic methods to define and calculate the Stiefel-Whitney and the Horn-Tarski invariants of a special group, establish a generalization of the APH to the setting of **reduced** special groups, in particular proving a different proof of the APH for formally real pythagorian fields.

Now, as an application of the previous developed constructions of quadratic extensions in the category of hyperfields, we expand the validity of the Arason-Pfister Hauptsatz for all special hyperfields.

We start establishing the following:

Notations:

- Let G be a special group and $F = G\dot{\cup}\{0\}$ its special hyperfield associated. In particular, if $\alpha \in F$, $\alpha \neq 0, 1$, the polynomial $f(X) \in F[X]$, $f(X) = X^2 - \alpha$ has no roots in F (basically because $\alpha^2 = 1$ for all $\alpha \in F^*$).

- Let φ, ψ be forms on a special hyperfield F. We say that φ and ψ are Witt equivalent, notation $\varphi \approx_{W,F} \psi$ iff there exist non negative integers k, l such that $k\langle 1, -1\rangle \oplus \varphi \equiv_F l\langle 1, -1\rangle \oplus \psi$. By Witt's Decomposition, if φ is a form on F, there are unique forms $\varphi_{an}, \varphi_{hip}, \varphi_0$ (up to isometry) with $\varphi \equiv \varphi_{an} \oplus \varphi_{hip} \oplus \varphi_0$, φ_{an} anisotropic, φ_{hip} hyperbolic and φ_0 totally isotropic. We define $\dim_{W,F}(\varphi) := \dim(\varphi_{an})$.

- Let F be a special hyperfield. For each $n \in \mathbb{N}$ consider the statement:
  $AP_F(n)$ For each $\varphi = \langle a_1, \cdots, a_k\rangle$, a non-empty ($k \geq 1$), regular ($a_i \in \dot{F}$) and anisotropic form, if $\varphi \in I^n(F)$, then $\dim(\varphi) \geq 2^n$.

Remark 6.3.1. *Let G be an special group. Recall that (see [28]):*

a - A Pfister form of degree $n \geq 1$, with coefficients $a_1, \cdots, a_n \in G$ is $\langle\langle a_1, \cdots, a_n\rangle\rangle = \otimes_{i=1}^{n}\langle 1, a_i\rangle$.

b - Let ψ be a Pfister form. Then ψ is hyperbolic iff it is isotropic. Moreover, if G is reduced and $-1 \in D_G(\psi)$, then ψ is hyperbolic.

c - $I^n(G) \subseteq W(G)$ is additively generated by the Pfister forms of degree n.

d - If $\varphi \in I^n(G) \setminus \{\emptyset\}$, then $\varphi = \varepsilon_1\varphi_1 + ... + \varepsilon_r\varphi_r$, where $r \geq 1$ and $\varepsilon_j = \pm 1$ for all $j = 1, ..., r$. Moreover, if φ is anisotropic, we suppose without loss of generality that $\varepsilon_j = 1$ for all $j = 1, ..., r$.

haup

Theorem 6.3.2 (Arason-Pfister Hauptsatz)**.** *Let F be a special hyperfield, then it holds $AP_F(n)$, for all $n \geq 0$. In more details: for each $n \geq 0$ and For each $\varphi = \langle a_1, \cdots, a_k\rangle$, a non-empty ($k \geq 1$), regular ($a_i \in \dot{F}$) and anisotropic form, if $\varphi \in I^n(F)$, then $\dim(\varphi) \geq 2^n$ $\varphi \in I^n(F)$, if $\varphi \neq \emptyset$ is anisotropic, then $\dim_{W,F}(\varphi) \geq 2^n$.*

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

Since φ is an anisotropic form such that $\varphi \in I^nF \setminus \{\emptyset\}$ and I^nF is additively generated by the Pfister forms, then there exists $r \geq 1$ and Pfister forms of degree n, $\varphi_1, \cdots \varphi_r$ such that $\varphi = \pm(\varphi_1 + ... + \varphi_r)$.

Since φ is anisotropic, we can suppose without loss of generality that $\varphi = \varphi_1 + ... + \varphi_r$ and proceed by induction on r.

If $r = 1$, then $\varphi = \varphi_1$, with $\dim(\varphi) = \dim(\varphi_1) = 2^n$.

Let $r \geq 2$. If φ_j is isotropic for all $j = 1, ..., r$ then φ is isotropic (hyperbolic, in fact): this fallows from Witt's cancellation law since $\varphi \oplus k\langle 1, -1\rangle \equiv (r2^{n-1} + m)\langle 1, -1\rangle$. So we can suppose without loss of generality that $\varphi_1 = \langle\langle a_1, ..., a_n\rangle\rangle$ is anisotropic.

Suppose $-1 \notin D_F(\varphi_1)$. By Corollary 6.2.13 Let $S_F(\varphi_1) := S_{F(\sqrt{a_1}, ..., \sqrt{a_n})}$. Then equivalence class of φ on $S_F(\varphi_1)$ is

$$[\varphi] = [\varphi_1 + ... + \varphi_r] = [\varphi_1] + ... + [\varphi_r] = 2^n\langle 1\rangle + [\varphi_2] + ... + [\varphi_r].$$

We already know that $\dim_{W,F}(\varphi) \geq \dim_{W,S_F(\varphi_1)}[\varphi]$. Then we have three cases:

I - $[\varphi]$ is hyperbolic. Then $([\varphi_2] + ... + [\varphi_r])_{an} \equiv_{S_F(\varphi_1)} 2^n\langle -1\rangle$. Then

$$\dim_{W,F}(\varphi) \geq \dim_{W,F}(\varphi_2 + ... + \varphi_r) \geq \dim_{W,F}(\varphi_2 + ... + \varphi_r)_{an} \geq \dim_{W,F}([\varphi_2] + ... + [\varphi_r])_{an} = 2^n.$$

II - $[\varphi]$ is not hyperbolic and $[\varphi_2] + ... + [\varphi_r]$ is anisotropic. Then $\varphi_2 + ... + \varphi_r$ is anisotropic. By induction hypothesis we have $\dim_{W,F}(\varphi_2 + ... + \varphi_r) \geq 2^n$. Then

$$\dim_{W,F}(\varphi) \geq \dim_{W,F}(\varphi_2 + ... + \varphi_r) \geq 2^n.$$

III - $[\varphi]$ is not hyperbolic and $[\varphi_2] + ... + [\varphi_r]$ is isotropic.

Since $[\varphi]$ is not hyperbolic, we can assume that $[\varphi_2]$ is anisotropic (otherwise, if $[\varphi_j]$ is isotropic for all $j = 2, ..., r$ then $[\varphi]$ is an isotropic Pfister form and then, is also hyperbolic). Denote $F_1 := S_F(\varphi_1)$. In $S_{F_1}([\varphi_2])$ (which is a special hyperfield) look at

$$\psi_2 := [[\varphi_2] + ... + [\varphi_r]] = 2^n\langle 1\rangle + [\varphi_3] + ... + [\varphi_r] \in S_{F_1}([\varphi_2]).$$

For $\psi_2 \in I^n(S_{F_1}([\varphi_2]))$ we have

$$\dim_{W,F}(\varphi) \geq \dim_{W,S_F(\varphi_1)}[\varphi] \geq \dim_{W,S_{F_1}([\varphi_2])}[\psi_2]$$

and the same cases I, II and III for ψ_2. Suppose without loss of generality that we are in case III, i.e, that $[\varphi_3] + ... + [\varphi_r]$ is isotropic in $S_{F_1}([\varphi_2])$. If $[\varphi_j]$ is isotropic in $S_{F_1}([\varphi_2])$ for all $j \geq 3$, then we are in case I. Now suppose $[\varphi_3]$ anisotropic in $S_{F_1}([\varphi_2])$ and denote $F_2 := S_{F_1}([\varphi_2])$. In $S_{F_2}([\varphi_3])$ (which is a special hyperfield) look at

$$\psi_3 := [[\varphi_3] + ... + [\varphi_r]] = 2^n\langle 1\rangle + [\varphi_4]... + [\varphi_r] \in S_{F_2}([\varphi_3]).$$

For $\psi_3 \in I^n(S_{F_2}([\varphi_3]))$ we have

$$\dim_{W,F}(\varphi) \geq \dim_{W,S_F(\varphi_1)}[\varphi] \geq \dim_{W,S_{F_1}([\varphi_2])}[\psi_2] \geq \dim_{W,S_{F_2}([\varphi_3])}[\psi_3].$$

and the same cases I, II and III for ψ_3. Repeating this process more $r-3$ times, we get at $[\varphi_r]$ in $S_{F_{r-1}}([\varphi_{r-1}])$ and

$$\begin{aligned}\dim_{W,F}(\varphi) &\geq \dim_{W,S_F(\varphi_1)}[\varphi] \geq \dim_{W,S_{F_1}([\varphi_2])}[\psi_2] \\ &\geq \dim_{W,S_{F_2}([\varphi_3])}[\psi_3] \geq ... \geq \dim_{W,S_{F_{r-2}}([\varphi_{r-2}])}[\psi_{r-1}].\end{aligned}$$

Now, if $[\varphi_r]$ is isotropic in $S_{F_{r-1}}([\varphi_{r-1}])$ then $[\varphi_r]$ is hyperbolic in $S_{F_{r-1}}([\varphi_{r-1}])$, which by case I imply $\dim_{W,S_{F_{r-2}}([\varphi_{r-2}])}[\psi_{r-1}] \geq 2^n$. If $[\varphi_r]$ is anisotropic in $S_{F_{r-1}}([\varphi_{r-1}])$ we are in case II and also $\dim_{W,S_{F_{r-2}}([\varphi_{r-2}])}[\psi_{r-1}] \geq 2^n$.

Now suppose $-1 \in D_F(\varphi)$. Then $S_F(\varphi_1) \cong \{0,1\}$ (see Theorem 6.2.1), which imply $[\varphi]$ is hyperbolic, enabling us to use the very an adapted version argument in Case (I) above: the equivalence class of φ on $S_F(\varphi_1)$ still is given by

$$[\varphi] = [\varphi_1 + ... + \varphi_r] = [\varphi_1] + ... + [\varphi_r] = 2^n\langle 1\rangle + [\varphi_2] + ... + [\varphi_r].$$

Then we have $[\varphi_2] + ... + [\varphi_r] \equiv_{S_F(\varphi_1)} 2^n\langle -1\rangle$, implying that

$$\dim_{W,F}(\varphi) \geq \dim_{W,F}(\varphi_2 + ... + \varphi_r) \geq \dim_{W,F}([\varphi_2] + ... + [\varphi_r]) = 2^n.$$

$\square$

Now, we turn our attention to graded rings associated to abstract quadratic forms theories (special hyperfields, or equivalently, special groups): we will apply the above established Theorem APH to obtain information on the *inductive graded rings* (Definition 3.1 in [27]) of a special group G: the graded Witt ring of G,

$$W_*(G) = (I^n(G)/I^{n+1}(G) \overset{\langle 1,1\rangle\otimes -}{\longrightarrow} I^{n+1}(G)/I^{n+2}(G))_{n\in\mathbb{N}},$$

and on the graded ring of k-theory of G,

$$k_*(G) = (k_n(G) \overset{\lambda(-1)\otimes -}{\longrightarrow} k_{n+1}(G))_{n\in\mathbb{N}}.$$

The uses of k-theoretic (and Boolean) methods in abstract theories of quadratic forms has been proved a very successful method, see for instance, these two papers of Dickmann and Miraglia:

[27] where they give an affirmative answer to Marshall's Signature Conjecture, and [29], where they give an affirmative answer to Lam's Conjecture (previously both conjecture have kept open for almost three decades). These two central papers makes us take a deeper look at the theory of special groups (and hence, hyperbolic/pre-special hyperfields) by itself. This is not mere exercise in abstraction: from Marshall's and Lam's Conjecture many questions arise in the abstract and concrete context of quadratic forms.

We will freely permute between a special group G and a special hyperfield F since the associations $G \mapsto F_G := G\dot{\cup}\{0\}$ and $F \mapsto G_F := F \setminus \{0\}$ are part of an equivalence of categories ([24], [17]). The graded Witt ring of a special group is studied in [27] and [28]; [30] is the reference for the k-theory of special groups; in [18] is developed a k-theory for all hyperbolic hyperfields (that includes all pre-special hyperfields).

For the reader's convenience we recall below some relevant definitions.

defn:ksg-aph

Definition 6.3.3 (The Dickmann-Miraglia k-theory [30]). *For each special group G (written multiplicatively) we associate a (inductive) graded ring*

$$k_*G = (k_0G, k_1G, ..., k_nG, ...)$$

as follows: $k_0G := \mathbb{F}_2$ and $k_1G := G$ written additively. With this purpose, we fix the canonical "logarithm" isomorphism $\lambda : G \to k_1G$, $\lambda(ab) = \lambda(a) + \lambda(b)$. Observe that $\lambda(1)$ is the zero of k_1G and k_1G has exponent 2, i.e, $\lambda(a) = -\lambda(a)$ for all $a \in G$. In the sequel, we define k_*G by the quotient of the $\mathbb{F}_2$-graded algebra

$$(\mathbb{F}_2, k_1G, k_1G \otimes_{\mathbb{F}_2} k_1G, k_1G \otimes_{\mathbb{F}_2} k_1G \otimes_{\mathbb{F}_2} k_1G, ...)$$

by the (graded) ideal generated by $\{\lambda(a) \otimes \lambda(ab),\, a \in D_G(1,b)\}$. In other words, for each $n \geq 2$,

$$k_nG := T^n(k_1G)/Q^n(G),$$

where

$$T^n(k_1G) := k_1G \otimes_{\mathbb{F}_2} k_1G \otimes_{\mathbb{F}_2} ... \otimes_{\mathbb{F}_2} k_1G$$

and $Q^n(G)$ is the subgroup generated by all expressions of type $\lambda(a_1) \otimes \lambda(a_2) \otimes ... \otimes \lambda(a_n)$ such that for some i with $1 \leq i < n$, there exist $b \in G$ such that $a_i \in D_G(1,b)$ and $a_i = a_{i+1}b$, which in symbols, means

$$\begin{aligned} Q^n(G) := \langle \{\lambda(a_1) \otimes \lambda(a_2) \otimes ... \otimes \lambda(a_n) :\ & \textit{exists } 1 \leq i < n \textit{ and } b \in G \\ & \textit{such that } a_i = a_{i+1}b \textit{ and } a_i \in D_G(1,b)\}\rangle. \end{aligned}$$

2.4kt-aph

Definition 6.3.4 ([27], [30]). *Let G be a formally real special group.*

a - It holds [MC(G)] (i.e., G satisfies "Marshall's conjecture") if for all $n \geq 1$ and all forms φ over G,

$$\textit{For all } \sigma \in X_G,\ \textit{if } \sigma(\varphi) \equiv 0 \bmod 2^n \textit{ then } \varphi \in I^nG.$$

b - It holds [WMC(G)] (i.e., G satisfies "Weak Marshall's conjecture") if for all $n \geq 1$, the multiplication by $\langle 1,1\rangle$ is an injection of $I^n(G)/I^{n+1}(G)$ into $I^{n+1}(G)/I^{n+2}(G)$.

c - It holds [SMC(G)] (i.e., G satisfies "Strong Marshall's conjecture") if for all $n \geq 1$, the multiplication by $\lambda(-1)$ is an injection of $k_n(G)$ into $k_{n+1}(G)$.

It follows from Proposition 4.6.(e) in [27] that [MC(G)] $\Rightarrow$ [WMC(G)]; in Proposition 4.4 in [29] is established [SMC(G)] $\Rightarrow$ [MC(G)], for all reduced special group G. Now we apply Theorem APH to obtain the following:

MC-aph

Proposition 6.3.5. *Let G be a formally real special group. Then G satisfy Marshall [MC] (i.e., Marshall's signature conjecture holds in G) iff G satisfy [WMC] (i.e., Weak Marshall's conjecture holds in G).*

Proof. In the theorem 5.3 of [27] is established the equivalence of [MC] and [WMC] for all formally real special groups G such that $2^k = \langle 1,1\rangle^k \notin I^{k+1}(G)$,for all $k \geq 1$. But, it follows from Theorem APH that *all* formally real special groups automatically satisfies that property: otherwise $\langle 1,1\rangle^k$ will be hyperbolic and thus $-1 \in Sat(G) = \bigcup_{k\in\mathbb{N}} D_G(2^k)$, contradicting that G is a formally real special group. $\square$

igr1-aph

Definition 6.3.6. *An **inductive graded ring** (or **Igr** for short) is a structure $\mathcal{R} = ((R_n)_{n\geq 0}, (h_n)_{n\geq 0}, *_{nm})$ where*

i - $R_0 \cong \mathbb{F}_2$.

ii - R_n *is a group of exponent 2 with a distinguished element* $\top_n$.

iii - $h_n : R_n \to R_{n+1}$ *is a group homomorphism such that* $h_n(\top_n) = \top_{n+1}$.

iv - For all $n \geq 0$, $h_n = *_{1n}(\top_1, \_)$.

v - The ring

$$R = \bigoplus_{n\geq 0} R_n$$

is a commutative graded ring.

vi - For $0 \leq s \leq t$ *define*

$$h_s^t = \begin{cases} Id_{R_s} \text{ if } s = t \\ h_{t-1} \circ ... \circ h_{s+1} \circ h_s \text{ if } s < t. \end{cases}$$

Then if $p \geq n$ *and* $q \geq m$, *for all* $x \in R_n$ *and* $y \in R_m$,

$$h_n^p(x) * h_m^q(y) = h_{n+m}^{p+q}(x * y).$$

*A **morphism** between Igr's $\mathcal{R}$ and $\mathcal{R}'$ is a morphism of pointed groups and*

$$f = \bigoplus_{n\geq 0} f_n : R \to R'$$

is a morphism of commutative rings with unity (thus $\alpha_{n+1} \circ h_n = h'_{n+1} \circ \alpha_n$). The category of inductive graded rings (in first version) and their morphisms will be denoted by IGR.

In [18] are considered some full subcategories of IGR and [21] deals with limits and colimits of IGR and these subcategories. A particularly useful subcategories is IGR_h, the full subcategory of Igr's $\mathcal{R}$ where for each $a \in R_1$, $\top_1 *_{1,1} a = a *_{1,1} a \in R_2$. Proposition 4.18 and Definition 4.19 therein describes a functor $\Gamma : IGR_h \to pSG$ (the category of pre-special groups, that is equivalent to the category of pre-special hyperfields).

Now, let $R \in IGR_h$. We have a pre-special group $\Gamma(\mathcal{R}) = (G(\mathcal{R}), +, -\cdot, 0, 1)$ by the following: firstly, fix an isomorphism $e_R : (R_1, +_1, 0_1, \top_1) \to (G(\mathcal{R}), \cdot, 1, -1)$. This isomorphism makes, for example, an element $a *_{11} (\top_1 + b) \in R_2$, $a, b \in R_1$ take the form $(e_R^{-1}(x)) *_{11} (e_R^{-1}((-1) \cdot y)) \in R_2$, $x, y \in G(\mathcal{R})$.

Now, let $\Gamma(\mathcal{R}) := G(\mathcal{R})$ and for $a, b, c, d \in R_1$ we have $\langle e_R(a), e_R(b)\rangle \equiv \langle e_R(c), e_R(d)\rangle$ iff $a + b = c + d \in R_1$ and $a *_{11} b = c *_{11} d \in R_2$

If $\alpha = (\alpha_n)_{n\in\mathbb{N}} : \mathcal{R} \to \mathcal{R}'$ is a IGR-morphism, then $\Gamma(\alpha) : G(\mathcal{R}) \to G(\mathcal{R}')$ is the unique function (that turns out to be a pSG-morphism) such that $\Gamma(\alpha) = e_{R'} \circ \alpha_1 \circ e_R^{-1}$.

For each $G \in pSG$, the Igr's $W_*(G)$ and $k_*(G)$ belongs to the subcategory IGR_h (Lemma 3.2 in [27], [30] and Lemma 9.12 in [28]) is defined a IGR-morphism $s_G : k_*(G) \to W_*(G)$ such that: $(s_G)_n(\lambda(a_1) \otimes \cdots \otimes \lambda(a_n)) = \langle 1, -a_1\rangle \otimes \cdots \otimes \langle 1, -a_n\rangle$ (Theorem 4.1 in [29]). In general $(s_G)_n : k_n(G) \to I^n(G)/I^{n+1}(G)$ is a surjective homomorphism of pointed 2-groups and if $n = 0, 1, 2$, then $(s_G)_n$ is an isomorphism of pointed 2-groups.

Theorem 4.20 in [18] establishes that the functor $k_* : pSG \to IGR_q$ is left adjoint to the functor Γ and the natural transformation that is the unity of this adjunction, $\kappa = (\kappa_G)_{G\in pSG}$, is such that for each $G \in pSG$, $\kappa_G : G \to \Gamma(k_*(G))$, $g \mapsto \lambda(g)$ is a pSG-morphism that is an isomorphism of the underlying pointed 2-groups.

In [46] M. Marshall proved that $\omega_G : G \to I(G)/I^2(G)$ $g \mapsto \langle 1, -g\rangle + I^2(G)$ is an isomorphism of pointed groups such that for each $a, b, c, d \in G$:

$$\langle a, b\rangle \equiv_G \langle c, d\rangle \Rightarrow \langle 1, -a\rangle \otimes \langle 1, -b\rangle + I^3(G) = \langle 1, -c\rangle \otimes \langle 1, -d\rangle + I^3(G).$$

Thus, for each special group G, we have the following commutative diagram of pre-special groups and pSG-morphisms

$$(G \overset{\omega_G}{\to} \Gamma(W_*(G))) = (G \overset{\kappa_G}{\to} \Gamma(k_*(G)) \overset{\Gamma(s_G)}{\to} \Gamma(W_*(G)))$$

that is, moreover, natural in G. Now we are in position to state the:

k-stable-aph

Proposition 6.3.7. *Let G be a special group. Then*

i - $\Gamma(s_G) : \Gamma(k_*(G)) \to \Gamma(W_*(G)))$ is a pSG-isomorphism.

ii - $\omega_G : G \to \Gamma(W_*(G))$ is a pSG-isomorphism.

iii - $\kappa_G : G \to \Gamma(k_*(G))$ is a pSG-isomorphism.

In particular, $\Gamma(k_*(G))$ and $\Gamma(W_*(G))$ are special groups.

Proof. This is essentially contained in the *proof of* Lemma 3.5 in [30], but for convince the reader we provide some details:

First observe that, from axiom [SG4] is enough to show that for $x, y \in G$ are equivalent:
(1) $x \in D_G(1, y)$;
(2) $\lambda(x) \in D_{\Gamma(k_*(G))}(\lambda(1), \lambda(y))$;
(3) $\langle 1, -x\rangle + I^2(G) \in D_{\Gamma(W_*(G))}(\langle 1, -1\rangle + I^2(G), \langle 1, -y\rangle + I^2(G))$

(1) $\Rightarrow$ (2): is clear from the definition of $k_*(G)$, just note that condition (2) is equivalent to $\lambda(x)\lambda(xy) = 0 \in k_2(G)$

(2) $\Rightarrow$ (3): this follows directly from $s_G : k_*(G) \to W_*(G)$ be a IGR_h-morphism

(3) $\Rightarrow$ (1): note that condition (3) is equivalent to $\langle 1, -x\rangle \otimes \langle 1, -xy\rangle + I^3(G)) = 0 + I^3(G))$. This means that $\langle 1, -x\rangle \otimes \langle 1, -xy\rangle \in I^3(G)$. Since $\dim(\langle 1, -x\rangle \otimes \langle 1, -xy\rangle) = 4 < 8 = 2^3$, then by Theorem APH, $\langle 1, -x\rangle \otimes \langle 1, -xy\rangle$ is an isotropic Pfister form. Thus it is an hyperbolic form, and then, by Proposition 2.2.(k) in [28], $x \in D_G(1, y)$. $\square$

The notion of k-stable hyperbolic hyperfield F, i.e. those such that canonical morphism $\kappa_F : F \to \Gamma(k_*(F))\dot{\cup}\{0\}$ is an isomorphism of hyperfields, it is fundamental in [14]. Thus the previous result establishes the:

k-stable-co

Corollary 6.3.8. *Every special hyperfield F is k-stable.*

The following result shows that the k-theory construction provides a very good encoding of the – neither complete neither cocomplete – category of special groups into the complete and cocomplete category of inductive graded rings.

epiK-aph

Proposition 6.3.9. *The functor $k_* : SG \to IGR$ is full and faithful.*

Proof. We have to show that for each special groups G_0 and G_1 and any $\beta : k_*G_0 \to k_*G_1$ be an *inductive graded* ring morphism between the associated inductive graded rings of k-theory, then there exist unique SG-morphism $f : G_0 \to G_1$ such that $\beta = k_*(f)$.

Proposition 3.6 in [30] establishes (from Lemma 3.5) that: for each special groups G_0 and G_1 and any $\beta : k_*(G_0) \to k_*(G_1)$ be a *graded* ring morphism between the induced k-theory graded rings, such that $\beta_0 = id_{\mathbb{F}_2}$ and G_1 is a AP(3) special group, then there exist a qSG-morphism $f : G \to H$ such that $\beta = k_*(f)$. Moreover, this f is uniquely determined since $\beta_1 \circ \lambda_{G_0} = \lambda_{G_1} \circ f$ and $\lambda_{G_i} : G_i \to k_1(G_i)$ is an isomorphism of groups of exponent 2 that preserves the distinguished elements $(-1_{G_i} \mapsto \lambda_{G_i}(-1_{G_i}))$.

Thus the result follows since any special group G_1 satisfies is AP(3) (by Theorem APH), and since β is a IGR-morphism then automatically $\beta_0 = id_{\mathbb{F}_2}$ and $\beta_1 = k_1(f)$ implies that $f(-1_{G_0}) = -1_{G_1}$, thus f the qSG-morphism f is a SG-morphism. □

Remark 6.3.10. *The previous result can be derived, alternatively from Corollary 6.3.8 and Theorem 4.20 in [18]: from an well known result on adjoint functors, a left adjoint is a full and faithful functor iff the unity of the adjunction is an isomorphism. Thus $k_* : SG \to IGR_h$ is a full and faithful functor and, since $IGR_h \subseteq IGR$ is a full subcategory, then $k_* : SG \to IGR$ is full and faithful.*

Chapter 7

The Galois group of a Special Group

The Igr's functors W_*, k_* were extended by M. Dickmann and F.Miraglia from the category of fields of characteristic $\neq 2$ to the category of special groups (equivalently, the category of special hyperfields). Another relevant Igr functor, the graded cohomology ring, $H^*(Gal(F^s|F), \{\pm 1\})$ remains defined only on the field setting. This chapter constitutes an attempt to provide an Igr functor associated to a (Galois) cohomology theory for special groups, based on the work of J. Minac and M. Spira [53]. We will define - by "generator and relations", $Gal(G)$, the *Galois Group of an SG G* (Definition 7.2.10), and provide some properties of this construction, as the encoding of the orderings on G. However, since deeper results will depend of a description of $Gal(G)$ "from below", and it still unavailable a complete theory of algebraic extension of (super)hyperfields, we will not pursue a more complete development of this cohomology theory in this thesis, reserving it for a future research. The main results here, established for the "standard pre-special groups", are Theorems 7.3.12, 7.3.13 and 7.3.15, that recover for the abstract context the characterization of orderings in terms of the involutions in the Galois group of a field. These results provide a clue that this profinite group $Gal(G)$, defined by generators and relations, is not -at this moment- a legitimate Galois group (since a characterization of it from quadratic subextensions is still missing), but it works in some aspects as a Galois group of a field in the sense that it can encode faithfully some relevant information on the structure of G.

We will work in the category of pro-2-groups, and take, as usual, the conventions: "subgroup" means "closed subgroup"; "subgroup generated by a subset" means "the closure of the abstract group generated by the subset"; "morphism" means "continuous homomorphism".

7.1 The motivation: W-groups

The context that we will keep in mind is essentially that of the results developed in sections 1 and 2 of [53]. In this Section we will reproduce (and expand the details of) part of these results.

Consider a field F. In [53], J. Minac and M. Spira define a special Galois extension of the base field F, and determine its structure and its Galois group through the behavior of quaternions algebras over F. As they developed in [53], this extension contain essentially all the information need to understand the behavior of quadratic forms over F.

Recall that the **quadratic closure** of F, denoted by F_q, is the smallest extension of F which is closed under taking of square roots (or more explicit, the compositum of all 2-towers over F inside a fixed algebraic closure of F). The group $\mathrm{Gal}_F(F_q)$ will be denoted by G^q_F.

Let $\{a_i : i \in I\}$ be a basis of $\dot{F}/\dot{F}^2$ (as Minac and Spira did in their paper, we will assume that $1, 2, .., n \in I$ with $1 < 2 < ... < n$ in order to easy our presentation). We define $F^{(2)} =$

$F(\sqrt{a} : a \in \dot{F})$ (note that $F^{(2)} = F(\sqrt{a_i} : i \in I)$, $\mathcal{E} = \{y \in F^{(2)} : F^{(2)}(\sqrt{y})|F$ is Galois$\}$ and $F^{(3)} = F^{(2)}(\sqrt{y} : y \in \mathcal{E})$ if F; if F is quadratically closed we set $F^{(2)} = F^{(3)} = F$.

Minac and Spira built a strong connection between $F^{(3)}$ and the Witt ring of F. They named $F^{(3)}$ as **Witt closure** of F. The group $G_F := \mathrm{Gal}_F(F^3|F)$ is called the **W-group** of F. Our goal here is to describe a way to factor G_F as $G_F \cong \mathcal{W}(I)/\mathcal{V}(I)$, with $\mathcal{W}(I)$ and $\mathcal{V}(I)$ interesting profinite groups. This procedure will reveal how to generalize G_F in the context of abstract theories of quadratic forms, and in particular, describe what would be a Galois group associated to a special group. The first step is to describe $\mathcal{W}(I)$.

For an arbitrary group G, define $\hat{G} = G^4[G^2, G]$, i.e, the (closed) subgroup generated by fourth powers and by commutators of the form $[g^2, h]$ for $g, h \in G$. Let $t^4[g^2, h] \in \hat{G}$. Then, for each $z \in G$:

$$z^{-1}(t^4[g^2,h])z = z^{-1}t^4[g^2,h]z = (z^{-1}t^4z)(z^{-1}[g^2,h]z)$$

with $z^{-1}t^4z = (z^{-1}tz)^4 \in G^4$ and $z^{-1}[g^2,h]z \in [G^2, G]$, because

$$\begin{aligned} z^{-1}[g^2,h]z &= z^{-1}g^{-2}h^{-1}g^2hz \\ &= (z^{-1}g^{-2}z)(z^{-1}h^{-1}z)(z^{-1}g^2z)(z^{-1}hz) \\ &= (z^{-1}gz)^{-2}(z^{-1}hz)^{-1}(z^{-1}gz)^2(z^{-1}hz) \\ &= [(z^{-1}gz)^2, (z^{-1}hz)]. \end{aligned}$$

Hence $\hat{G}$ is a normal subgroup of G, and we define $\overline{G} = G/\hat{G}$. Let $\mathcal{C}$ denote the class of profinite 2-groups G such that $\hat{G} = \{1\}$.

The main example (and the motivation to consider this full subcategory of pro-2-groups) is the following fact: If $char(F) \neq 2$ then $G = Gal(F^{(3)}|F)$ satisfies this condition $\hat{G} = \{1\}$, since, by Proposition 2.1 in [53], $G \cong G_q/{G_q}^4.[{G_q}^2, G_q]$, where $G_q = Gal(F_q|F)$ and F_q is a quadratic closure of F .

A pro-$\mathcal{C}$-group will be called just $\mathcal{C}$-group, and $\mathcal{C}$-group on I if it has a minimal set of generators of cardinality $|I|$.

Let I be a well-ordered set. The next step is to describe a canonical way to represent the elements of $\overline{S}$ where S is the free pro-2-group on a nonempty set I. Let

$$\mathcal{W}(I) := \prod_{i\in I}\mathbb{Z}_2 \times \prod_{\substack{i,j\in I\\ i<j}}\mathbb{Z}_2 \times \prod_{i\in I}\mathbb{Z}/2\mathbb{Z}.$$

Here we are considering $\mathbb{Z}_2$ *multiplicatively*, i.e, $\mathbb{Z}_2 \cong \{1, -1\}$. A typical element of $\mathcal{W}_I$ will be written as $(t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(x_i^{\gamma_i})$, where $\alpha_i, \beta_{ij}, \gamma_i \in \{0,1\}$ and $t_i = t_{ij} = x_i = -1$ for all $i, j \in I$.

Let $g, h \in \mathcal{W}(I)$

$$\begin{aligned} g &= (t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(x_i^{\gamma_i}) \\ h &= (t_i^{\alpha'_i})(t_{ij}^{\beta'_{ij}})(x_i^{\gamma'_i}). \end{aligned}$$

We define

$$gh = (t_i^{\alpha_i+\alpha'_i+\gamma_i\gamma'_i})(t_{ij}^{\beta_{ij}+\beta'_{ij}+\gamma'_i\gamma_j})(x_i^{\gamma_i+\gamma'_i}),$$

where the exponents are taken modulo 2.

Lemma 7.1.1. *With the notation described above, $\mathcal{W}(I)$ is a group.*

Proof. Let

$$\begin{aligned} g &= (t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(x_i^{\gamma_i}) \\ h &= (t_i^{\alpha_i'})(t_{ij}^{\beta_{ij}'})(x_i^{\gamma_i'}) \\ k &= (t_i^{\alpha_i''})(t_{ij}^{\beta_{ij}''})(x_i^{\gamma_i''}) \\ 1 &= (t_i^{0})(t_{ij}^{0})(x_i^{0}). \end{aligned}$$

First of all,

$$\begin{aligned} g \cdot 1 &= (t_i^{\alpha_i+0+\gamma_i\cdot 0})(t_{ij}^{\beta_{ij}+0+0\cdot\gamma_j})(x_i^{\gamma_i+0}) = g, \\ 1 \cdot g &= (t_i^{0+\alpha_i+0\cdot\gamma_i})(t_{ij}^{0+\beta_{ij}+\gamma_i\cdot 0})(x_i^{0+\gamma_i}) = g, \end{aligned}$$

hence 1 is in fact the neutral element of $\mathcal{W}(I)$. In order to find g^{-1}, we need to solve a system of modulo 2 congruences.

$$gh := 1 \Rightarrow \begin{cases} \alpha_i + \alpha_i' + \gamma_i\gamma_i' \equiv_2 0 \\ \beta_{ij} + \beta_{ij}' + \gamma_i'\gamma_j \equiv_2 0 \\ \gamma_i + \gamma_i' \equiv_2 0 \end{cases} \Rightarrow \begin{cases} \gamma_i' \equiv_2 \gamma_i \\ \beta_{ij}' \equiv_2 \beta_{ij} + \gamma_i\gamma_j \\ \alpha_i' \equiv_2 \alpha_i + \gamma_i \end{cases}$$

Then, taking

$$g^{-1} = (t_i^{\alpha_i+\gamma_i})(t_{ij}^{\beta_{ij}+\gamma_i\gamma_j})(x_i^{\gamma_i})$$

we obtain $g \cdot g^{-1} = g^{-1} \cdot g = 1$.

Finally, for associativity, we have

$$\begin{aligned} (g \cdot h) \cdot k &= [(t_i^{\alpha_i+\alpha_i'+\gamma_i\gamma_i'})(t_{ij}^{\beta_{ij}+\beta_{ij}'+\gamma_i'\gamma_j})(x_i^{\gamma_i+\gamma_i'})] \cdot k \\ &= (t_i^{\alpha_i+\alpha_i'+\alpha_i''+\gamma_i\gamma_i'+(\gamma_i+\gamma_i')\gamma_i''})(t_{ij}^{\beta_{ij}+\beta_{ij}'+\beta_{ij}''+\gamma_i'\gamma_j+\gamma_i''(\gamma_j+\gamma_j')})(x_i^{\gamma_i+\gamma_i'+\gamma_i''}) \\ &= (t_i^{\alpha_i+\alpha_i'+\alpha_i''+\gamma_i\gamma_i'+\gamma_i\gamma_i''+\gamma_i'\gamma_i''})(t_{ij}^{\beta_{ij}+\beta_{ij}'+\beta_{ij}''+\gamma_i'\gamma_j+\gamma_i''\gamma_j+\gamma_i''\gamma_j'})(x_i^{\gamma_i+\gamma_i'+\gamma_i''}) \end{aligned}$$

and

$$\begin{aligned} g \cdot (h \cdot k) &= g \cdot [(t_i^{\alpha_i'+\alpha_i''+\gamma_i'\gamma_i''})(t_{ij}^{\beta_{ij}'+\beta_{ij}''+\gamma_i''\gamma_j'})(x_i^{\gamma_i'+\gamma_i''})] \\ &= (t_i^{\alpha_i+\alpha_i'+\alpha_i''+\gamma_i'\gamma_i''+\gamma_i(\gamma_i'+\gamma_i'')})(t_{ij}^{\beta_{ij}+\beta_{ij}'+\beta_{ij}''+\gamma_i''\gamma_j'+(\gamma_i'+\gamma_i'')\gamma_j})(x_i^{\gamma_i+\gamma_i'+\gamma_i''}) \\ &= (t_i^{\alpha_i+\alpha_i'+\alpha_i''+\gamma_i'\gamma_i''+\gamma_i\gamma_i'+\gamma_i\gamma_i''})(t_{ij}^{\beta_{ij}+\beta_{ij}'+\beta_{ij}''+\gamma_i''\gamma_j'+\gamma_i'\gamma_j+\gamma_i''\gamma_j})(x_i^{\gamma_i+\gamma_i'+\gamma_i''}). \end{aligned}$$

Thus $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ completing the proof. □

Remark 7.1.2. *1. Note that, if $|I| = n$, then*

$$|\mathcal{W}(I)| = \left| \prod_{i \in I} \mathbb{Z}_2 \times \prod_{\substack{i,j \in I \\ i \leq j}} \mathbb{Z}_2 \times \prod_{i \in I} \mathbb{Z}_2 \right| = 2^{(n^2+3n)/2}.$$

2. The example above is the free $\mathcal{C}$ in n-generators. In fact: for each $n \in \mathbb{N}$, let $F(n)$ be the free *group in n-generators, then* $\mathcal{W}(n) \cong F(n)/\hat{F}(n)$.

3. *It follows that the category of finite (discrete) groups* G *with* $\hat{G} = \{1\}$ *is a category of* $\mathbb{Z}_2$-*modules that is closed by homomorphic images, subgroups and finite products. In particular,* $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$ *and* $\mathbb{D}_4 \cong \mathbb{Z}_2 \ltimes \mathbb{Z}_4$ *(the 8-element dihedral group), are finite* $\mathcal{C}$-*groups.*

Lets denote, for $k, l \in I$,

$$\begin{aligned} t_k &:= (t_i^{\delta_{ik}})(1_{ij})(1_i) \\ t_{kl} &:= (1_i)(t_{ij}^{\delta_{(ij)(kl)}})(1_i) \\ x_k &:= (1_i)(1_{ij})(x_i^{\delta_{ik}}) \end{aligned}$$

where for all $i, j, k, l \in I$, $\delta_{ik} = 1$ if $i = k$ and $\delta_{ik} = 0$ otherwise; and $\delta_{(ij)(kl)} = 1$ if $i = k$ and $j = l$, and $\delta_{(ij)(kl)} = 0$ otherwise. After some straightforward calculations we obtain the following results.

fixms1

Lemma 7.1.3. *Consider* t_k, t_{kl}, x_k *as above. Then for all* $g, h \in \mathcal{W}(I)$, *with* $g = (t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(x_i^{\gamma_i})$, $h = (t_i^{\alpha'_i})(t_{ij}^{\beta'_{ij}})(x_i^{\gamma'_i})$ *and* $z = (t_i^{\alpha''_i})(t_{ij}^{\beta''_{ij}})(x_i^{\gamma''_i})$, *we have the following:*

i - $t_k \cdot t_k = 1$.

ii - $x_k \cdot x_k = t_k$.

iii - *If* $k < l$ *then* $[x_k, x_l] = t_{kl}$.

iv - $g^{-1} = (t_i^{\alpha_i+\gamma_i})(t_{ij}^{\beta_{ij}+\gamma_i\gamma_j})(x_i^{\gamma_i})$.

v - $g^2 = (t_i^{\gamma_i})(t_{ij}^{\gamma_i\gamma_j})(1_i)$.

vi - $h^g = ghg^{-1} = (t_i^{\alpha'_i})(t_{ij}^{\beta'_{ij}+\gamma_i\gamma'_j+\gamma'_i\gamma_j})(x_i^{\gamma'_i})$.

vii - $[g, h] = (1_i)(t_{ij}^{\gamma_i\gamma'_j+\gamma'_i\gamma_j})(1_j)$.

viii - $g^4 = [g^2, h] = 1$.

ix - $[[z, w], h] = 1$.

Remark 7.1.4. *In [53], they simply denote*

$$g = (x_i^{2\alpha_i})([x_i, x_j]^{\beta_{ij}})(x_i^{\gamma_i}).$$

But we are not going to use this simplification here.

Now, for each $i, j \in I$, consider the following three sets:

$$\begin{aligned} M_i &:= \left\{ g = (t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(x_i^{\gamma_i}) \in \mathcal{W}(I) : \gamma_i = 0 \right\}, \\ S_i &:= \left\{ g = (t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(x_i^{\gamma_i}) \in \mathcal{W}(I) : \alpha_i = \gamma_i = 0 \right\}, \\ D_{ij} &:= \left\{ g = (t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(x_i^{\gamma_i}) \in \mathcal{W}(I) : \beta_{ij} = \gamma_i = \gamma_j = 0 \right\}. \end{aligned}$$

Now, consider the following families

$$\begin{aligned} &M(I) := \{M_i : i \in I\},\ S(I) := \{S_i : i \in I\},\ D(I) := \{D_{ij} : i, j \in I, i \leq j\}, \\ &V := M(I) \cup S(I) \cup D(I). \end{aligned}$$

fixms2

Proposition 7.1.5. *Let $i, j \in I$.*

a - M_i is a maximal normal subgroup of $\mathcal{W}(I)$ such that $\mathcal{W}(I)/M_i \cong \mathbb{Z}_2$.

b - S_i is a normal subgroup of $\mathcal{W}(I)$ such that $S_i \subseteq M_i$ and $\mathcal{W}(I)/S_i \cong \mathbb{Z}_4$.

c - D_{ij} is a normal subgroup of $\mathcal{W}(I)$ such that $D_{ij} \subseteq M_i \cap M_j$ and $\mathcal{W}(I)/D_{ij} \cong \mathbb{D}_4$.

d - $\bigcap V = \{1\}$.

Proof. We establish the following notation: let $g \in \mathcal{W}(I)$. Then $g = (t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(x_i^{\gamma_i})$ for suitable $\alpha_i, \beta_{ij}, \gamma_i \in \{0, 1\}$. We denote

$$\alpha_i(g) := \alpha_i,\ \beta_{ij}(g) := \beta_{ij} \text{ and } \gamma_i(g) := \gamma_i.$$

In this sense, if $g, h \in \mathcal{W}(I)$ then

$$gh = (t_i^{\alpha_i(g)+\alpha_i(h)+\gamma_i(g)\gamma_i(h)})(t_{ij}^{\beta_{ij}(g)+\beta_{ij}(h)+\gamma_i(h)\gamma_j(g)})(x_i^{\gamma_i(g)+\gamma_i(h)}).$$

Moreover, using the formulas in Lemma 7.1.3, we obtain that for all $i, j \in I$, M_i, S_i and D_{ij} are proper normal subgroups of $\mathcal{W}(I)$.

a - Let $\tau, \theta \in \mathcal{W}(I) \setminus M_i$. Then $\gamma_i(\tau) = \gamma_i(\theta) = 1$ and

$$\gamma_i(\theta^{-1}\tau) = \gamma_i(\theta) + \gamma_i(\tau) = 0.$$

Therefore $\theta^{-1}\tau \in M_i$ which imply

$$\mathcal{W}(I)/M_i = \{\overline{1}, \overline{\tau}\} \cong \mathbb{Z}_2.$$

b - Note that $S_i \subseteq M_i$. Now, let $\tau, \theta \in M_i \setminus S_i$. Then $\alpha_i(\tau) = \alpha_i(\theta) = 1$ and

$$\alpha_i(\theta^{-1}\tau) = [\alpha_i(\theta) + \gamma_i(\theta)] + \alpha_i(\tau) + \gamma_i(\theta)\gamma_i(\tau) = 0.$$

Hence $\theta^{-1}\tau \in S_i$, and $M_i/S_i \cong \mathbb{Z}_2$. So we have an exact sequence

$$1 \to M_i/S_i \xrightarrow{\iota} \mathcal{W}(I)/S_i \xrightarrow{\pi} \mathcal{W}(I)/M_i \to 1,$$

where ι and π are respectively the canonical inclusion and canonical projection. Moreover

$$\mathcal{W}(I)/S_i \cong M_i/S_i \rtimes \mathcal{W}(I)/M_i \text{ or } \mathcal{W}(I)/S_i \cong \mathcal{W}(I)/M_i \ltimes M_i/S_i.$$

In both cases,

$$|\mathcal{W}(I)/S_i| = |M_i/S_i \times \mathcal{W}(I)/M_i| = |\mathbb{Z}_2 \times \mathbb{Z}_2| = 4.$$

Now let $\sigma \in \mathcal{M} \setminus M_i$. We have $\sigma^4 = 1 \in S_i$ with

$$\gamma_i(\sigma^3) := \gamma_i(\sigma) = 1.$$

Then $\overline{\sigma}^3 \neq \overline{1}$ in $\mathcal{W}(I)/S_i$, which proves that $\mathcal{W}(I)/S_i$ has an element of order 4. Then

$$\mathcal{W}(I)/S_i \cong \mathbb{Z}_4.$$

c - Remember that

$$\mathbb{D}_4 := \langle r, s : r^4 = s^2 = (sr)^2 = 1 \rangle.$$

Using the same argument of item (b), we get $(M_i \cap M_j)/D_{ij} \cong \mathbb{Z}_2$ and $|\mathcal{W}(I)/(M_i \cap M_j)| = 4$ with

$$|\mathcal{W}(I)/D_{ij}| = |(M_i \cap M_j)/D_{ij} \times \mathcal{W}(I)/(M_i \cap M_j)| = 8.$$

More specifically, if we get $\tau_1 \in (M_i \cap M_j) \setminus D_{ij}$, $\tau_2, \theta_2 \in M_i \setminus M_j$, $\tau_3, \theta_3 \in M_j \setminus M_i$ and $\tau_4, \theta_4 \in \mathcal{W}(I) \setminus (M_i \cup M_j)$, with

$$\beta_{ij}(\tau_2) = \beta_{ij}(\tau_3) = \beta_{ij}(\tau_4) = 1$$
$$\beta_{ij}(\theta_2) = \theta_{ij}(\theta_3) = \theta_{ij}(\tau_4) = 0$$

then the following equations hold in $\mathcal{W}(I)/D_{ij}$

$$\overline{\tau_1}^2 = \overline{1}$$
$$\overline{\tau_4^{-1}\theta_4} = \overline{\tau_3^{-1}\theta_3} = \overline{\tau_2^{-1}\theta_2} = \overline{\tau_1}$$

Then

$$\mathcal{W}(I)/D_{ij} = \{\overline{1}, \overline{\tau_1}, \overline{\tau_2}, \overline{\tau_3}, \overline{\tau_4}, \overline{\tau_1\tau_2}, \overline{\tau_1\tau_3}, \overline{\tau_1\tau_4}\},$$

with the following table of multiplication:

$\cdot$	$\overline{\tau_1}$	$\overline{\tau_2}$	$\overline{\tau_3}$	$\overline{\tau_4}$	$\overline{\tau_1\tau_2}$	$\overline{\tau_1\tau_3}$	$\overline{\tau_1\tau_4}$
$\overline{\tau_1}$	$\overline{1}$	$\overline{\tau_1\tau_2}$	$\overline{\tau_1\tau_3}$	$\overline{\tau_1\tau_4}$	$\overline{\tau_2}$	$\overline{\tau_3}$	$\overline{\tau_4}$
$\overline{\tau_2}$	$\overline{\tau_1\tau_2}$	$\overline{1}$	$\overline{\tau_1\tau_4}$	$\overline{\tau_3}$	$\overline{\tau_1}$	$\overline{\tau_4}$	$\overline{\tau_1\tau_3}$
$\overline{\tau_3}$	$\overline{\tau_1\tau_3}$	$\overline{\tau_4}$	$\overline{1}$	$\overline{\tau_1\tau_2}$	$\overline{\tau_1\tau_4}$	$\overline{\tau_1}$	$\overline{\tau_2}$
$\overline{\tau_4}$	$\overline{\tau_1\tau_4}$	$\overline{\tau_1\tau_3}$	$\overline{\tau_2}$	$\overline{\tau_1}$	$\overline{\tau_3}$	$\overline{\tau_1\tau_2}$	$\overline{1}$
$\overline{\tau_1\tau_2}$	$\overline{\tau_2}$	$\overline{\tau_1}$	$\overline{\tau_4}$	$\overline{\tau_1\tau_3}$	$\overline{1}$	$\overline{\tau_1\tau_4}$	$\overline{\tau_3}$
$\overline{\tau_1\tau_3}$	$\overline{\tau_3}$	$\overline{\tau_1\tau_4}$	$\overline{\tau_1}$	$\overline{\tau_2}$	$\overline{\tau_4}$	$\overline{1}$	$\overline{\tau_1\tau_2}$
$\overline{\tau_1\tau_4}$	$\overline{\tau_4}$	$\overline{\tau_3}$	$\overline{\tau_1\tau_2}$	$\overline{1}$	$\overline{\tau_1\tau_3}$	$\overline{\tau_2}$	$\overline{\tau_1}$

Then denoting $r = \tau_4$ and $s = \tau_2$ we get $r^4 = s^2 = (sr)^2 = 1$ and

$$\begin{aligned}
\overline{1} &= s^2 = r^4, \\
\overline{\tau_1} &= r^2, \\
\overline{\tau_2} &= s, \\
\overline{\tau_3} &= sr, \\
\overline{\tau_4} &= r, \\
\overline{\tau_1\tau_2} &= r^2 s, \\
\overline{\tau_1\tau_3} &= r^2 sr = rs, \\
\overline{\tau_1\tau_4} &= r^3;
\end{aligned}$$

witnessing the desired isomorphism.

d - By the very definition

$$\bigcap V = \left\{ g = (t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(x_i^{\gamma_i}) \in \mathcal{W}(I) : \beta_{ij} = \alpha_i = \gamma_i = \gamma_j = 0 \text{ for all } i, j \in I \right\} = \{1\}.$$

□

Let V as in Proposition 7.1.5 and let $P_{fin}(V)$ be the set of finite subsets of V and for $A \in P_{fin}(V)$, denote

$$X_A = W_I / \bigcap A.$$

Note that $P_{fin}(V)$ is a directed poset with the partial ordering induced by inclusion. If $B \subseteq A$, denote by $\pi_{AB} : X_A \to X_B$ the canonical projection. Then $(X_A, \pi_{AB}, P_{fin}(V))$ is a projective system, in the sense that $\pi_{AA} = id_{X_A}$ and, if $E \subseteq B \subseteq A$, then $\pi_{AE} = \pi_{BE} \circ \pi_{AB}$.

`fixms3`

Proposition 7.1.6. *The canonical "diagonal" function*

$$\mathcal{W}(I) \to \varprojlim_{A \in P_{fin}(V)} X_A, \text{ which is given by the rule } g \mapsto (g/X_A)_{A \in P_{fin}(V)}$$

is an abstract group isomorphism, so, by transport, $\mathcal{W}(I)$ is a (topological) profinite 2-group with $P_{fin}(V)$ as fundamental system of clopen neighborhoods of $\{1\}$.

Proof. Let $X = \prod_{A \in P_{fin}(V)} X_A$ and $\pi_A : X \to X_A$ be the canonical projection. Denote $\Delta : \mathcal{W}(I) \to X$ the morphism given by the rule $\Delta(g) := (g/X_A)_{A \in P_{fin}(V)}$. This morphism Δ is injective since

$$\mathrm{Ker}(\Delta) = \bigcap_{A \in P_{fin}(V)} = \{1\}.$$

Now, let $\overline{g} = (g/X_A)_{A \in P_{fin}(V)} \in \mathrm{Im}(\Delta)$. If $B \subseteq A$, we get

$$\overline{g}_B = g/X_B = (g/X_A)/X_B = (\pi_{AB}(g))/X_B.$$

Moreover $\mathrm{Im}(\Delta) \subseteq \varprojlim_{A \in P_{fin}(V)} X_A$. To prove the surjectivity of Δ, consider the morphism $\pi_A : \mathcal{W}(I) \to X_A$ given by the canonical projection. Then $(\mathcal{W}(I), \pi_A)$ is a compatible system of surjective morphisms where Δ is the exact morphism induced by $(\mathcal{W}(I), \pi_A)$. Then $\mathrm{Im}(\Delta)$ is a dense subset of $\varprojlim_{A \in P_{fin}(V)} X_A$ (for instance, see Lemma 1.1.7 of [56]) which is also closed. If $\varphi_A : \varprojlim_{A \in P_{fin}(V)} X_A \to X_A$ denote the projection, we have a new projective system $(\varphi_A(\mathrm{Im}(\Delta), \pi_{AB}|_{\varphi_A(\mathrm{Im}(\Delta)})$. Then (using Corollary 1.1.8 of [56]) we get

$$\mathrm{Im}(\Delta) = \varprojlim_{A \in P_{fin}(V)} \varphi_A(\mathrm{Im}(\Delta) = \overline{\mathrm{Im}(\Delta)} = \varprojlim_{A \in P_{fin}(V)} X_A.$$

Moreover

$$\{\mathrm{Ker}(\pi_A) : \mathcal{W}(I) \to X_A\}_{A \in P_{fin}(V)} = P_{fin}(V)$$

is a fundamental system of neighborhoods of $\{1\}$. □

Lets invoke some terminology from the theory of profinite groups:

Definition 7.1.7. *Let G be a profinite group.*

*i - We say that X **generates** G **as a profinite group** if $G = \overline{\langle G \rangle}$. In that case, we call X a set of **topological generators** of G.*

*ii - We say that $X \subseteq G$ **converges to 1** if every open subgroup U of G contains all but a finite number of the elements in X.*

*iii - Let G be a profinite group. The **Frattini subgroup** of G, notation $\Phi(G)$, is the intersection of all its maximal open subgroups.*

Fact 7.1.8. *Let G be a profinite group.*

i - G is compact, Hausdorff and totally disconnected (has a topological basis of clopens).

ii - A subgroup U is open if and only if is closed of finite index (Lemma 2.1.2 of [56]).

iii - A closed subgroup H of a profinite group G is the intersection of all open subgroups of G containing H. If H is normal, then H is the intersection of all open normal subgroups of G containing H (Proposition 2.1.4 of [56]).

iv - A maximal closed subgroup is necessarily open.

v - $\Phi(G)$ is a characteristic subgroup of G: for every automorphism $\psi : G \to G$ of G we have $\psi[\Phi(G)] = \Phi(G)$.

vi - If $h : H \to G$ is a continuous homomorphism of pro-2-groups then $h[\Phi(H)] \subseteq \Phi[G]$.

rz2.8.7

Lemma 7.1.9 (Lemma 2.8.7 of [56])**.** *Let p be a prime number and let G be a pro-p group.*

a - Every maximal closed subgroup M of G has index p.

b - The Frattini quotient $G/\Phi(G)$ is a p-elementary abelian profinite group and hence a vector space of the field $\mathbb{F}_p$ with p elements.

c - $\Phi(G) = \overline{G^p[G,G]}$, where $G^p = \{x^p : x \in G\}$ and $[G,G]$ denotes the commutator subgroup of G.

lifting-le

Lemma 7.1.10. *Let $\mathcal{G}_i$, $i = 0, 1$ be* projectives *profinite groups and $\mathcal{V}_i \subseteq \mathcal{G}_i$ be normal closed subgroups such that $\mathcal{V}_i \subseteq \Phi(\mathcal{G}_i)$. If $f : \mathcal{G}_0/\mathcal{V}_0 \to \mathcal{G}_1/\mathcal{V}_1$ is an epimorphism (respectively an isomorphism) then there is some continuous homomorphism $\tilde{f} : \mathcal{G}_0 \to \mathcal{G}_1$ such that $q_1 \circ \tilde{f} = f \circ q_0$ where the q_i are the projections on quotient; besides any such lifting $\tilde{f}$ is an epimorphism (resp. an isomorphism).*

$$
\begin{tikzcd}
\mathcal{G}_0 \arrow[r, "\tilde{f}"] \arrow[d, "q_0"'] & \mathcal{G}_1 \arrow[d, "q_1"] \\
\mathcal{G}_0/\mathcal{V}_0 \arrow[r, "f"'] & \mathcal{G}_1/\mathcal{V}_1
\end{tikzcd}
$$

In [53] is established the main categorical property of $\mathcal{W}(I)$:

fixms4

Theorem 7.1.11 (Universal Property of $\mathcal{W}(I)$, Theorem 1.1 of [53])**.** *The group $\mathcal{W}(I)$ is the $\mathcal{C}$-free group on I-generators. In other words, $I \subseteq \mathcal{W}(I)$ is a generator set converging to 1 and if $f : I \to G$ is any function to a $\mathcal{C}$-group G such that $f[I] \subseteq G$ converges to 1 then there is an (unique) continuous homomorphism $\tilde{f} : \mathcal{W}(I) \to G$ such that $\tilde{f}|_I = f$. Moreover, if H is any $\mathcal{C}$-group then H has a generator set converging to 1 of cardinality $|I|$ if and only if there is an epimorphism $\mathcal{W}(I) \twoheadrightarrow H$ with kernel V contained in $\Phi(I)$, the Frattini subgroup of $\mathcal{W}(I)$.*

Corollary 7.1.12. *Let $X = \{x_i : i \in I\} \subseteq \mathcal{W}(I)$. Then X is a set of generators of $\mathcal{W}(I)$ converging to 1.*

fixms5

Proposition 7.1.13. *We have $\Phi(I) = \mathcal{W}_I^2$, and $\Phi(I)$ has $\{x_i, t_{ij} : i < j \in I\}$ as a minimal set of generators converging to 1. Moreover*

$$\begin{aligned}\Phi(I) &= \mathcal{W}_I^2 = \bigcap M(I) \\ &= \left\{g = (t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(x_i^{\gamma_i}) \in \mathcal{W}(I) : \gamma_i = 0 \text{ for all } i \in I\right\} \\ &= \{g \in \mathcal{W}(I) : \text{there exists } g_1, g_2, g_3 \in \mathcal{W}(I) \text{ such that } g = g_1^2 g_2^2 g_3^2\}.\end{aligned}$$

We have some kind of duality theorems for $\Phi(I)$ and $\mathcal{W}(I)$.

fixms6

Proposition 7.1.14. *Consider the $\mathbb{Z}_2$-module of homogeneous quadratic polynomials in I variables $\{z_i\}_{i\in I}$*

$$P_2(I) = \{q \in \mathbb{Z}_2[I] : q = \sum_{i\in I} a_i z_i^2 + \sum_{i<j\in I} b_{ij} z_i z_j\} \cong \bigoplus_{i\in I} \mathbb{Z}_2 \oplus \bigoplus_{i<j\in I} \mathbb{Z}_2.$$

Then we have a topological group isomorphism

$$\Phi(I) \cong Hom(P_2(I), \mathbb{Z}_2) \cong \prod_{i\in I} \mathbb{Z}_2 \times \prod_{i<j\in I} \mathbb{Z}_2,$$

with the associated "perfect pairing"

$$\langle \_, \_ \rangle : \Phi(I) \times P_2(I) \to \mathbb{Z}_2.$$

Proof. First of all, note that $P_2(I)$ is generated (as $\mathbb{Z}_2$-vector space) by the set of monomials $B = \{z_i^2, z_i z_j\}_{i<j\in I}$. In fact, this is a $\mathbb{Z}_2$-basis of $P_2(I)$. Let B^* be the dual basis

$$B^* := \{\varphi_{ij}\}_{i\le j\in I},$$

where $\varphi_{ij} : P_2(I) \to \mathbb{Z}_2$ is given by

$$\varphi_{ij}(z_k z_l) = \begin{cases} 1 \text{ if } i = k \text{ and } j = l \\ 0 \text{ otherwise} \end{cases}$$

Now we define a function $\lambda : \{t_i, t_{ij} : i < j \in I\} \to B^*$ by the rules $t_i \mapsto \varphi_{ii}$ and $t_{ij} \mapsto \varphi_{ij}$. Since $\{t_i, t_{ij} : i < j \in I\}$ is a set of generators of $\Phi(I)$, this function λ induces a continuous group homomorphism $\tilde{\lambda} : \Phi(I) \to \mathrm{Hom}(P_2(I), \mathbb{Z}_2)$ by the following: let $g = (t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(1_i) \in \Phi(I)$ (see Proposition 7.1.13). Define $\tilde{\lambda}(g) : P_2(I) \to \mathbb{Z}_2$ for $q = \sum_{i\in I} a_i z_i^2 + \sum_{i<j\in I} b_{ij} z_i z_j \in P_2(I)$ by

$$\tilde{\lambda}(g)(q) := \sum_{i\in I} a_i \alpha_i + \sum_{i<j\in I} b_{ij} \beta_{ij}.$$

We immediately have that $\tilde{\lambda}$ is a continuous injective group homomorphism. Since λ is bijective and B^* is a $\mathbb{Z}_2$-basis of $\mathrm{Hom}(P_2(I), \mathbb{Z}_2)$, we have that $\tilde{\lambda}$ is an isomorphism. □

fixms7

Proposition 7.1.15. *Consider the $\mathbb{Z}_2$-module of homogeneous linear polynomials in I variables*

$\{z_i\}_{i\in I}$

$$P_1(I) = \{q \in \mathbb{Z}_2[I] : q = \sum_{i\in I} c_i z_i\} \cong \bigoplus_{i\in I} \mathbb{Z}_2.$$

Then we have a topological group isomorphism

$$\mathcal{W}(I)/\Phi(I) \cong Hom(P_1(I), \mathbb{Z}_2) \cong \prod_{i\in I} \mathbb{Z}_2,$$

with the associated "perfect pairing"

$$\langle \_, \_ \rangle : \mathcal{W}(I)/\Phi(I) \times P_1(I) \to \mathbb{Z}_2.$$

Proof. First of all, note that $P_1(I)$ is generated (as $\mathbb{Z}_2$-vector space) by the set of monomials $B = \{z_i\}_{i\in I}$. In fact, this is a $\mathbb{Z}_2$-basis of $P_1(I)$. Let B^* be the dual basis

$$B^* := \{\varphi_i\}_{i\in I},$$

where $\varphi_i : P_1(I) \to \mathbb{Z}_2$ is given by

$$\varphi_i(z_j) = \begin{cases} 1 \text{ if } i = j \\ 0 \text{ otherwise} \end{cases}$$

Now we define $\theta : \mathcal{W}(I) \to \mathrm{Hom}(P_1(I), \mathbb{Z}_2)$ by the following: for $g = (t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(x_i^{\gamma_i}) \in \mathcal{W}(I)$, let $\theta(g) : P_1(I) \to \mathbb{Z}_2$ be the morphism defined by the rule

$$\text{For } q = \sum_{i\in I} c_i z_i \in P_1(I),\ \theta(g)(q) = \sum_{i\in I} c_i \gamma_i.$$

Then θ is a surjective morphism (because $B^* \subseteq \mathrm{Im}(\theta)$) and by Proposition 7.1.13 $\mathrm{Ker}(\theta) = \Phi(I)$. Hence

$$\mathcal{W}(I)/\Phi(I) = \mathcal{W}(I)/\mathrm{Ker}(\theta) \cong \mathrm{Hom}(P_1(I), \mathbb{Z}_2).$$

□

Now, is time to return to our first goal: present the description of $G_F := \mathrm{Gal}_F(F^{(3)})$ by $G_F \cong \mathcal{W}(I)/\mathcal{V}(I)$.

Proposition 7.1.16 (2.1 in [53])**.** $G_F \cong \overline{G_F^q}$.

Then G_F is a C-group on B, where $B = \{a_i : i \in I\}$ is an well-ordered basis of $\dot{F}/\dot{F}^2$, so, using Theorem 7.1.11, there exists an epimorphism $\pi_B : \mathcal{W}(B) \to G_F$. Then we simply take $\mathcal{V}(B) := \mathrm{Ker}(\pi_B)$.

Moreover, J. Minac and M. Spira (again, in [53]) gave a nice explicit description to $\mathcal{V}(B)$. Let $\mathrm{Quat}(F)$ be the subgroup of $Br(F)$, the Brauer group of F, generated by the quaternion algebras of F. By Merkurjev's Theorem ([59]), we have

$$\mathrm{Quat}(F) \cong \mathrm{Br}_2(F) \cong k_2(F),$$

where $Br_2(F)$ is the subgroup of $Br(F)$ generated by elements of order 2 and $k_*(F)$ is the graded ring of Milnor's mod 2 reduced K-theory.

Consider $\varphi_B : P_2(B) \twoheadrightarrow k_2(F)$ as the epimorphism defined by the rule

$$\left(\sum_{i\in I}\alpha_i z_i^2 + \sum_{i<j\in I}\beta_{ij}z_iz_j\right) \mapsto \left(\sum_{i\in I}\alpha_i l(a_i)l(a_i) + \sum_{i<j\in I}\beta_{ij}l(a_i)l(a_j)\right).$$

Let $Q_B := \mathrm{Ker}(\varphi_B)$.

Fact 7.1.17 (Essentially 2.20 in [53]). *$\mathcal{V}(B) = Q_B^{\perp}$, where $Q_B^{\perp} = \{v \in \Phi(B) : \langle v, Q_B\rangle = 0\}$ and $\langle\ ,\ \rangle$ is the perfect pairing described in Proposition 7.1.14.*

Let a F be a field with $char(F) \neq 2$. By "Pontryaguin duality", let M_F denotes the unique maximal clopen subgroup of $F_F = Gal_F(F^{(3)})$ corresponding to $-1 \in SG(F) = \dot{F}/\dot{F}^2$ (Proposition 7.1.15).

Fact 7.1.18 (Essentially 3.3, 3.5, 3.6, 3.7 in [53]). *Let $F, L \in Field_2$. Then are equivalent:*

a - $(W(F), \dot{F}/\dot{F}^2) \cong (W(L), \dot{L}/\dot{L}^2)$ *as* abstract Witt rings.

b - $SG(F) \cong SG(L)$ *as* special groups.

c - $(G_F, M_F) \cong (G_L, M_L)$ *as* pointed profinite-$\mathcal{C}$-groups.

Our next step, is use all these facts to obtain a group associated to a (pre)-special group.

7.2 The Galois Group of a Pre Special Group

Lets deal first, with a special group G. Let $B = \{a_i : i \in I\}$ be a well ordered $\mathbb{Z}_2$-basis of G and consider the $\mathcal{C}$-free group in B-generators $\mathcal{W}(B)$. Define an epimorphism $\pi_B : P_2(B) \to k_2(G)$ by the rule

$$\left(\sum_{i\in I}\alpha_i z_i^2 + \sum_{i<j\in I}\beta_{ij}z_iz_j\right) \mapsto \left(\sum_{i\in I}\alpha_i l(a_i)l(a_i) + \sum_{i<j\in I}\beta_{ij}l(a_i)l(a_j)\right)$$

with kernel $Q(B)$. Take $\mathcal{V}(B) := Q(B)^{\perp} \subseteq \Phi(B) \subseteq \mathcal{W}(B)$. Since $\Phi(B)$ is the center of $\mathcal{W}(B)$ then $\mathcal{V}(B) \subseteq \mathcal{W}(B)$ is a (closed) normal subgroup of $\mathcal{W}(B)$ and we can consider the $\mathcal{C}$-group $\mathcal{W}(B)/\mathcal{V}(B)$.

defn:gal1

Definition 7.2.1 (Galois Group - base dependent version). *Let G be a special group and $B, \mathcal{W}(B)$ and $\mathcal{V}(B)$ as above. We define the **Galois group of G with respect to B** by*

$$Gal(G, B) := \mathcal{W}(B)/\mathcal{V}(B)$$

The most essential information of our Galois group is encoded by $Q(B) = \mathrm{Ker}(\pi_B)$. We have a useful description by generators that generalizes the one described by J. Minac and M. Spira:

fixsg1

Proposition 7.2.2. *Let G be a special group and $B, \mathcal{W}(B)$ and $\mathcal{V}(B)$ as above. Consider a finite subset $B' \subseteq B$, $B' = \{a_{i_0}, ..., a_{i_{n-1}}\}$ $(i_0 < ... < i_{n-1})$, and a, b in the linear span of B', say*

$$a = \prod_{k<n} a_{i_k}^{\alpha_{i_k}} \text{ and } b = \prod_{k<n} a_{i_k}^{\beta_{i_k}},\ \alpha_{i_k}, \beta_{i_k} \in \{0,1\}.$$

Consider the polynomial $q^B_{a,b} \in P_2(B)$ *given by*

$$q^B_{a,b} = \sum_{k<n} \alpha_{i_k}\beta_{i_k} z^2_{i_k} + \sum_{k<l<n} (\alpha_{i_k}\beta_{i_l} + \alpha_{i_l}\beta_{i_k}) z_{i_k} z_{i_l}.$$

Note that $q^B_{a,(b_0\cdot\ldots\cdot b_{n-1})} = \sum_{k<n} q^B_{a,b_k}$. *Moreover we have the following properties.*

i - $\pi_B(q^B_{a,b}) = l(a)l(b) \in k_2(G)$.

ii - $q^B_{a,b}$ *does not depend on the particular choice of the finite subset* $B' \subseteq B$.

iii - $Q(B)$ *is generated by* $\{q^B_{a,b} : l(a)l(b) = 0\}$.

Proof.

i - Note that

$$l(a) = \sum_{k<n} \alpha_{i_k} l(a_{i_k}) \text{ and } l(b) = \sum_{k<n} \beta_{i_k} l(a_{i_k}).$$

Then

$$\begin{aligned} l(a)l(b) &= \left(\sum_{k<n} \alpha_{i_k} l(a_{i_k})\right)\left(\sum_{k<n} \beta_{i_k} l(a_{i_k})\right) = \sum_{k<n}\sum_{p<n} \alpha_{i_k}\beta_{i_p} l(a_{i_k})l(a_{i_p}) \\ &= \sum_{k<n} \alpha_{i_k}\beta_{i_k} l(a_{i_k})l(a_{i_k}) + \sum_{k<n}\sum_{k<p<n} \alpha_{i_k}\beta_{i_p} l(a_{i_k})l(a_{i_p}) + \sum_{k<n}\sum_{p<k<n} \alpha_{i_k}\beta_{i_p} l(a_{i_k})l(a_{i_p}) \\ &= \sum_{k<n} \alpha_{i_k}\beta_{i_k} l(a_{i_k})l(a_{i_k}) + \sum_{k<n}\sum_{k<p<n} (\alpha_{i_k}\beta_{i_p} + \alpha_{i_p}\beta_{i_k}) l(a_{i_k})l(a_{i_p}) \end{aligned}$$

On the other hand, by definition of π_B we get

$$\pi_B(q^B_{a,b}) = \sum_{k<n} \alpha_{i_k}\beta_{i_k} l(a_{i_k})l(a_{i_k}) + \sum_{k<p<n} (\alpha_{i_k}\beta_{i_p} + \alpha_{i_p}\beta_{i_k}) l(a_{i_k})l(a_{i_p}),$$

completing the proof.

ii - It is an immediate consequence of previous item: if B_1, B_2 are finite subsets of B and a, b are elements in the linear span of B_1 and in the linear span of B_2, then

$$q^{B_1}_{a,b} = q^{B_2}_{a,b}.$$

iii - Of course, $q^B_{a,b} \in Q(B)$ if and only if $l(a)l(b) = 0$ in $k_2(G)$ and hence

$$[\{q^B_{a,b} : l(a)l(b) = 0\}] \subseteq Q(B).$$

To get the reverse inclusion, let $q = \sum_{k<n} \alpha_{i_k} z^2_{i_k} + \sum_{k,p<n} \beta_{i_k i_p} z_{i_k} z_{i_p} \in Q$. Then

$$\sum_{k<n} \alpha_{i_k} l(a_{i_k})l(a_{i_k}) + \sum_{k,p<n} \beta_{i_k i_p} l(a_{i_k})l(a_{i_p}) = 0 \text{ in } k_2(G).$$

Now, for each $k < n$ let

$$b_k := a_{i_k}^{\alpha_{i_k}} \prod_{k<p} a_{i_p}^{\beta_{i_k i_p}}.$$

Then $q = \sum_{k<n} q^B_{a_{i_k}, b_{i_k}}$ and

$$\sum_{k<n} l(a_{i_k}) l(b_{i_k}) = 0 \text{ in } k_2(G).$$

We are under the hypothesis of Lemma 7.2.3. Thus, according Theorem 4.3.8, there exists subsets $\{c_0, ..., c_{m-1}\}, \{d_0, ..., d_{n-1}\}$ of G with $m \geq n$ such that

(a) $\{c_0, ..., c_{m-1}\}$ is linearly independent and $c_k = a_{i_k}$ for all $k < n$;

(b) $d_k = b_{i_k}$ for all $k < n$ and $d_k = 1$ for $k = n, ..., m-1$.

(c) For all $x \in [c_0, ..., c_{m-1}]$, there is some $r_x \in D_G(1, -x)$ such that for each $k < m$

$$d_k = \prod_{x \in C_k} r_x$$

where

$$C_k = \left\{ \prod_{p<m} c_p^{\varepsilon_p} : \varepsilon_p \in \{0,1\} \text{ and } \varepsilon_k = 1 \right\}.$$

It follows that

$$\begin{aligned} q &= \sum_{k<n} q^B_{a_{i_k}, b_{i_k}} = \sum_{k<m} q^B_{c_k, d_k} = \sum_{k<m} q^B_{c_k, \prod_{x \in C_k} r_x} \\ &= \sum_{k<m} \sum_{x \in C_k} q^B_{c_k, r_x}. \end{aligned}$$

Denoting $C := [c_0, ..., c_{m-1}]$, we have $C = C_0 \cup ... \cup C_{m-1}$. Then

$$q = \sum_{k<m} \sum_{x \in C_k} q^B_{c_k, r_x} = \sum_{x \in C} q^B_{x, r_x}.$$

Since $r_x \in D_G(1, -x)$, we have $l(x) l(r_x) = 0$ in $k_2(G)$. Then

$$q = \sum_{x \in C} q^B_{x, r_x} \in [\{q^B_{a,b} : l(a) l(b) = 0\}].$$

□

Now, we will generalize the Galois group for pre-special groups. The K-theory developed by M. Dickmann and F. Miraglia in [30] is available for pre-special groups. Then we can take the same $B, \mathcal{W}(B)$ and $\mathcal{V}(B)$ we are considering until now.

Let G be a special group and $B = \{v_i\}_{i \in I}$, $C = \{w_i\}_{i \in I}$, $D = \{z_i\}_{i \in I}$ be ordered $\mathbb{Z}_2$-basis of G. Then, for all $i \in I$ we have an expression

base-change-prod

$$w_i = \prod_{k \in I} v_k^{m_{ik}}, \; m_{ik} \in \{0,1\} \text{ for all } i, k \in I, \tag{7.1}$$

where the above product has finite support (i.e, $|\{i, k \in I : m_{ik} \neq 0\}| < \infty$). In other words, for all $i \in I$, there exist unique sequence in I $i_0 < i_1 < \cdots < i_n$ such that

base-change

$$w_i = v_{i_0} \cdot v_{i_1} \cdot ... \cdot v_{i_{n(i)}}. \tag{7.2}$$

By abuse of notation, let $C = \{x_i : i \in I\} \subseteq \mathcal{W}(C)$. We define a function $\mu_{BC} : C \to \mathcal{W}(B)$ by the rule

base-change-2
$$x_i \mapsto x_{i_0} \cdot x_{i_1} \cdot ... \cdot x_{i_n} \text{ if } w_i = v_{i_0} \cdot v_{i_1} \cdot ... \cdot v_{i_n}. \tag{7.3}$$

This function is well-defined because both B and C are basis, so the expression 7.2 is unique.

fixsg2

Lemma 7.2.3. *Let G be a pre-special group and B, C, μ_{BC} as above. There is a unique continuous homomorphism $\mu_{BC} : \mathcal{W}(C) \to \mathcal{W}(B)$ that extends μ_{BC}. Also $\mu_{BC}[\Phi(C)] \subseteq \Phi(B)$.*

Proof. By abuse of notation, let $B = \{x_i : i \in I\} \subseteq \mathcal{W}(B)$ and $C = \{x_i : i \in I\} \subseteq \mathcal{W}(C)$. We have B and C as a set of generators converging to 1 in $\mathcal{W}(B)$ and $\mathcal{W}(C)$ respectively.

Let $X = \mu_{BC}[C] \subseteq \mathcal{W}(B)$. Since $\langle X\rangle = \langle B\rangle$ and $\mathcal{W}(B) = \overline{\langle B\rangle}$, we have that X is a set of generators of $\mathcal{W}(B)$.

Let $U \subseteq \mathcal{W}(B)$ be an open subgroup. Since B is a set of generators converging to 1, there is a finite subset $Y = \{x_{i_1}, ..., x_{j_m}\} \subseteq B$ with $U \cap Y = \emptyset$. Since the set of $\mathbb{F}_2$-linear combinations of a finite set is finite, there is a finite quantity of elements in $\mu_{BC}[C]$ not belonging to U.

The existence and continuity of μ_{BC} is an immediate consequence of the Universal Property of $\mathcal{W}(I)$ (Theorem 7.1.11). An explicit formula for μ_{BC} is given by the following rule: for $g = (t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(x_i^{\gamma_i})$ we set

$$\mu_{BC}(g) := \left(t_i^{(\alpha_i \sum_{k\in I} m_{ik})}\right)\left(t_{ij}^{(\beta_{ij} \sum_{r,s\in I} m_{ir}m_{js})}\right)\left(x_i^{(\gamma_i \sum_{k\in I} m_{ik})}\right).$$

Since $\Phi(\mathcal{W}(C)) = \mathcal{W}(C)^2$ and $\Phi(\mathcal{W}(B)) = \mathcal{W}(B)^2$, we get $\mu_{BC}[\Phi(C)] \subseteq \Phi(B)$. □

change-rem

Remark 7.2.4. *A direct calculation show for all $a, b \in G$ that*

$$m^2_{B,B'}(q^B_{ab}) = q^{B'}_{ab}.$$

Denote $\mu^{(2)}_{B,B'} : \Phi(B') \to \Phi(B)$ the restriction of $\mu_{B,B'}$ to the Frattini's subgroups and $\mu^{(1)}_{B,B'} : \mathcal{W}(B')/\Phi(B') \to \mathcal{W}(B)/\Phi(B)$ the quotient of $\mu_{B,B'}$. Then, from the isomorphism in Proposition 7.1.14 $\Phi(B) \cong Hom(P_2(B), \mathbb{Z}_2)$, we have:

$$\Phi(B') \times P_2(B) \to \mathbb{Z}_2 :< \mu^1_{B,B'} -, - >_B = < -, m^1_{B,B'} - >_{B'}$$

so , for all $\sigma' \in \Phi(B')$

$$< \mu^2_{B,B'}(\sigma'), q^B_{ab} >_B = < \sigma', m^2_{B,B'}(q^B_{ab}) >_{B'} = < \sigma', q^{B'}_{ab} >_{B'}$$

and then $\mu^2_{B,B'}[(q^{B'}_{a,b})^\perp] = (q^B_{ab})^\perp$

fixsg3

Lemma 7.2.5. *The morphism μ_{BC} is an isomorphism, $\mu_{BB} = id_{\mathcal{W}(B)}$, $\mu^{-1}_{BC} = \mu_{CB}$ and*

$$\mu_{BD} = \mu_{BC} \circ \mu_{CD}.$$

Proof. The fact that $\mu_{BB} = id_{\mathcal{W}(B)}$ and $\mu^{-1}_{BC} = \mu_{CB}$ is an immediate consequence of Lemma 7.2.3. For the other part, let $B = \{v_i\}_{i\in I}$, $C = \{w_i\}_{i\in I}$ and $D = \{z_i\}_{i\in I}$ be $\mathbb{F}_2$-basis of G. Then for all

$i \in I$,

$$w_i = \prod_{k\in I} v_k^{m_{ik}},\ z_i = \prod_{k\in I} w_k^{n_{ik}},\ z_i = \prod_{k\in I} v_k^{p_{ik}},$$

such that all these products has finite support. Then

$$z_i = \prod_{k\in I} w_k^{n_{ik}} = \prod_{k\in I}\left(\prod_{r\in I} v_r^{m_{kr}}\right)^{n_{ik}} = \prod_{k\in I}\prod_{r\in I} v_r^{n_{ik}m_{kr}} = \prod_{r\in I}\prod_{k\in I} v_r^{n_{ik}m_{kr}} = \prod_{r\in I} v_r^{p_{ir}}.$$

Moreover

$$\sum_{k\in I}\sum_{r\in I} n_{ik}m_{kr} = \sum_{r\in I}\sum_{k\in I} n_{ik}m_{kr} = \sum_{r\in I} p_{ir}.$$

Then for all $g = (t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(x_i^{\gamma_i}) \in \mathcal{W}(D)$,

$$\begin{aligned}
&\mu_{BC}\circ\mu_{CD}(g) = \mu_{BC}(\mu_{CD}(g)) = \\
&\mu_{BC}\left(\left(t_i^{\alpha_i(\sum_{k\in I} n_{ik})}\right)\left(t_{ij}^{(\beta_{ij}\sum_{r,s\in I} n_{ir}n_{js})}\right)\left(x_i^{(\gamma_i\sum_{k\in I} n_{ik})}\right)\right) = \\
&\left(t_i^{\alpha_i(\sum_{k\in I} n_{ik})(\sum_{r\in I} m_{kr})}\right)\left(t_{ij}^{\beta_{ij}(\sum_{r,s\in I} n_{ir}n_{js})(\sum_{e,f\in I} m_{re}m_{sf})}\right)\left(x_i^{\gamma_i(\sum_{k\in I} n_{ik})(\sum_{r\in I} m_{kr})}\right) = \\
&\left(t_i^{\alpha_i(\sum_{r\in I}\sum_{k\in I} n_{ik}m_{kr})}\right)\left(t_{ij}^{\beta_{ij}(\sum_{r,s\in I}\sum_{e,f\in I}(n_{ir}m_{re})(n_{js}m_{sf}))}\right)\left(x_i^{\gamma_i(\sum_{r\in I}\sum_{k\in I} n_{ik}m_{kr})}\right) = \\
&\left(t_i^{\alpha_i(\sum_{r\in I} p_{ir})}\right)\left(t_{ij}^{\beta_{ij}(\sum_{e,f\in I} p_{ie}p_{jf})}\right)\left(x_i^{\gamma_i(\sum_{r\in I} p_{ir})}\right) = \mu_{BD}(g).
\end{aligned}$$

Then we get $\mu_{BD} = \mu_{BC}\circ\mu_{CD}$. □

Now, consider the Equation 7.1. This expression induce isomorphisms $m^1_{BC} : P_1(B) \to P_1(C)$ and $m^2_{BC} : P_2(B) \to P_2(C)$ given by the rules

$$m^1_{BC}\left(\sum_{i\in I} c_iz_i\right) := \sum_{i\in I} c_i\left(\sum_{k\in I} m_{ik}\right) z_i$$

$$m^2_{BC}\left(\sum_{i\in I} a_iz_i^2 + \sum_{i<j\in I} b_{ij}z_iz_j\right) := \sum_{i\in I} a_i\left(\sum_{k\in I} m_{ik}\right) z_i^2 + \sum_{i<j\in I} b_{ij}\left[\left(\sum_{r\in I} m_{ir}\right)\left(\sum_{s\in I} m_{js}\right)\right] z_iz_j.$$

where all these sums has finite support.

fixsg4

Lemma 7.2.6. *We have*

$$m^1_{BD} = m^1_{BC}\circ m^1_{CD} \text{ and } m^2_{BD} = m^2_{BC}\circ m^2_{CD}.$$

Proof. Lets recover the calculations in the proof of Lemma 7.2.5: let $B = \{v_i\}_{i\in I}$, $C = \{w_i\}_{i\in I}$ and $D = \{z_i\}_{i\in I}$ be $\mathbb{F}_2$-basis of G. Then for all $i \in I$,

$$w_i = \prod_{k\in I} v_k^{m_{ik}},\ z_i = \prod_{k\in I} w_k^{n_{ik}},\ z_i = \prod_{k\in I} v_k^{p_{ik}},$$

such that all these products has finite support. Then

$$z_i = \prod_{k\in I} w_k^{n_{ik}} = \prod_{k\in I}\left(\prod_{r\in I} v_r^{m_{kr}}\right)^{n_{ik}} = \prod_{k\in I}\prod_{r\in I} v_r^{n_{ik}m_{kr}} = \prod_{r\in I}\prod_{k\in I} v_r^{n_{ik}m_{kr}} = \prod_{r\in I} v_r^{p_{ir}}.$$

Moreover

$$\sum_{k\in I}\sum_{r\in I} n_{ik}m_{kr} = \sum_{r\in I}\sum_{k\in I} n_{ik}m_{kr} = \sum_{r\in I} p_{ir}.$$

Then

$$m^1_{BC}\left(m^1_{CD}\left(\sum_{k\in I} c_k z_i\right)\right) = m^1_{BC}\left(\sum_{i\in I} c_i\left(\sum_{k\in I} n_{ik}\right) z_i\right) = \sum_{i\in I} c_i\left(\sum_{k\in I} n_{ik}\right)\left(\sum_{r\in I} m_{kr}\right) z_i$$
$$= \left(\sum_{r\in I} p_{ir}\right) z_i = m^1_{BD}\left(\sum_{k\in I} c_k z_i\right)$$

and hence $m^1_{BD} = m^1_{BC}\circ m^1_{CD}$. In the same reasoning,

$$m^2_{BC}\left(m^2_{CD}\left(\sum_{i\in I} a_i z_i^2 + \sum_{i<j\in I} b_{ij}z_iz_j\right)\right) =$$
$$m^2_{BC}\left(\sum_{i\in I} a_i\left(\sum_{k\in I} n_{ik}\right) z_i^2 + \sum_{i<j\in I} b_{ij}\left[\left(\sum_{r\in I} n_{ir}\right)\left(\sum_{s\in I} n_{js}\right)\right] z_iz_j\right) =$$
$$\sum_{i\in I} a_i\left(m^2_{BC}\left(\left(\sum_{k\in I} n_{ik}\right) z_i^2\right)\right) + m^2_{BC}\left(\sum_{i<j\in I} b_{ij}\left[\left(\sum_{r\in I} n_{ir}\right)\left(\sum_{s\in I} n_{js}\right)\right] z_iz_j\right) =$$
$$\sum_{i\in I} a_i\left(\sum_{k\in I} n_{ik}\left(\sum_{r\in I} m_{kr}\right) z_i^2\right) + \sum_{i<j\in I} b_{ij}\left[\left(\sum_{r\in I} n_{ir}\right)\left(\sum_{s\in I} n_{js}\right)\left(\sum_{e\in I} m_{re}\right)\left(\sum_{f\in I} m_{sf}\right)\right] z_iz_j =$$
$$\sum_{i\in I} a_i\left(\left(\sum_{r\in I}\sum_{k\in I} n_{ik}m_{kr}\right) z_i^2\right) + \sum_{i<j\in I} b_{ij}\left[\left(\sum_{e\in I}\sum_{r\in I} n_{ir}m_{re}\right)\left(\sum_{f\in I}\sum_{s\in I} n_{js}m_{sf}\right)\right] z_iz_j =$$
$$\sum_{i\in I} a_i\left(\sum_{r\in I} p_{ir}\right) z_i^2 + \sum_{i<j\in I} b_{ij}\left[\left(\sum_{e\in I} p_{ie}\right)\left(\sum_{f\in I} p_{jf}\right)\right] z_iz_j =$$
$$m^2_{BD}\left(\sum_{i\in I} a_i z_i^2 + \sum_{i<j\in I} b_{ij}z_iz_j\right)$$

provide that $m^2_{BD} = m^2_{BC}\circ m^2_{CD}$. $\square$

Note that m^1_{BC}, m^2_{BC} induces respectively the isomorphisms

$$\mathfrak{m}^1_{BC} : \mathrm{Hom}(P_1(C),\mathbb{Z}_2) \to \mathrm{Hom}(P_1(B),\mathbb{Z}_2)$$
$$\mathfrak{m}^2_{BC} : \mathrm{Hom}(P_2(C),\mathbb{Z}_2) \to \mathrm{Hom}(P_2(B),\mathbb{Z}_2).$$

given by the respective rules: if $f : P_1(C) \to \mathbb{Z}_2$ and $q = \sum_{i\in I} c_i z_i \in P_1(B)$ then

$$\mathfrak{m}^1_{BC}(f)(q) := f(m^1_{BC}(q)) = f\left(\sum_{i\in I} c_i \left(\sum_{k\in I} m_{ik}\right) z_i\right).$$

In the same reasoning, if $f : P_2(C) \to \mathbb{Z}_2$ and $q = \sum_{i\in I} a_i z_i^2 + \sum_{i<j\in I} b_{ij} z_i z_j \in P_2(B)$ then

$$\mathfrak{m}^2_{BC}(f)(q) := f(m^2_{BC}(q)) = f\left(\sum_{i\in I} a_i \left(\sum_{k\in I} m_{ik}\right) z_i^2 + \sum_{i<j\in I} b_{ij}\left[\left(\sum_{r\in I} m_{ir}\right)\left(\sum_{s\in I} m_{js}\right)\right] z_i z_j\right)$$

Now denote

$$\mu^1_{BC} : \mathcal{W}(C)/\Phi(C) \to \mathcal{W}(B)/\Phi(B)$$

the quotient of μ_{BC} and

$$\mu^2_{BC} : \Phi(C) \to \Phi(B)$$

the restriction of μ_{BC} to the Frattini's subgroups. Also consider the isomorphisms

$$\tilde{\theta} : \mathcal{W}(I)/\Phi(I) \xrightarrow{\cong} \mathrm{Hom}(P_1(I), \mathbb{Z}_2)$$
$$\tilde{\lambda} : \Phi(I) \xrightarrow{\cong} \mathrm{Hom}(P_2(I), \mathbb{Z}_2)$$

of Propositions 7.1.14, and 7.1.15.

fixsg5

Lemma 7.2.7. *Denote $\pi_B : \mathcal{W}(B) \to \mathcal{W}(B)/\Phi(B)$ the canonical projection, with the same for π_C. Then we have a commutative diagram*

$$\begin{tikzcd}
\mathcal{W}(C) \arrow[r, "\theta_C"] \arrow[d, "\mu_{BC}"'] & Hom(P_1(C), \mathbb{Z}_2) \arrow[d, "\mathfrak{m}^1_{BC}"] \\
\mathcal{W}(B) \arrow[r, "\theta_B"] & Hom(P_1(B), \mathbb{Z}_2)
\end{tikzcd}$$

which induces a commutative diagram

$$\begin{tikzcd}
\mathcal{W}(C) \arrow[d, "\pi_C"'] \arrow[dr, "\theta_C"] & \\
\mathcal{W}(C)/\Phi(C) \arrow[r, "\tilde{\theta}_C"] \arrow[d, "\mu^1_{BC}"'] & Hom(P_1(C), \mathbb{Z}_2) \arrow[d, "\mathfrak{m}^1_{BC}"] \\
\mathcal{W}(B)/\Phi(B) \arrow[r, "\tilde{\theta}_B"] & Hom(P_1(B), \mathbb{Z}_2) \\
\mathcal{W}(B) \arrow[u, "\pi_B"] \arrow[ur, "\theta_B"'] &
\end{tikzcd}$$

Proof. Let $g = (t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(x_i^{\gamma_i}) \in \mathcal{W}(C)$ and $q = \sum_{i \in I} c_i z_i \in P_1(B)$. Then

$$\begin{aligned}
(\mathfrak{m}^1_{BC} \circ \theta)(g)(q) &= \mathfrak{m}^1_{BC}(\theta(g)(q)) = \theta(g)(m^1_{BC}(q)) \\
&= \theta(g)\left(\sum_{i\in I} c_i \left(\sum_{k\in I} m_{ik}\right) z_i\right) = \sum_{i\in I} c_i \left(\sum_{k\in I} m_{ik}\right)\gamma_i \\
&= \sum_{i\in I}\sum_{k\in I} c_i m_{ik}\gamma_i.
\end{aligned}$$

On the other hand,

$$\begin{aligned}
(\theta \circ \mu_{BC})(g)(q) &= \theta(\mu_{BC}(g))(q) \\
&= \theta\left(\left(t_i^{\alpha_i(\sum_{k\in I} m_{ik})}\right)\left(t_{ij}^{\beta_{ij}(\sum_{r,s\in I} m_{ir}m_{js})}\right)\left(x_i^{\gamma_i(\sum_{k\in I} m_{ik})}\right)\right)\left(\sum_{i\in I} c_i z_i\right) \\
&= \sum_{i\in I} c_i\left(\gamma_i\left(\sum_{k\in I} m_{ik}\right)\right) = \sum_{i\in I}\sum_{k\in I} c_i m_{ik}\gamma_i = (\mathfrak{m}^1_{BC} \circ \theta)(g)(q).
\end{aligned}$$

Then $\mathfrak{m}^1_{BC} \circ \theta = \theta \circ \mu_{BC}$. Since $\theta_B = \tilde{\theta}_B \circ \pi_B$ and $\theta_C = \tilde{\theta}_C \circ \pi_C$ we have the desired commutative diagram. $\square$

fixsg5b

Lemma 7.2.8. *We have a commutative diagram*

$$\begin{tikzcd}
\Phi(C) \arrow[r, "\tilde{\lambda}_C"] \arrow[d, "\mu^2_{BC}"'] & Hom(P_2(C),\mathbb{Z}_2) \arrow[d, "\mathfrak{m}^2_{BC}"] \\
\Phi(B) \arrow[r, "\tilde{\lambda}_B"'] & Hom(P_2(B),\mathbb{Z}_2)
\end{tikzcd}$$

Proof. Let $g=(t_i^{\alpha_i})(t_{ij}^{\beta_{ij}})(1_i)\in\Phi(C)$ and $\sum_{i\in I}a_iz_i^2+\sum_{i<j\in I}b_{ij}z_iz_j\in P_2(B)$. We have

$$(\mathfrak{m}^2_{BC}\circ\tilde{\lambda}_C)(g)(q)=\tilde{\lambda}_C(g)(m^2_{BC}(q))=$$
$$\tilde{\lambda}_C(g)\left(\sum_{i\in I}a_i\left(\sum_{k\in I}m_{ik}\right)z_i^2+\sum_{i<j\in I}b_{ij}\left[\left(\sum_{r\in I}m_{ir}\right)\left(\sum_{s\in I}m_{js}\right)\right]z_iz_j\right)=$$
$$\sum_{i\in I}a_i\left(\sum_{k\in I}m_{ik}\right)\alpha_i+\sum_{i<j\in I}b_{ij}\left[\left(\sum_{r\in I}m_{ir}\right)\left(\sum_{s\in I}m_{js}\right)\right]\beta_{ij}$$

On the other hand,

$$(\tilde{\lambda}_B\circ\mu^2_{BC})(g)(q)=\tilde{\lambda}(\mu^2_{BC}(g)(q))$$
$$=\tilde{\lambda}_B\left(\left(t_i^{\alpha_i(\sum_{k\in I}m_{ik})}\right)\left(t_{ij}^{\beta_{ij}(\sum_{r,s\in I}m_{ir}m_{js})}\right)(1_i)\right)\left(\sum_{i\in I}a_iz_i^2+\sum_{i<j\in I}b_{ij}z_iz_j\right)=$$
$$\sum_{i\in I}a_i\left(\alpha_i\left(\sum_{k\in I}m_{ik}\right)\right)+\sum_{i<j\in I}b_{ij}\left(\beta_{ij}\left(\sum_{r,s\in I}m_{ir}m_{js}\right)\right)$$

proving that $\mathfrak{m}^2_{BC}\circ\tilde{\lambda}_C=\tilde{\lambda}_B\circ\mu^2_{BC}$. □

fixsg6

Lemma 7.2.9. *With the notations of Lemmas 7.2.2-7.2.7 we have the following.*

i - The arrows μ^1_{BC} and μ^2_{BC} are isomorphisms. Moreover, for all well-ordered basis B,C,D we have $\mu^1_{BB}=id$, $\mu^2_{BB}=id$, $\mu^1_{BD}=\mu^1_{BC}\circ\mu^1_{CD}$ and $\mu^2_{BD}=\mu^2_{BC}\circ\mu^2_{CD}$.

ii - The isomorphism $\mu_{BC}:\mathcal{W}(C)\to\mathcal{W}(B)$ restricts to an isomorphism $\mathcal{V}(C)\to\mathcal{V}(B)$ so we get quotient isomorphism
$$\tilde{\mu}_{BC}:\mathcal{W}(C)/\mathcal{V}(C)\to\mathcal{W}(B)/\mathcal{V}(B).$$

iii - If B,C,D are well-ordered base of G, then $\tilde{\mu}_{CC}=id$ and $\tilde{\mu}_{BD}=\tilde{\mu}_{BC}\circ\tilde{\mu}_{CD}$.

Proof.

i - Just use the same calculations made in Lemma 7.2.5.

ii - By Proposition 7.2.2 we have
$$\mathfrak{m}^2_{BC}(Q(B))=Q(C).$$

Since $\mathcal{V}(B) = Q(B)^{\perp}$, we have an induced isomorphism $\mu_{BC}|_{\mathcal{V}(B)} : \mathcal{V}(B) \xrightarrow{\cong} \mathcal{V}(C)$, legitimating the quotient isomorphism

$$\tilde{\mu}_{BC} : \mathcal{W}(C)/\mathcal{V}(C) \to \mathcal{W}(B)/\mathcal{V}(B).$$

iii - It is an immediate consequence of item (i).

□

defn:gal2

Definition 7.2.10 (Galois Group - base independent version)**.** *Let G be a pre-special group. Take*

$$E_G = \{B : B \textit{ is a well-ordered } \mathbb{F}_2\textit{-basis of } G\}.$$

Consider the set E_G endowed with the trivial groupoid operation of concatenation of pairs (i.e., the arrows are $E_G \times E_G$) and take the functor $Gal : E_G \to \mathcal{C}$, (where $\mathcal{C}$ is the category of $\mathcal{C}$-groups) given by the following rules: for an object $B \in E_G$, $Gal(B) := \mathcal{W}(B)/\mathcal{V}(B)$ and for an arrow $(B, C) \in E_G^2$,

$$Gal(B, C) = \mu_{BC} : \mathcal{W}(C)/\mathcal{V}(C) \to \mathcal{W}(B)/\mathcal{V}(B).$$

*We define the **Galois group** of G, notation $Gal(G)$ by*

$$Gal(G) := \varprojlim_{B \in E_G} \mathcal{W}(B)/\mathcal{V}(B).$$

Remark 7.2.11. *Keeping the notation above, note that*

$$\pi_B : Gal(G) := \varprojlim_{B \in E_G} \mathcal{W}(B)/\mathcal{V}(B) \to \mathcal{W}(B)/\mathcal{V}(B)$$

is an isomorphism, for each $B \in E_G$. This holds because

$$Gal(B, C) = \mu_{BC} : \mathcal{W}(C)/\mathcal{V}(C) \to \mathcal{W}(B)/\mathcal{V}(B)$$

is an isomorphism for each arrow $(B, C) \in E_G^2$.

It is desirable to achieve explicit calculations of Gal(G) for finite reduced special groups and boolean algebras.

7.3 On the structure of Galois Groups of Pre Special Groups

As occurs with fields, the Galois group of a pre-special groups (in a certain subclass) is able to encode many relevant quadratic information.

All pre-special groups occurring is this section will be assumed k-stable.

We start this Section, by providing more details on the structure of $\mathcal{C}$-groups.

Let $\mathcal{G}$ be a $\mathcal{C}$-group on I-minimal generators. By Theorem 7.1.11, There is an epimorphism $\lambda : \mathcal{W}(I) \to \mathcal{G}$ with kernel $\mathcal{V} \subseteq \Phi(I)$, and then, we have an isomorphism $\tilde{\lambda} : \mathcal{W}(I)/\mathcal{V} \to \mathcal{G}$.

fixhugo2

Proposition 7.3.1. *With the above notation, we have the following.*

i - *We have a natural bijection*

$$\{M \subseteq \mathcal{G} : M \textit{ is a maximal open subgroup}\} \cong$$
$$\{M \subseteq \mathcal{W}(I) : M \textit{ is a maximal open subgroup}\}.$$

Then $\Phi(\mathcal{G}) \cong \Phi(I)/\mathcal{V}$ *and* $\mathcal{G}/\Phi(\mathcal{G}) \cong \mathcal{W}(I)/\Phi(I)$.

ii - *The maximal closed subgroups of* $\mathcal{W}(I)$ *are precisely the clopen (normal) subgroups with quotient* $\mathbb{Z}_2$. *Moreover, we have a natural bijection*

$$\{M \subseteq \mathcal{G} : M \textit{ is a maximal open subgroup}\} \cong P_{fin}(I) \setminus \{\emptyset\}.$$

and that extends to a natural bijection

$$\{N \subseteq \mathcal{G} : N \textit{ is an open subgroup with index} \leq 2\} \cong P_{fin}(I).$$

iii - *We have a natural isomorphism of* $\mathbb{Z}_2$*-modules*

$$Homcont(\mathcal{G}, \mathbb{Z}_2) \cong fsFunc(I, \mathbb{Z}_2)$$

where $fsFunc(I, \mathbb{Z}_2)$ *is the set of all function* $f : I \to \mathbb{Z}_2$ *with finite support.*

Proof.

i - The desired bijection follows by the bijection

$$\{M \subseteq \mathcal{W}(I)/\mathcal{V} : M \text{ is a maximal open subgroup}\} \cong$$
$$\{M \subseteq \mathcal{W}(I) : M \text{ is a maximal open subgroup}\}.$$

given by the following rule: lets $q : \mathcal{W}(I) \to \mathcal{W}(I)/\mathcal{V}$ denote the canonical projection. We have a function $\overline{q} : \mathcal{P}(\mathcal{W}(I)/\mathcal{V}) \to \mathcal{P}(\mathcal{W}(I))$ given by the rule

$$\overline{q}(X) := q^{-1}[X] \text{ (the inverse image)}.$$

This function $\overline{q}$ induces the desired bijection. Since the Frattini subgroup of $\mathcal{G}$ is the intersection of all open normal subgroups we have (via $\tilde{\lambda}$ and the bijection) $\Phi(\mathcal{G}) \cong \Phi(I)/\mathcal{V}$. Then

$$\mathcal{G}/\phi(\mathcal{G}) \cong (\mathcal{W}(I)/\mathcal{V})/(\Phi(I)/\mathcal{V}) \cong \mathcal{W}(I)/\Phi(I).$$

ii - For $\{i_0, ..., i_n\} \subseteq I$ denote

$$\zeta_I(i_0, ..., i_n) := \{\sigma \in \mathcal{W}(I) : \gamma_{i_0}(\sigma) + ... + \gamma_{i_n}(\sigma) = 0\}.$$

We have that $\zeta_I(i_0, ..., i_n)$ is a subgroup of $\mathcal{W}(I)$. Now let $\tau, \theta \in \mathcal{W}(I) \setminus \zeta_I(i_0, ..., i_n)$. Then for all $i \in I$,

$$\gamma_i(\theta^{-1}\tau) = \gamma_i(\theta) + \gamma_i(\tau).$$

Therefore

$$\sum_{p=1}^{n} \gamma_{i_p}(\theta^{-1}\tau) = \sum_{p=1}^{n} [\gamma_{i_p}(\theta) + \gamma_{i_p}(\tau)] = \sum_{p=1}^{n} \gamma_{i_p}(\theta) + \sum_{p=1}^{n} \gamma_{i_p}(\tau) = 1 + 1 = 0.$$

Then $\theta^{-1}\tau \in \zeta_I(i_0,...,i_n)$ which imply

$$\mathcal{W}(I)/\zeta_I(i_0,...,i_n) = \{\overline{1},\overline{\tau}\} \cong \mathbb{Z}_2.$$

To verify that $\zeta_I(i_0,...,i_n)$ is clopen, note that

$$\gamma_{i_0}(\sigma)+...+\gamma_{i_n}(\sigma)=0 \text{ iff } \begin{cases}\gamma_{i_0}(\sigma)+...+\gamma_{i_{n-1}}(\sigma)=0 \text{ and } \gamma_{i_n}(\sigma)=0 \text{ or}\\ \gamma_{i_0}(\sigma)+...+\gamma_{i_{n-1}}(\sigma)=1 \text{ and } \gamma_{i_n}(\sigma)=1.\end{cases}$$

In other words,

$$\zeta_I(i_0,...,i_n) = [\zeta_I(i_0,...,i_{n-1})\cap M_{i_n}]\cup[\zeta_I(i_0,...,i_{n-1})^c\cap M_{i_n}^c].$$

So, in order to verify that $\zeta_I(i_0,...,i_n)$ is clopen is enough to deal with the case $n=0$. But $\zeta_I(i_0)=M_{i_0}$ is in fact a clopen, which provide (by induction) that $\zeta_I(i_0,...,i_n)$ is clopen for all $i_0,...,i_n\in I$. Then $\zeta_I(i_0,...,i_n)$ is a maximal clopen subgroup of $\mathcal{W}(I)$, and we have a well-defined injective function

$$\zeta_I:\mathcal{P}_{fin}(I)\setminus\{\emptyset\}\to\{M\subseteq\mathcal{W}(I): M \text{ is a maximal open subgroup}\}$$

given by the rule $\{i_0,...,i_n\}\mapsto\zeta_I(i_0,...,i_n)$.

For surjectivity, let M be a maximal open subgroup. Then M is closed of finite index and by Lemma 7.1.9(a), M has index 2 in G. Using Propositions 7.1.5 and 7.1.6 and the compacity of $\mathcal{W}(I)$, there exists $i_1,...,i_n,j_1,...,j_m,k_1,...,k_p\in I$ with

$$M_{i_1}\cap...\cap M_{i_n}\cap S_{j_1}\cap...\cap S_{j_m}\cap D_{k_1}\cap...\cap D_{k_p}\subseteq M.$$

Note that we have

$$M_{i_1}\cap...\cap M_{i_n}\cap S_{j_1}\cap...\cap S_{j_m}\cap D_{k_1}\cap...\cap D_{k_p}\subseteq \zeta_I(i_1,...,i_n,j_1,...,j_m,k_1,...,k_p).$$

Lets denote $\zeta_I(i_1,...,i_n,j_1,...,j_m,k_1,...,k_p):=\zeta_I(\vec{i},\vec{j},\vec{k})$ and $H:=M\cap\zeta_I(\vec{i},\vec{j},\vec{k})$. Suppose $H\neq M$ and let $\tau,\theta\in M\setminus H$. The same calculations made for injectivity shows that $\theta^{-1}\tau\in\zeta_I(\vec{i},\vec{j},\vec{k})$ which imply

$$M/H=\{\overline{1},\overline{\tau}\}\cong\mathbb{Z}_2.$$

Moreover, using the same calculations made in Proposition 7.1.5(b) we have that H has index $\mathbb{Z}_4$ in $\mathcal{W}(I)$. Since $H\subseteq M$ and $H\subseteq\zeta_I(\vec{i},\vec{j},\vec{k})$ with both maximal clopen subgroups, by Lemma 7.3.7(i) we have $M=\zeta_I(\vec{i},\vec{j},\vec{k})$, contradicting the assumption $H\neq M$. Then $H=M$ and we have $M=\zeta_I(\vec{i},\vec{j},\vec{k})$. Therefore we have bijections

$$\begin{aligned}\mathcal{P}_{fin}(I)\setminus\{\emptyset\}&\cong\{M\subseteq\mathcal{W}(I): M \text{ is a maximal open subgroup}\}\\ &\cong\{M\subseteq\mathcal{G}: M \text{ is a maximal open subgroup}\}.\end{aligned}$$

Therefore

$$\{N\subseteq\mathcal{G}: N \text{ is an open subgroup with index}\leq 2\}\cong P_{fin}(I).$$

iii - Since $\mathcal{G}=\mathcal{W}(I)/\mathcal{V}$ and

$$\mathcal{V}\subseteq\Phi(I)=\bigcap\{ker(\varphi):\varphi\in Homcont(\mathcal{W}(I),\mathbb{Z}_2)\},$$

then the natural epimorphism $\mathcal{W}(I) \twoheadrightarrow \mathcal{W}(I)/\mathcal{V}$ induces the isomorphism

$$Homcont(\mathcal{G}, \mathbb{Z}_2) \cong Homcont(\mathcal{W}(I), \mathbb{Z}_2).$$

Since $\mathbb{Z}_2$ is a finite/discrete $\mathcal{C}$-group, then the universal property of $\mathcal{W}(I)$ (Theorem 7.1.11) gives a natural isomorphism $Homcont(\mathcal{W}(I), \mathbb{Z}_2) \cong fsFunc(I, \mathbb{Z}_2)$.

Alternatively, the result follows also from the item (ii) above and the (obvious) natural bijections

$$Homcont(\mathcal{G}, \mathbb{Z}_2) \cong \{N \subseteq \mathcal{G} : N \text{ is an open subgroup with index} \leq 2\}$$

$$P_{fin}(I) \cong fsFunc(I, \mathbb{Z}_2).$$

□

fixhugo3

Proposition 7.3.2 (Prontryagin duality). *Let $\mathcal{G} = Gal(G)$ for some pre-special group G. Then*

i - *There is a canonical bijection*

$$\mathbb{M} : G \overset{\cong}{\to} \{M \subseteq \mathcal{G} : M \textit{ is a (closed, normal) subgroup of index less or equal to } 2\}$$

$a \mapsto M_a$ such that it induces a canonical bijection

$$G \setminus \{1\} \cong \{M \subseteq \mathcal{G} : M \textit{ is a maximal subgroup}\}.$$

ii - *There is a canonical isomorphism of $\mathbb{Z}_2$-modules $\psi_G : G \overset{\cong}{\to} Homcont(\mathcal{G}, \mathbb{Z}_2)$, $a \mapsto \mu_a$, where $\mu_a : \mathcal{G} \to \mathbb{Z}_2$ is the unique continuous homomorphism such that $ker(\mu_a) = M_a$.*

iii - *There is a canonical isomorphism of pro-2-groups $\phi_G : \mathcal{G}/\Phi(\mathcal{G}) \to Hom(G, \mathbb{Z}_2)$.*

Proof.

i - This follows directly from Proposition 7.3.1, since $\pi_B : Gal(G) \overset{\cong}{\to} \mathcal{W}(B)/\mathcal{V}(B)$ and $\mathcal{V}(B) \subseteq \Phi(B)$, for every well orderd basis B of G.

ii - By Proposition 7.3.1(iii), for each well ordered basis B in G, we have a natural isomorphism of $\mathbb{Z}_2$-modules.

$$Homcont(\mathcal{W}(B)/\mathcal{V}(B), \mathbb{Z}_2) \cong fsFunc(B, \mathbb{Z}_2)$$

This is, in fact, an isomorphism of $\mathbb{Z}_2$-modules. Taking into account the isomorphisms of "change of base", we glue the above isomorphisms to obtain the natural isomorphism

$$Homcont(Gal(G), \mathbb{Z}_2) = Homcont(\varprojlim_{B \in E_G} \mathcal{W}(B)/\mathcal{V}(B), \mathbb{Z}_2) \cong \varprojlim_{B \in E_G} fSFunc(B, \mathbb{Z}_2) \cong G$$

iii - Note that $\pi_{\mathcal{G}} : \mathcal{G} \twoheadrightarrow \mathcal{G}/\Phi(\mathcal{G})$ induces a $\mathbb{Z}_2$-isomorphism

$$\pi_{\mathcal{G}}^* : Homcont(\mathcal{G}/\Phi(\mathcal{G}), \mathbb{Z}_2) \overset{\cong}{\to} Homcont(\mathcal{G}, \mathbb{Z}_2).$$

By Lemma 7.2.7, the isomorphisms described in Proposition 7.1.15, namely

$$\mathcal{W}(B)/\Phi(B) \cong \mathrm{Hom}(P_1(B), \mathbb{Z}_2),$$

are natural. Thus we obtain a natural isomorphism

$$\mathcal{G}/\Phi(\mathcal{G}) \cong Hom(G, \mathbb{Z}_2)$$

$\square$

Remark 7.3.3. *Note that combining items (iii), (ii) of the Proposition above, we obtain the Pontryagin duality:*

$$\mathcal{G}/\Phi(\mathcal{G}) \cong Hom(G, \mathbb{Z}_2) \cong Hom(Homcont(\mathcal{G}/\Phi(\mathcal{G}), \mathbb{Z}_2), \mathbb{Z}_2)$$

$$G \cong Homcont(\mathcal{G}/\Phi(\mathcal{G}), \mathbb{Z}_2) \cong Homcont(Hom(G, \mathbb{Z}_2), \mathbb{Z}_2)$$

This induces a canonical duality between the pointed $\mathbb{Z}_2$-module $(G, -1)$ and the "pointed" pro-2-group $(Gal(G), M)$, where $M \subseteq Gal(G)$ is an open subgroup of index ≤ 2.

Let G be a k-stable special group. Write $\mathcal{G} = \mathrm{Gal}(G)$.

The isomorphism of pro-2-groups $\phi_G : \mathcal{G}/\Phi(\mathcal{G}) \to \mathrm{Hom}(G, \mathbb{Z}_2)$, determines a "perfect pairing" $\hat{\phi}_G : \mathcal{G}/\Phi(\mathcal{G}) \times G \to \mathbb{Z}_2$ given by the rule

$$\hat{\phi}_G(\overline{\alpha}, g) := \langle \overline{\alpha}, g \rangle := \phi_G(\overline{\alpha})(g).$$

We will denote $(\ )^{\perp}$, generically, both the correspondences between subsets of $\mathcal{G}/\Phi(\mathcal{G})$ and subsets of G.

pairing-prop

Proposition 7.3.4. *The perfect pairing $\hat{\phi}_G : \mathcal{G}/\Phi(\mathcal{G}) \times G \to \mathbb{Z}_2$ gives an anti-isomorphism of complete lattices between the poset*

$$\{R \subseteq \mathcal{G}/\Phi(\mathcal{G}) : R \textit{ is a closed subgroup of } \mathcal{G}/\Phi(\mathcal{G})\} =$$

$$\{\pi(T) \subseteq \mathcal{G}/\Phi(\mathcal{G}) : T \textit{ is a closed subgroup of } \mathcal{G}\},$$

with $\pi : \mathcal{G} \to \mathcal{G}/\Phi(\mathcal{G})$ being the canonical projection, and the poset

$$\{\Delta \subseteq G : \Delta \textit{ is a subgroup of } G\}.$$

These anti-isomorphisms are given by the rules

$$\pi(T) \mapsto \pi(T)^{\perp} := \{a \in G : \hat{\phi}_G(\sigma/\Phi(G), a) = 0 \textit{for all } \sigma \in T\}$$
$$H \mapsto H^{\perp} := \{\sigma/\Phi(G) : \hat{\phi}_G(\sigma/\Phi(G), a) = 0 \textit{ for all } a \in H\}.$$

From this we get:

i - An anti-isomorphism of complete lattices between the posets

$$\{\Delta \subseteq G : \Delta \textit{ is a subgroup of } G\}$$

and

$$\{T \subseteq \mathcal{G} : T \textit{ is a closed subgroup and } \Phi(\mathcal{G}) \subseteq T\}.$$

ii - A bijection between the sets

$$\{\Delta \subseteq G : \Delta \textit{ is a maximal subgroup of } G\}$$

and

$$\{\pi(T) \subseteq \mathcal{G}/\Phi(\mathcal{G}) : T \text{ is a discrete subgroup with order } 2\} =$$
$$\{\pi(T) \subseteq \mathcal{G}/\Phi(\mathcal{G}) : T \text{ is a closed subgroup with } \pi(T) = \{id, \sigma/\Phi\}, \text{ for some } \sigma \in \mathcal{G} \setminus \Phi(\mathcal{G})\}.$$

Proof. All items are immediate consequences of the isomorphism.

Since $\mathcal{G}$ is a compact Hausdorff group and $\Phi(\mathcal{G}) \subseteq \mathcal{G}$ is a closed normal subgroup, note that then the quotient map $\mathcal{G} \twoheadrightarrow \mathcal{G}/\Phi(\mathcal{G})$ gives an isomorphism of complete lattices between the poset of closed subgroups of $\mathcal{G}$ which contains $\Phi(\mathcal{G})$ and the poset of closed subgroups of $\mathcal{G}/\Phi(\mathcal{G})$. □

Remark 7.3.5. *Let $\sigma \in \mathcal{G} \setminus \Phi(\mathcal{G})$. It follows from the definition of pairing that:*

- *For any $x \in G - \{1\}$: $\sigma \in M_x$ iff $< \sigma/\Phi(\mathcal{G}), x >= 0$ iff $x \in \{\Phi(\mathcal{G}), \sigma.\Phi(\mathcal{G})\}^\perp$.*
- *If there is an involution in $\sigma.\Phi(\mathcal{G})$ then of all element in $\sigma.\Phi(\mathcal{G})$ are involutions.*

To obtain quadratic information from the Galois groups, we will need develop deeper group theoretic results.

Zd-le

Lemma 7.3.6. *Let B an well ordered basis of G and consider $\eta_B = \pi_B^{-1} : \mathcal{W}(B)/\mathcal{V}(B) \overset{\cong}{\to} Gal(G)$.*

i- *Let $a \neq 1$, choose $B = \{a_i : i \in I\}$ an well ordered basis of G such that $a \in B$, say $a = a_i$. Then $\eta_B[M'_i/\mathcal{V}(B)] = M_a$.*

ii- *Let $a, b \neq 1$, $a \neq b$ so $\{a, b\}$ is a $\mathbb{Z}_2$-l.i. subset of G, choose $B = \{a_i : i \in I\}$ an well ordered basis of G such that $a, b \in B$, say $a = a_i$, $b = a_j$, $i < j \in I$. Let $\{M'_i, M'_j, M'\}$ be the three maximal subgroups of $\mathcal{W}(B)$ above $M'_i \cap M'_j$. Then $\eta_B[M'_i/\mathcal{V}(B)] = M_a$, $\eta_B[M'_j/\mathcal{V}(B)] = M_b$ and $\eta_B[M'/\mathcal{V}(B)] = M_{ab}$.*

iii- *Let $\{M_1, M_2, M_3\} \subseteq Gal(G)$ maximal subgroups that are pairwise distinct. Then are equivalent:*

- *$\{M_1, M_2, M_3\}$ are independent, which means that for* each *of 3 enumerations $\{u, v, w\}$ of $\{1, 2, 3\}$, $M_u \cap M_v \nsubseteq M_w$.*
- *There is* some *enumeration $\{u, v, w\}$ of $\{1, 2, 3\}$ with $M_u \cap M_v \nsubseteq M_w$.*
- *$Gal(G)/(M_1 \cap M_2 \cap M_3) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$*

Proof.

i- Recall that $\mathcal{V}(B) \subseteq \Phi(B) \subseteq M'_k, \forall k \in I$, $M'_i = \{\sigma \in \mathcal{W}(B) : \gamma_i(\sigma) = 0\}$. The "isomorphic" perfect pairings,

$$<,>_B : \mathcal{W}(B)/\Phi(B) \times P_1(B) \to \mathbb{Z}_2$$
$$<,> : Gal(G)/\Phi(Gal(G)) \times G \to \mathbb{Z}_2$$

provides $M'_i/\Phi(B) = \{z_i\}^\perp$ and $M_{a_i}/\Phi(Gal(G)) = \{a_i\}^\perp$. Since the pairings are "compatible", i.e., the dual of the isomorphism $P_1(B) \overset{\cong}{\to} G : z_k \mapsto a_k$, $k \in I$ corresponds to the isomorphism

$$\mathcal{W}(B)/\Phi(B) \underset{can}{\overset{\cong}{\to}} (\mathcal{W}(B)/\mathcal{V}(B))/\Phi((\mathcal{W}(B)/\mathcal{V}(B))) \underset{\bar{\eta}_B}{\overset{\cong}{\to}} Gal(G)/\Phi(Gal(G)),$$

we have $\bar{\eta}_B \circ can[M'_i/\Phi(B)] = M_{a_i}/\Phi(Gal(G))$. Therefore, as the Frattini subgroups are contained in all maximal open subgroups, we get $\eta_B[M'_i/\mathcal{V}(B)] = M_{a_i}$.

ii- $M' = \{\sigma \in \mathcal{W}(B) : \gamma_i(\sigma) + \gamma_j(\sigma) = 0\}$. The "isomorphic" perfect pairings,

$$\mathcal{W}(B)/\Phi(B) \times P_1(B) \to \mathbb{Z}_2 \text{ and } Gal(G)/\Phi(Gal(G)) \times G \to \mathbb{Z}_2$$

provides $M_a/\Phi(Gal(G)) = \{a\}^\perp$ and $M_b/\Phi(Gal(G)) = \{b\}^\perp$, so

$$\begin{aligned} M_{ab}/\Phi(Gal(G)) &= \{ab\}^\perp = \{\theta/\Phi(Gal(G)) :< \theta/\Phi(Gal(G)), ab >= 0\} \\ &\subseteq (M_a)/\Phi(Gal(G)) \cap M_b)/\Phi(Gal(G))) = (M_a \cap M_b)/\Phi(Gal(G)) \end{aligned}$$

Therefore $\{M_a, M_b, M_{ab}\}$ *are the three maximal subgroups of* $Gal(G)$ *above* $M_a \cap M_b$. Since $\{M_i', M_j', M'\}$ are the three maximal subgroups of $\mathcal{W}(B)$ above $M_i' \cap M_j'$ and

$$\eta_B[M_i'/\mathcal{V}(B)] = M_a \text{ and } \eta_B[M_j'/\mathcal{V}(B)] = M_b,$$

we must have $\eta_B[M'/\mathcal{V}(B)] = M_{ab}$

iii- We have uniquely determined $\{a, b, c\} \subseteq G \setminus \{1\}$, with $M_1 = M_a, M_2 = M_b, M_3 = M_c$ and, from the hypothesis, a, b, c are pairwise distinct so the result follows from (ii) since if $\{x, y\}$ is a $\mathbb{Z}_2$-li set then $\{x, xy\}$ and $\{y, xy\}$ are $\mathbb{Z}_2$-li sets and those 3 sets are $\mathbb{Z}_2$-basis of the group $\{1, x, y, xy\}$.

□

`ZqDq-le`

Lemma 7.3.7. *Let G be a k-stable pre-special group and denote $\mathcal{G} := Gal(G)$.*

i - Let $S \subseteq \mathcal{G}$ a normal closed of with $\mathcal{G}/S \cong \mathbb{Z}_4$ then there is a unique maximal subgroup $H \subseteq \mathcal{G}$ such that $S \subseteq H$.

ii - Let $D \subseteq \mathcal{G}$ a normal closed of with $\mathcal{G}/S \cong \mathbb{D}_4$ then there is a unique set $\{H_1, H_2\}$ with $H_1 \neq H_2$, $H_i \subseteq \mathcal{G}$ maximal subgroups such that $D \subseteq H_1 \cap H_2$ and if $\{H, H_1, H_2\}$ are the three *maximal subgroups above $H_1 \cap H_2$ then $H/D \cong \mathbb{Z}_4$.*

Proof.

i - For the existential part take $r \in \mathcal{G} \setminus S$ such that $r^2 \notin S$ and $\mathcal{G}/S = \{1.S, r.S, r^2.S, r^3.S\} \cong \mathbb{Z}_4$ and take the maximal subgroup $H = 1S \cup r^2S$. Then $S \subseteq H$ and the canonical epimorphism $\mathcal{G}/S \twoheadrightarrow \mathcal{G}/H$ corresponds to the epimorphism $\mathbb{Z}_4 \twoheadrightarrow \mathbb{Z}_2$. This maximal $H \supseteq S$ is unique because if $S \subseteq H_1, H_2$ with $H_1 \neq H_2$, then $S \subseteq H_1 \cap H_2$ and there will be an epimorphism $\mathbb{Z}_4 \cong \mathcal{G}/S \twoheadrightarrow \mathcal{G}/H_1 \cap H_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, however there is no element in $\mathbb{Z}_2 \times \mathbb{Z}_2$ of order 4.

ii - For the existential part let $r, s \in \mathcal{G} \setminus D$ be such that $r^2 \notin D, s^2 \in D$ and then

$$\mathbb{D}_4 \cong \mathcal{G}/D = \{1.D, r.D, r^2.D, r^3.D, s.D, sr.D, sr^2.D, sr^3.D\}$$

Then each one of the maximal subgroups above D is a reunion of four classes so they must contain $1D, r^2D$. they are three:

$$\begin{gathered} 1D \cup r^2D \cup rD \cup r^3D \\ 1D \cup r^2D \cup sD \cup sr^2D \\ 1D \cup r^2D \cup srD \cup sr^3D \end{gathered}$$

Then take

$$\begin{aligned}\{H_1, H_2\} &= \{1D \cup r^2D \cup sD \cup sr^2D, 1D \cup r^2D \cup srD \cup sr^3D\} \text{ and}\\ H &= 1D \cup r^2D \cup rD \cup r^3D.\end{aligned}$$

Then $D \subseteq H_1 \cap H_2 = 1D \cup r^2D \subseteq H, H_1, H_2$. Then the canonical epimorphism $\mathcal{G}/D \twoheadrightarrow \mathcal{G}/H_1 \cap H_2$ corresponds to the epimorphism $\mathbb{D}_4 \twoheadrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ and $H/D \cong \mathbb{Z}_4$. This pair of maximals $H_1, H_2 \supseteq D$ is unique because if H_3 is a maximal $S \subseteq H_3$ with $H_3 \neq H_1, H_2$, then $D \subseteq H_1 \cap H_2 \cap H_3$ and we have two to consider:

• $H_1 \cap H_2 \subseteq H_3$: in this case $H_3 = H = 1D \cup r^2D \cup rD \cup r^3D$, then

$$1D = \cup r^2D = H_1 \cap H_2 = H \cap H_1 = H \cap H_2$$

so $D \subseteq H \cap H_1$, but we see directly that $H_2/D \ncong \mathbb{Z}_4$; similarly $D \subseteq H \cap H_2$ but also $H_1/D \ncong \mathbb{Z}_4$;

• $H_1 \cap H_2 \nsubseteq H_3$ then $H_3 \neq H, H_1, H_2$, also $H_1 \cap H_3 \nsubseteq H_2$ (because if $H_1 \cap H_3 \subseteq H_2$, then $H_1 \cap H_2 \nsubseteq H_3$, see the previous Lemma) and similarly $H_2 \cap H_3 \nsubseteq H_1$, then $\{H_1, H_2, H_3\}$ are *independent*, so in this case, the epimorphism $\mathcal{G}/D \twoheadrightarrow \mathcal{G}/H_1 \cap H_2 \cap H_3$ corresponds to an epimorphism $\mathbb{D}_4 \twoheadrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ but there is no element in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ of order 4.

□

standardteo

Theorem 7.3.8.

i - *Let $a \in G \setminus \{1\}$.*

$$l(a).l(a) = 0 \in k_2(G) \;\Rightarrow$$

There is $S \subseteq Gal(G)$, a normal clopen subgroup such that $Gal(G)/S \cong \mathbb{Z}_4$ and $S \subseteq M_a$.

ii - *Let $a, b \in G \setminus \{1\}$ such that $a \neq b$*

$$l(a).l(b) = 0 \in k_2(G) \;\Rightarrow$$

There is $D \subseteq Gal(G)$, a normal clopen subgroup such that $Gal(G)/D \cong \mathbb{D}_4$ and $D \subseteq M_a \cap M_b$, $M_{ab}/D \cong \mathbb{Z}_4$.

Proof.

i - Since $\{a\} \subseteq G$ is a l.i. subset, take an well ordered basis $B = \{a_i : i \in I\} \subseteq G$ such that $a \in B$, say $a = a_i$. Then $\eta_B : \mathcal{W}(B)/\mathcal{V}(B) \overset{\cong}{\to} Gal(G)$ with $\mathcal{V}(B) \subseteq \Phi(B)$ and $\mathcal{V}(B) = Q(B)^\perp$ where $Q(B) = ker(P_2(B) \twoheadrightarrow k_2(G))$, then, by Proposition 7.2.2, $Q(B) = [\{q^B_{xy} : l(x)l(y) = 0\}]$ so

$$\mathcal{V}(B) = \bigcap\{(q^B_{xy})^\perp : l(x)l(y) = 0\} = \bigcap\{(q^B_{xy})^\perp : x, y \neq 1, l(x)l(y) = 0\}.$$

Denote $M'_i = \{\sigma \in \mathcal{W}(B) : \gamma_i(\sigma) = 0\}$ and $S'_i = \{\sigma \in \mathcal{W}(B) : \alpha_i(\sigma) = \gamma_i(\sigma) = 0\}$ then, by Proposition 7.1.5(i), $S'_i \subseteq M'_i \subseteq \mathcal{W}(B)$ are clopen normal subgroups with $\mathcal{W}(B)/M'_i \cong \mathbb{Z}_2$, $\mathcal{W}(B)/S'_i \cong \mathbb{Z}_4$. We have $\mathcal{V}(B) \subseteq \Phi(B) \subseteq M'_i$, and we state the

Claim: $\mathcal{V}(B) \subseteq S'_i$.

This entails that $M_a = \eta_B[M'_i/\mathcal{V}(B)] \subseteq Gal(G)$, $Gal(G)/M_a \cong \mathbb{Z}_2$ and

$$S := \eta_B[S'_i/\mathcal{V}(B)] \subseteq Gal(G)$$

is a clopen normal subgroup of $Gal(G)$ with $Gal(G)/S \cong \mathbb{Z}_4$ and $S \subseteq M_a$, as we need.

Proof of the Claim: We will see that $S'_i \cap \Phi(B) = (q^B_{a_i a_i})^{\perp}$ then as $a = a_i$ and $l(a)l(a) = 0$ we get $\mathcal{V}(B) \subseteq (q^B_{a_i a_i})^{\perp}$ so $\mathcal{V}(B) \subseteq S'_i \cap \Phi(B)$. Since $1 \neq a = a_i$ it follows that $q^B_{a_i a_i} = z_i^2 \in P_2(B)$ is such that $(q^B_{a_i a_i})^{\perp} \subseteq \Phi(B)$ has *index 2* and we will proof that $S'_i \cap \Phi(B) \subseteq \Phi(B)$ has also *index 2* and $S'_i \cap \Phi(B) \subseteq (q^B_{a_i a_i})^{\perp}$ so we get $S'_i \cap \Phi(B) = (q^B_{a_i a_i})^{\perp}$. Firstly we show that $\Phi(B)/S'_i \cap \Phi(B) \cong \mathbb{Z}_2$: as $\Phi(B) \hookrightarrow M'_i$ then $\Phi(B)/S'_i \cap \Phi(B) \rightarrowtail M'_i/S'_i$ and $M'_i/S'_i \cong \mathbb{Z}_2$ so $\Phi(B)/S'_i \cap \Phi(B)$ has 1 or 2 elements. However, it cannot has 1 element: if $S'_i \cap \Phi(B) = \Phi(B)$ then, by Proposition 7.1.13,

$$\bigcap\{M'_j : j \in I\} = \Phi(B) \subseteq S'_i$$

but $\mathcal{W}(B)$ is a compact space and $S'_i \subseteq \mathcal{W}(B)$ is open subset , $M'_j \subseteq \mathcal{W}(B)$ is a closed subset $j \in I$ so there is a *finite subset* $\{j_0, \ldots, j_n\} \subseteq I$ such that $M'_{j_0} \cap \ldots \cap M'_{j_n} \subseteq S'_i$, choose $n \in \mathbb{N}$ *minimum* with this property so for each $m \leq n$, $\bigcap\{M'_{j_l} : l \neq m\} \nsubseteq M'_{j_m}$ then we have an *isomorphism*

$$Gal(G)/\bigcap\{M'_{j_l} : l \leq n\} \overset{\cong}{\to} \prod_{l \leq n} Gal(G)/M'_{j_l}$$

so the epimorphim $Gal(G)/\bigcap\{M'_{j_l} : l \leq n\} \twoheadrightarrow Gal(G)/S'_i$ corresponds to an epimorphism $\prod_{l \leq n} \mathbb{Z}_2 \twoheadrightarrow \mathbb{Z}_4$, but the two elements of order 4 in $\mathbb{Z}_4$ cannot be in the image of the homomorphism. Now we prove that $S'_i \cap \Phi(B) \subseteq (q^B_{a_i a_i})^{\perp}$: we have $(q^B_{a_i a_i})^{\perp} = \{z_i^2\}^{\perp}$ and

$$S'_i \cap \Phi(B) = \{\sigma \in \mathcal{W}(I) : \alpha_i(\sigma) = 0 \text{ and } \gamma_j(\sigma) = 0 \text{ for each } j \in I\}$$

and it follows from of the group operation and the definition of the pairing $<,>: \Phi(B) \times P_2(B) \to \mathbb{Z}_2$ that

$$\{x_k x_l : k < l \in I\} \cup \{x_j^2 : i \neq j \in I\} \subseteq \big(S'_i \cap \Phi(B)\big) \cap \{z_i^2\}^{\perp}$$

Since $S'_i \cap \Phi(B), \{z_i^2\}^{\perp} \subseteq \Phi(B)$ are closed subgroups,

$$closure([\{x_k x_l : k < l \in I\} \cup \{x_j^2 : i \neq j \in I\}]) \subseteq \big(S'_i \cap \Phi(B)\big) \cap \{z_i^2\}^{\perp}.$$

Now we will prove that $S'_i \cap \Phi(B) \subseteq closure([\{x_k x_l : k < l \in I\} \cup \{x_j^2 : i \neq j \in I\}])$; it is enough find for each $\sigma \in S'_i \cap \Phi(B)$ and each *basic* neighborhood T of $1 \in \mathcal{W}(B)$ two finite sets $\{j_1, \ldots j_n\} \subseteq I - \{i\}$ and $\{(k_1, l_1), \ldots (k_m, l_m) : k_u < l_u \in I, 1 \leq u \leq m\}$ such that $(x^2_{j_1}.\ldots.x^2_{j_n}.x_{k_1}x_{l_1}.\ldots.x_{k_m}.x_{l_m}) \in \sigma.T$: let $T = \bigcap U$ where

$$U \subseteq_{fin} V = \{M'_j : j \in I\} \cup \{S'_j : j \in I\} \cup \{D'_{kl} : k < l \in I\}$$

and take

$$\{j_1, \ldots j_n\} = \{j \in I : S'_j \in U, \alpha_j(\sigma) = 1\} \subseteq I \setminus \{i\} \text{ and}$$
$$\{k_1 < l_1, \ldots k_m < l_m\} = \{k < l \in I : D'_{kl} \in U, \beta_{kl}(\sigma) = 1\}$$

$\{j_1, \ldots j_n\} = \{j \in I : S'_j \in U, \alpha_j(\sigma) = 1\} \subseteq I \setminus \{i\}$ and $\{k_1 < l_1, \ldots k_m < l_m\} = \{k < l \in I : D'_{kl} \in U, \beta_{kl}(\sigma) = 1\}$ then, since $\gamma_j(\sigma) = 0$, for all $j \in I$, we get

$$(x^2_{j_1}.\ldots.x^2_{j_n}.x_{k_1}x_{l_1}.\ldots.x_{k_m}.x_{l_m}) \in \sigma.T$$

ii - Since $\{a, b\} \subseteq G$ is a l.i. subset, take an well ordered basis $B = \{a_i : i \in I\} \subseteq G$ such that $a, b \in B$, say $a = a_i, b = a_j, i < j \in I$. We denote

$$\begin{aligned} M'_i &= \{\sigma \in \mathcal{W}(B) : \gamma_i(\sigma) = 0\} \\ M'_j &= \{\sigma \in \mathcal{W}(B) : \gamma_j(\sigma) = 0\} \\ M' &= \{\sigma \in \mathcal{W}(B) : \gamma_i(\sigma) + \gamma_j(\sigma) = 0\} \\ D'_{ij} &= \{\sigma \in \mathcal{W}(B) : \beta_{ij}(\sigma) = \gamma_i(\sigma) = \gamma_j(\sigma) = 0\} \end{aligned}$$

By Proposition 7.1.5(ii), $D'_{ij} \subseteq M'_i, M'_j \subseteq \mathcal{W}(B)$ are clopen normal subgroups with $\mathcal{W}(B)/M'_i \cap M'_j \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathcal{W}(B)/D'_{ij} \cong \mathbb{D}_4$. Besides $\mathcal{V}(B) \subseteq \Phi(B) \subseteq M'_i \cap M'_j$ and we stat the

<u>Claim</u>: $\mathcal{V}(B) \subseteq D'_{ij}$.

This entails that $M_a = \eta_B[M'_i/\mathcal{V}(B)] \subseteq Gal(G)$, $M_b = \eta_B[M'_j/\mathcal{V}(B)]$, $M_{ab} = \eta_B[M'/\mathcal{V}(B)]$, $Gal(G)/M_a \cong \mathbb{Z}_2 \cong Gal(G)/M_b$ and $D \doteq \eta_B[S'_i/\mathcal{V}(B)] \subseteq Gal(G)$ is a clopen normal subgroup of $Gal(G)$ with $Gal(G)/D \cong \mathbb{D}_4$ such that $D \subseteq M_a \cap M_b$ and $M_{ab}/D \cong \mathbb{Z}_4$, as we need.

<u>Proof of the Claim</u>: We will see that $D'_{ij} \cap \Phi(B) = (q^B_{a_i a_j})^{\perp}$ then as $a = a_i, b = a_j$ and $l(a)l(b) = 0$ we get $\mathcal{V}(B) \subseteq (q^B_{a_i a_j})^{\perp}$ so $\mathcal{V}(B) \subseteq D'_{ij} \cap \Phi(B)$. As $1 \neq a = a_i$ and $1 \neq b = a_j$ with $i < j \in I$, it follows that $q^B_{a_i a_j} = z_i z_j \in P_2(B)$ is such that $(q^B_{a_i a_j})^{\perp} \subseteq \Phi(B)$ has *index 2* and we will proof that $D'_{ij} \cap \Phi(B) \subseteq \Phi(B)$ has also *index 2* and $D'_{ij} \cap \Phi(B) \subseteq (q^B_{a_i a_j})^{\perp}$ so we get $D'_{ij} \cap \Phi(B) = (q^B_{a_i a_j})^{\perp}$.

Firstly, we will prove that $\Phi(B)/D'_{ij} \cap \Phi(B) \cong \mathbb{Z}_2$: since $\Phi(B) \hookrightarrow M'_i \cap M'_j$ then

$$\Phi(B)/D'_{ij} \cap \Phi(B) \rightarrowtail M'_i \cap M'_j/D'_{ij} \text{ and } M'_i \cap M'_j/D'_{ij} \cong \mathbb{Z}_2$$

so $\Phi(B)/D'_{ij} \cap \Phi(B)$ has 1 or 2 elements. However it cannot has 1 element: if $D'_{ij} \cap \Phi(B) = \Phi(B)$ then $\bigcap\{M'_k : k \in I\} = \Phi(B) \subseteq D'_{ij}$ but $\mathcal{W}(B)$ is a compact space and $D'_{ij} \subseteq \mathcal{W}(B)$ is open subset , $M'_k \subseteq \mathcal{W}(B)$ is a closed subset $k \in I$ so there is a *finite subset* $\{k_0, \ldots, k_n\} \subseteq I$ such that $M'_{k_0} \cap \ldots \cap M'_{k_n} \subseteq D'_{ij}$, choose $n \in \mathbb{N}$ *minimum* with this property so for each $m \leq n$, $\bigcap\{M'_{k_l} : l \neq m\} \nsubseteq M'_{k_m}$ then we have an *isomorphism*

$$Gal(G)/\bigcap\{M'_{k_l} : l \leq n\} \overset{\cong}{\to} \prod_{l \leq n} Gal(G)/M'_{k_l}$$

so the epimorphism $Gal(G)/\bigcap\{M'_{k_l} : l \leq n\} \twoheadrightarrow Gal(G)/D'_{ij}$ corresponds to an epimorphism $\prod_{l \leq n} \mathbb{Z}_2 \twoheadrightarrow \mathbb{D}_4$, but the two elements of order 4 in $\mathbb{D}_4$ cannot be in the image of the homomorphism.

Now we prove that $D'_{ij} \cap \Phi(B) \subseteq (q^B_{a_i a_j})^{\perp}$: we have $(q^B_{a_i a_j})^{\perp} = \{z_i z_j\}^{\perp}$ and

$$D'_{ij} \cap \Phi(B) = \{\sigma \in \mathcal{W}(I) : \beta_{ij}(\sigma) = 0 \text{ and } \gamma_k(\sigma) = 0 \text{ for each } k \in I\}$$

and it follows from of the group operation and the definition of the pairing

$$<,>: \Phi(B) \times P_2(B) \to \mathbb{Z}_2$$

that

$$\{x_k x_l : k < l \in I, (k,l) \neq (i,j)\} \cup \{x_k^2 : k \in I\} \subseteq \big(D'_{ij} \cap \Phi(B)\big) \cap \{z_i z_j\}^{\perp}$$

then, since $D'_{ij} \cap \Phi(B), \{z_i z_j\}^{\perp} \subseteq \Phi(B)$ are closed subgroups,

$$closure([\{x_k x_l : k < l \in I, (k,l) \neq (i,j)\} \cup \{x_k^2 : k \in I\}]) \subseteq \big(D'_{ij} \cap \Phi(B)\big) \cap \{z_i z_j\}^{\perp}.$$

Now we will prove that $D'_{ij} \cap \Phi(B) \subseteq closure([\{x_k x_l : k < l \in I, (k,l) \neq (i,j)\} \cup \{x_k^2 : k \in I\}])$; it is enough find for each $\sigma \in D'_{ij} \cap \Phi(B)$ and each *basic* neighborhood T of $1 \in \mathcal{W}(B)$ two finite sets $\{j_1, \ldots, j_n\} \subseteq I$ and $\{(k_1,l_1), \ldots (k_m,l_m) : k_u < l_u \in I, (k_u,l_u) \neq (i,j), 1 \leq u \leq m\}$ such that $(x_{j_1}^2 \ldots . x_{j_n}^2 . x_{k_1} x_{l_1} \ldots . x_{k_m} . x_{l_m}) \in \sigma.T$: let $T = \bigcap U$ where

$$U \subseteq_{fin} V = \{M'_j : j \in I\} \cup \{S'_j : j \in I\} \cup \{D'_{kl} : k < l \in I\}$$

and take

$$\{j_1, \ldots j_n\} = \{j \in I : S'_j \in U, \alpha_j(\sigma) = 1\} \subseteq I \text{ and}$$
$$\{k_1 < l_1, \ldots k_m < l_m\} = \{k < l \in I : D'_{kl} \in U, \beta_{kl}(\sigma) = 1\} \subseteq I \times I \setminus \{(i,j)\}$$

then, since $\gamma_k(\sigma) = 0$, for all $k \in I$, we get

$$(x_{j_1}^2 \ldots . x_{j_n}^2 . x_{k_1} x_{l_1} \ldots . x_{k_m} . x_{l_m}) \in \sigma.T.$$

□

The above proposition suggests the following:

pSGstandard-def

Definition 7.3.9. *A pre-special group G is said to be **standard** if it is a k-stable pre-special group and holds both the reverse implications in the Theorem 7.3.8 above.*

Remark 7.3.10. *Lemma 7.3.7 determines (injective) maps*

$$\begin{aligned} &j_1 : \{S \subseteq \mathcal{G} : S \text{ is a normal subgroup of index } \mathbb{Z}_4\} \to \\ &\quad \{M \subseteq \mathcal{G} : M \text{ is a maximal subgroup}\}; \\ &j_2 : \{D \subseteq \mathcal{G} : D \text{ is a normal subgroup of index } \mathbb{D}_4\} \to \\ &\quad\quad \{\{M_1, M_2\} : M_1, M_2 \subseteq \mathcal{G}, \ M_1 \neq M_2 \text{ are maximal subgroups}\}. \end{aligned}$$

By the canonical bijection $\mathbb{M} : G \setminus \{1\} \overset{\cong}{\to} \{M \subseteq Gal(G) : M \text{ is a maximal clopen subgroup }\}$, it is natural to ask:
(1) Which subset of $\{a \in G : a \neq 1\}$ corresponds bijectively with $image(j_1)$?
(2) Which subset of $\{\{a,b\} \subseteq G : a, b \neq 1, a \neq b\}$ corresponds bijectively with $image(j_2)$?

The concept of standard *pre-special group provides a full answer to these questions:*
(1) The set $\{\{a\} \subseteq G : \{a\} l.i., l(a)l(a) = 0 \in k_2(G)\}$ corresponds bijectively with $image(j_1)$.
(2) The set $\{\{a,b\} \subseteq G : \{a,b\} l.i., l(a)l(b) = 0 \in k_2(G)\}$ corresponds bijectively with $image(j_2)$.

It follows from Propositions 2.3 and 2.4 in [53] that $SG(F)$ is a standard special group, for every field F with $char(F) \neq 2$.

We have already established that every special group G is k-stable (see Proposition 6.3.7(iii)).

These suggest the following:

Question 7.3.11. *Is every special group G standard?*[1]

In the sequel, we will see the relevance of the subclass of standard pre-special groups. We invite the reader to recall Proposition 7.3.4.

`encoding-teo`

Theorem 7.3.12. *Let G be a k-stable pre-special group and denote $\mathcal{G} := Gal(G)$.*

i- *Let $\sigma \in \mathcal{G} \setminus \Phi(\mathcal{G})$ be such that $\sigma^2 = id$. Then $\{\Phi(\mathcal{G}), \sigma.\Phi(\mathcal{G})\}^\perp \subseteq G$ is a maximal saturated subgroup of G.*

ii- *Suppose that G is a* standard pre-special group*. Let $\sigma \in \mathcal{G} \setminus \Phi(\mathcal{G})$ be such that $\sigma^2 \neq id$ (so $\sigma^4 = id$). Then $\{\Phi(\mathcal{G}), \sigma.\Phi(\mathcal{G})\}^\perp \subseteq G$ is* not *a saturated subgroup of G.*

iii- *Suppose that G is a* standard special group*. The set of all classes of conjugacy of involutions $\sigma \in \mathcal{G} \setminus \Phi(G)$ corresponds to the set of all orderings (= maximal saturated subgroups) of G.*

iv- *Suppose that G is a* standard pre-special group*. Then we have an anti-isomorphism of complete lattices between the posets*

$$\{\Delta \subseteq G : \Delta \textit{ is a saturated subgroups of } G\}$$

and

$$\{T \subseteq \mathcal{G} : T \textit{ is a closed subgroup of } \mathcal{G} \textit{ (topologically) generated by involutions such that } \Phi(\mathcal{G}) \subseteq T\}$$

Proof.

i- Let $\bar{T} = \{\Phi(\mathcal{G}), \sigma\Phi(\mathcal{G})\}$.

<u>Claim:</u> To have that $\bar{T}^\perp \subseteq G$ is a *saturated* subgroup it is enough to prove the following: $\forall x, y \in G$ if $< x, y > \equiv < 1, xy >$, then $x \in \bar{T}^\perp$ or $y \in \bar{T}^\perp$.

<u>Proof of Claim:</u> Firstly we prove that $-1 \notin \bar{T}^\perp$: take any $x \notin \bar{T}^\perp$ (there is some x, as $\bar{T}^\perp \subseteq G$ has index 2) then as $< x, -x > \equiv < 1, -1 >$ it follows from assumption in the claim that $-x \in \bar{T}^\perp$ so if $-1 \in \bar{T}^\perp$ then $x = -1.(-x) \in \bar{T}^\perp$, a contradiction. Now let us prove that $\bar{T}^\perp$ is saturated: take any $a, b \in G$ such that $b \in D_G(< 1, a >)$, assume $a \in \bar{T}^\perp$ then we have to prove that $b \in \bar{T}^\perp$: as $(-a).a = -1 \notin \bar{T}^\perp$ then $-a \notin \bar{T}^\perp$ and as $< b, ba > \equiv < 1, a >$ we have $< b, -a > \equiv < 1, -ba >$ so, by the assumption in the claim, we get $b \in \bar{T}^\perp$.
Now we will prove that $\sigma^2 = id$ entails $\forall x, y \in G$ if $< x, y > \equiv < 1, xy >$ then $x \in \bar{T}^\perp$ or $y \in \bar{T}^\perp$:
We have three cases:
$*$ x (or y) is 1;
$*$ $x = y \neq 1$;
$*$ $x, y \neq 1$ and $x \neq y$.
There is nothing to proof in the first case. Now consider $x \in G \setminus \{1\}$ such that $< x, x > \equiv < 1, 1 >$: we must prove that $x \in \bar{T}^\perp$. Since G is k-stable, we have $l(x)l(x) = l(1)l(1) = 0$ then, by Theorem 7.3.8(i), there is a $S \subseteq \mathcal{G}$ a clopen normal subgroup such that $\mathcal{G}/S \cong \mathbb{Z}_4$ and

[1] We are unable to solve this question with the methods so far developed. We believe that to address this question, we will have to develop the theory of quadratic extensions of pre-special hyperfields.

$S \subseteq M_x$. Consider the quotient map $p_S : \mathcal{G} \twoheadrightarrow \mathcal{G}/S$ and write $\mathcal{G}/S = \{1/S, r/S, r^2/S, r^3/S\}$ then as $\sigma^2 = id$ we must have $\sigma/S \in \{1/S, r^2/S\}$. If $\sigma/S = 1/S$ then $\sigma \in S \subseteq M_x$ i.e. $< \sigma/\Phi(\mathcal{G}), x >= 0$ so $x \in \{\Phi(\mathcal{G}), \sigma\Phi(\mathcal{G})\}^{\perp}$. If $\sigma/S = r^2/S$ then $\sigma.r^2 = \sigma.r^{-2} \in S \subseteq M_x$ i.e. $< (\sigma.r^2)/\Phi(\mathcal{G}), x >= 0$ but

$$< (\sigma.r^2)/\Phi(\mathcal{G}), x >=< \sigma/\Phi(\mathcal{G}), x > + < r/\Phi(\mathcal{G}), x > + < r/\Phi(\mathcal{G}), x >=< \sigma/\Phi(\mathcal{G}), x >$$

then $< \sigma/\Phi(\mathcal{G}), x >= 0$ so $x \in \{\Phi(\mathcal{G}), \sigma\Phi(\mathcal{G})\}^{\perp}$. Now take $x, y \in G \setminus \{1\}$ with $x \neq y$ and $< x, y >\equiv< 1, xy >$ and supose $x \notin \bar{T}^{\perp}$ then we must prove that $y \in \bar{T}^{\perp}$. As $\{x, y\}$ is a two element l.i. set and $l(x)l(y) = l(1)l(xy) = 0$ we have, by Theorem 7.3.8(ii), some $D \subseteq \mathcal{G}$ a clopen normal subgroup such that $\mathcal{G}/D \cong \mathbb{D}_4$, $D \subseteq M_x \cap M_y$ and $M_{x.y}/D \cong \mathbb{Z}_4$. Consider the quotient morphism $p_D : \mathcal{G} \twoheadrightarrow \mathcal{G}/D$ and write

$$\mathcal{G}/D = \{1/D, r/D, r^2/D, r^3/D, s/D, sr/D, sr^2/D, sr^3/D\}$$

then, as $\sigma^2 = id$, we have $\sigma/D \notin \{r/D, r^3/D\}$. Let us prove that $\sigma/D \notin \{1/D, r^2/D\}$: as $< 1/\Phi(\mathcal{G}), x >=< r^2/\Phi(\mathcal{G}), x >= 0$ we have $\{id, r^2\} \subseteq M_x$ and as we selected $x \notin \{\Phi, \sigma\Phi\}^{\perp}$ we have $\sigma \notin M_x$ then if $\sigma/D = r^2/D$ then $\sigma.r^{-2} \in D \subseteq M_x$ so

$$\sigma = (\sigma.r^{-2}).r^2 \in D.M_x \subseteq M_x.M_x \subseteq M_x,$$

a contradiction; similarly $\sigma/D \neq 1/D$. So we have $\sigma/D \in \{s/D, sr/D, sr^2/D, sr^3/D\}$. Now, as $M_{x.y}/D \cong \mathbb{Z}_4$ we have $M_{x.y} = 1D \cup r^2D \cup rD \cup r^3D$ (see the proof of Theorem 7.3.8(ii)) and

$$\{M_x, M_y\} = \{1D \cup r^2D \cup sD \cup sr^2D, 1D \cup r^2D \cup srD \cup sr^3D\}.$$

If $M_x = 1D \cup r^2D \cup sD \cup sr^2D$ then as $\sigma \notin M_x$ we have $\sigma/D \notin \{s/D, sr^2/D\}$ so

$$\sigma/D \in \{sr/D, sr^3/D\} \subseteq M_y/D$$

then $\sigma \in M_y$ that is $y \in \{\Phi(\mathcal{G}), \sigma\Phi(\mathcal{G})\}^{\perp}$; similarly if $M_x = 1D \cup r^2D \cup srD \cup sr^3D$ then $y \in \{\Phi(\mathcal{G}), \sigma\Phi(\mathcal{G})\}^{\perp}$.

ii- Let $\bar{T} = \{\Phi(\mathcal{G}), \sigma\Phi(\mathcal{G})\}$.

Claim: To have that $\bar{T}^{\perp} \subseteq G$ *is not* a saturated subgroup it is enough to prove the following: $\exists x, c \in G \setminus \bar{T}^{\perp}$ such that $< x, c >\equiv< 1, xc >$.

Proof of Claim: If $-1 \in \bar{T}^{\perp}$ then $\bar{T}^{\perp} \subsetneq G$ so $G = D_G < 1, -1 >\nsubseteq \bar{T}^{\perp}$ so $\bar{T}^{\perp}$ is not a saturated subgroup. If $-1 \notin \bar{T}^{\perp}$ then take $x, c \in G \setminus \bar{T}^{\perp}$ such that $< x, c >\equiv< 1, xc >$ so we have $< c, -xc >\equiv< 1, -x >$, that is $c \in D_G < 1, -x >$ and $-x \in \bar{T}^{\perp}$: if $-x \notin \bar{T}^{\perp}$ then as $\bar{T}^{\perp} \subseteq G$ has index 2 $-1.\bar{T}^{\perp} = -x.\bar{T}^{\perp}$ so $x = -1. - x \in \bar{T}^{\perp}$; that is we established that there are $a(= -x) \in \bar{T}^{\perp}$ and $c \in D_G < 1, a >$ with $c \notin \bar{T}^{\perp}$: this means that $\bar{T}^{\perp}$ is not saturated.
Now we will prove that $\sigma^2 \neq id$ entails $\exists x, c \in G \setminus \bar{T}^{\perp}$ such that $< x, c >\equiv< 1, xc >$:
Take B any well ordered base of G and consider the composition

$$\mathcal{W}(B) \twoheadrightarrow \mathcal{W}(B)/\mathcal{V}(B) \overset{\cong}{\to} \mathcal{G}$$

and, by Lemma 7.1.10, *choose* any lifting $\widetilde{\sigma} \in \mathcal{W}(B)$ of $\sigma \in \mathcal{G}$. Since $\sigma^2 \neq id \in \mathcal{G}$ we get

$\widetilde{\sigma}^2 \in \Phi(B) \setminus \mathcal{V}(B)$. Since

$$\begin{aligned}\mathcal{V}(B) = Q_B^{\perp} &= [\{q_{ab}^B \in P_2(B) : l(a)l(b) = 0 \in k_2(G)\}]^{\perp} \\ &= \bigcap\{(q_{ab}^B)^{\perp} \subseteq \Phi(B) : a, b \neq 1, l(a)l(b) = 0\}\end{aligned}$$

we get $a, b \neq 1$ with $l(a)l(b) = 0 \in k_2(G)$ and $\widetilde{\sigma}^2 \in \Phi(B) \setminus (q_{ab}^B)^{\perp}$. There are two cases to consider: $a = b$ and $a \neq b$. In the first case $\{a\}$ is a singleton l.i. set and in the second $\{a, b\}$ is a two element l.i. set: consider any well ordered basis $B' = \{a_i' : i \in I\}$ *such that* $a = a_i$ for some $i \in I$ in the first case and, $a = a_i, b = a_j$ for some $i < j \in I$ in the second case. Now consider the isomorphism of change of basis $\mu_{B'B} : \mathcal{W}(B) \overset{\cong}{\to} \mathcal{W}(B')$ (see Lemma 7.2.3)) and take $\sigma' = \mu_{B'B}(\widetilde{\sigma}) \in \mathcal{W}(B')$. Then $\sigma' \in \mathcal{W}(B')$ is a lifting of $\sigma \in \mathcal{G}$ with respect to the epimorphism $\mathcal{W}(B') \twoheadrightarrow \mathcal{W}(B')/\mathcal{V}(B') \overset{\cong}{\to} \mathcal{G}$ (Lemma 7.1.10, again) and $\sigma'^2 \in \Phi(B') \setminus \mu_{B'B}[(q_{a,b}^B)^{\perp}] = \Phi(B') \setminus (q_{a,b}^{B'})^{\perp}$ (see Remark 7.2.4). As $l(a)l(b) = 0$, by the proof of the Theorem 7.3.8, we have $(q_{a_i,a_i}^B)^{\perp} = S_i' \cap \Phi(B')$ in first case and $(q_{a_i,a_j}^B)^{\perp} = D_{ij}' \cap \Phi(B')$ in the second case, then $\sigma'^2 \in \Phi(B') \setminus S_i'$ (resp. $\sigma'^2 \in \Phi(B') \setminus D_{ij}'$). A straightforward calculation with the group operation in $\mathcal{W}(B')$ gives $\sigma' \notin M_i' \subseteq \mathcal{W}(B')$ in the first case and $\sigma' \notin M_i' \cup M_j' \subseteq \mathcal{W}(B')$ in the second case, then applying $\mathcal{W}(B') \twoheadrightarrow \mathcal{G}$ we have $\sigma \notin M_{a_i} \subseteq \mathcal{G}$ (resp. $\sigma \notin M_{a_i} \cup M_{a_j} \subseteq \mathcal{G}$). Now recall that for each $y \in G \setminus \{1\}$ and each $\theta \in \mathcal{G} \setminus \Phi(\mathcal{G})$, $\theta \notin M_y$ iff $< \{\Phi(\mathcal{G}), \theta.\Phi(\mathcal{G})\}, y >= 1$ iff $y \notin \{\Phi(\mathcal{G}), \theta.\Phi(\mathcal{G})\}^{\perp}$. Then, since G is a standard pre-special group we have, in both cases, $1 \neq a, b$, $l(a)l(b) = 0 \in k_2(G)$, $a, b \notin \{\Phi(\mathcal{G}), \sigma.\Phi(\mathcal{G})\}^{\perp}$ and, in particular, since G is a k-stable pre-special group, $1 \in D_G(< a, b >)$ or, equivalently, $< a, b > \equiv < 1, ab >$.

iii- Recall that for *special groups* the maximal saturated subgroups are precisely the index 2 saturated subgroups so the result follows from items (i) and (ii).

iv- Let $\Delta \subseteq G$ be a saturated subgroup: as G is a *special group* $\Delta = \bigcap\{\Sigma \subseteq G : \Sigma \in X_{\Delta}\}$ where

$$X_{\Delta} = \{\Sigma \subseteq G : \Sigma \text{ is a maximal saturated subgroup and } \Delta \subseteq \Sigma\}$$

then, by Proposition 7.3.4,

$$\Delta^{\perp} = \bigvee\{\Sigma^{\perp} \subseteq \mathcal{G}/\Phi(\mathcal{G}) : \Sigma \in X_{\Delta}\};$$

by item (iii) $\Sigma^{\perp} = \{\Phi(\mathcal{G}), \sigma\Phi(\mathcal{G})\}$ for some $\sigma \in \mathcal{G} \setminus \Phi(\mathcal{G})$, $\sigma^2 = id$; take $T_{\Sigma} = \Phi(\mathcal{G}) \cup \sigma\Phi(\mathcal{G})$ then $T_{\Sigma} \subseteq \mathcal{G}$ is a closed (normal) subgroup such that $\Phi(\mathcal{G}) \subseteq T_{\Sigma}$ and all elements of $T_{\Sigma} \setminus \{1\}$ are involutions so

$$\bigvee\{T_{\Sigma} : \Sigma \in X_{\Delta}\} = closure([\{T_{\Sigma} : \Sigma \in X_{\Delta}\}])$$

is a closed subgroup of $\mathcal{G}$ that contains $\Phi(\mathcal{G})$ and is (topologically) generated by involutions. Now note that $T_{\Sigma}/\Phi(\mathcal{G}) = \{\Phi(\mathcal{G}), \sigma\Phi(\mathcal{G})\} = \Sigma^{\perp}$ and then

$$\begin{aligned}\Delta^{\perp} &= \bigvee\{\Sigma^{\perp} \subseteq \mathcal{G}/\Phi(\mathcal{G}) : \Sigma \in X_{\Delta}\} = \bigvee\{T_{\Sigma}/\Phi(\mathcal{G}) \subseteq \mathcal{G}/\Phi(\mathcal{G}) : \Sigma \in X_{\Delta}\} \\ &= (\bigvee\{T_{\Sigma} \subseteq \mathcal{G} : \Sigma \in X_{\Delta}\})/\Phi(\mathcal{G})\end{aligned}$$

as $q : \mathcal{G} \twoheadrightarrow \mathcal{G}/\Phi(\mathcal{G})$ gives an isomorphism of complete lattices between the set of closed subgroups of $\mathcal{G}$ which contains $\Phi(\mathcal{G})$ and the set of closed subgroups of $\mathcal{G}/\Phi(\mathcal{G})$.

Now take $T \subseteq \mathcal{G}$ a closed subgroup of $\mathcal{G}$ such that $\Phi(\mathcal{G}) \subseteq T$ and T is topologically generated by involutions. Write $I_T = \{\sigma \in T : \sigma \in \mathcal{G} \setminus \Phi(\mathcal{G}), \sigma^2 = id\}$ then, for each $\sigma \in I_T$, $\sigma\Phi(\mathcal{G}) \subseteq T$, $T_\sigma = \Phi(\mathcal{G}) \cup \sigma\Phi(\mathcal{G})$ is a closed (normal) subgroup of $\mathcal{G}$ and

$$T = closure([\bigcup\{T_\sigma : \sigma \in I_T\}]) = \bigvee\{T_\sigma : \sigma \in I_T\},$$

also $T_\sigma/\Phi(\mathcal{G}) = \{\Phi(\mathcal{G}), \sigma\Phi(\mathcal{G})\}$ and, by item (iv), $(T_\sigma/\Phi(\mathcal{G}))^\perp \subseteq G$ is a maximal saturated subgroup of G. Then we have

$$\begin{aligned}(T/\Phi(\mathcal{G}))^\perp &= ((\bigvee\{T_\sigma : \sigma \in I_T)/\Phi(\mathcal{G}))^\perp = (\bigvee\{T_\sigma/\Phi(\mathcal{G}) : \sigma \in I_T\})^\perp \\ &= \bigcap\{(T_\sigma/\Phi(\mathcal{G}))^\perp : \sigma \in I_T\}\end{aligned}$$

which is a saturated subgroup of G.

□

reduced-teo

Theorem 7.3.13. *Let G be a standard special group. Are equivalent*

i - G is "Pythagorean" or "almost reduced"[2].

ii - $Gal(G)$ is generated by involutions.

Proof. Note that the unique non-formally real Pythagorean special group (equivalently, $-1 \neq 1$) is $G = \{1\}$ and thus $Gal(G) = \{1\}$.

$(i) \Rightarrow (ii)$: The hypothesis means that $\{1\} \subseteq G$ is a saturated subset of G, then by item (iv) of the previous Proposition, $Gal(G)$ is generated by involutions.

$(ii) \Rightarrow (i)$: It follows the hypothesis that there is no continuous epimorphism $\mathcal{G}/\Phi(\mathcal{G}) \twoheadrightarrow \mathbb{Z}_4$. Since G is standard SG, for all $a \in G \setminus \{1\}$, $l(a)l(a) \neq 0 = l(1)l(1)$ and, since G is in particular k-stable, then for all $a \in G \setminus \{1\}$, is not the case $< a, a > \equiv < 1, 1 >$, that is: G is Pythagorean. □

Remark 7.3.14. *Another Galois theoretic characterization of the Pythagoreaness of G is*

$$\Phi(Gal(G)) = [Gal(G), Gal(G)].$$

teomain2

Theorem 7.3.15. *Let G be a standard special group. Consider the following*

i- G is not formally real.

ii- Every involution is is $\Phi(Gal(G))$.

iii- Every involution in $Gal(G)$ is central.

Then $(i) \Rightarrow (ii) \Rightarrow (iii)$ and if $card(Gal(G)) > 2$, then all are equivalent.

Proof. By Theorem 7.3.12(iii) G is formally real iff there is an involution $\sigma \in Gal(G) \setminus \Phi(Gal(G))$, so we get $(i) \Rightarrow (ii)$. As $Gal(G)$ is a $\mathcal{C}$-group we have $[\sigma^2, \tau] = 1$ and, since $\Phi(Gal(G)) = Gal(G)^2$ (pro-2-group), then $\Phi(Gal(G)) \subseteq center(Gal(G))$ so $(ii) \Rightarrow (iii)$. Now suppose $card(Gal(G)) > 2$: to prove $(iii) \Rightarrow (i)$ let us assume G formally real and note that any involution $\notin \Phi(Gal(G))$ *is not in* the center of $Gal(G)$. □

[2]I.e. for all $a \in G$, $< a, a > \equiv < 1, 1 >$ iff $a = 1$, but eventually $-1 = 1$.

7.4 The functorial behavior of Gal and SG-cohomology

We have developed the theme "basis change induced *isomorphisms*" in the general context of *pre-Special Groups*, as the fundamental step to get a *single* Galois group of a pre-special group. In this final section, we analyze some functorial behavior of the Gal construction of SG-theory and provide the first steps to a (profinite) "Galoisian" cohomology for the SG-theory, in an attempt to complete the "Milnor scenario" of Igr's ([52]) in abstract theories of quadratic forms.

7.4.1 From PSG to Galois groups

construPSGGAL-ct

7.4.1. Construction:

Let $f : G \to G'$ a pSG-homomorphism of pre-special groups.

Let $B'_1 = \{a'_k : k \in I'_1\}$ be an well ordered basis of $f[G]$ and extends it to $B' = \{a'_k : k \in I'\}$, an well ordered basis of G'. Now select *$a_k \in f^{-1}[\{a'_k\}], k \in I'_1$. Then the set $B_1 = \{a_i : i \in I'_1\} \subseteq G$ is linearly independent, now complete this to basis of G, $B = \{a_i : i \in I\}$: we just need to glue a well ordered basis of $ker(f)$.*

We have some induced functions:

(0) $f^0_{B,B'} : B' \to \mathcal{W}(B)$ is such that $f^0_{B,B'}(a'_k) = a_k$, if $a'_k \in B'_1$ and $f^0_{B,B'}(a'_k) = 1$, if $a'_k \in B' \backslash B'_1$.

(1) $f^{(1)}_{B,B'} : B \to P_2(B')$ is such that $f^1_{B,B'}(a_k) = a'_k$, if $a_k \in B_1$ and $f^1_{B,B'}(a_k) = 0$, if $a_k \in B \backslash B_1$.

(2) $f^{(2)}_{B,B'} : \{(a_i, a_j) \in B \times B : i, j \in I, i \le j\} \to P_2(B')$ is such that $f^2_{B,B'}(a_i, a_j) = a'_i.a'_j$, if $(a_i, a_j) \in B_1 \times B_1$ and $f^2_{B,B'}(a_i, a_j) = 0$, if $(a_i, a_j) \in B \times B \setminus B_1 \times B_1$.

Keeping the notation above, we have

GaltoSG-pr

Proposition 7.4.2. *The function $f^0_{B,B'} : B' \to \mathcal{W}(B)$ induces a continuous homomorphism $\bar{f}_{B,B'} : \mathcal{W}(B')/\mathcal{V}(B') \to \mathcal{W}(B)/\mathcal{V}(B)$.*

Proof. It follows from Proposition 7.1.6 and the definition of $f^0_{B,B'} : B' \to \mathcal{W}(B)$, that its image converges to $1 \in \mathcal{W}(B)$. Thus, by the universal property $\mathcal{W}(B')$ (Theorem 7.1.11), $f^0_{B,B'}$ extends uniquely to a continuous homomorphism of pro-2-groups $\hat{f}^0_{B,B'} : \mathcal{W}(B') \to \mathcal{W}(B)$.

Now, $f : G \to G'$ also induces a $\mathbb{Z}_2$-module homomorphism $\hat{f}^{(2)}_{B,B'} : P_2(B) \to P_2(B')$: this is just the unique $\mathbb{Z}_2$-linear extension of the induced map $f^{(2)}_{B,B'} : \{(a_i, a_j) \in B \times B : i, j \in I, i \le j\} \to P_2(B')$. Moreover, since $k_*(f) : k_*(G) \to k_*(G')$ is an Igr-morphism, then for each $a, b \in G$ such that $l(a)l(b) = 0 \in k_2(G)$, we have $l(fa).l(fb) = 0 \in k_2(G')$. From this we obtain that $\hat{f}^{(2)}_{B,B'}(q^B_{a,b}) = q^{B'}_{fa,fb}$ (see Proposition 7.2.2) and, therefore, $f^{(2)}_{B,B'}[Q(B)] \subseteq Q(B')$.

For each $a, b \in G$ and $\sigma' \in \mathcal{W}(B')$, we have

$$< \hat{f}^{(0)}_{B,B'}(\sigma'), q^B_{a,b} >=< \sigma', \hat{f}^{(2)}_{B,B'}(q^B_{a,b} >=< \sigma', q^{B'}_{fa,fb} > .$$

Thus $\hat{f}^{(0)}_{B,B'}[\mathcal{V}(B')] \subseteq \mathcal{V}(B)$ and then, $\hat{f}^0_{B,B'} : \mathcal{W}(B') \to \mathcal{W}(B)$ induces a unique continuous homomorphism of pro-2-groups $\bar{f}_{B,B'} : \mathcal{W}(B')/\mathcal{V}(B') \to \mathcal{W}(B)/\mathcal{V}(B)$.

□

Proposition 7.4.3. *Let $f : G \to G'$ be an injective pSG-morphism.*

i - Then $\hat{f}^0_{B,B'} : \mathcal{W}(B') \to \mathcal{W}(B)$ and $\bar{f}_{B,B'} : \mathcal{W}(B')/\mathcal{V}(B') \to \mathcal{W}(B)/\mathcal{V}(B)$ are surjective morphisms of pro-2-groups (thus they can be identified with projections*).*

ii - Let $f' : G'' \to G$ is an injective pSG-morphism. If B' is an well ordered basis of G' obtained by successive extensions of an well ordered basis B'_2 of $f \circ f'[G'']$ to B'_1, an well ordered basis of $f[G] \supseteq f \circ f'[G'']$, then applying the construction above described, we obtain

$\hat{f}^0_{B'',B'} = \hat{f}^0_{B'',B} \circ \hat{f}^0_{B,B'} : \mathcal{W}(B') \to \mathcal{W}(B'')$ and $\bar{f}^0_{B'',B'} = \bar{f}^0_{B'',B} \circ \bar{f}^0_{B,B'} : \mathcal{W}(B')/\mathcal{V}(B') \to \mathcal{W}(B'')/\mathcal{V}(B'')$

Proof.

i - By the injectivity hypothesis, we have $f^0_{B,B'}[B'] = B \cup \{1\} \subseteq \mathcal{W}(B)$, thus $\hat{f}^0_{B,B'} : \mathcal{W}(B') \to \mathcal{W}(B)$ is a continuous function with dense image from a compact space into a Hausdorff space. Therefore $\hat{f}^0_{B,B'}$ and $\bar{f}^0_{B,B'}$ are surjective continuous homomorphisms.

ii - It follows from a straightforward calculation that $f^0_{B'',B'} = \hat{f}^0_{B'',B} \circ f^0_{B,B'}$. Therefore, the uniqueness of extensions and the homomorphism theorem guarantees that $\hat{f}^0_{B'',B'} = \hat{f}^0_{B'',B} \circ \hat{f}^0_{B,B'}$ and $\bar{f}^0_{B'',B'} = \bar{f}^0_{B'',B} \circ \bar{f}^0_{B,B'}$.

□

7.4.2 From Galois Groups to PSG

Let G be a pre-special group an denote $\mathcal{G} = Gal(G)$. We have seen in Proposition 7.3.2 that there is a *canonical* isomorphism $\phi_G : \mathcal{G}/\Phi(\mathcal{G}) \overset{\cong}{\to} Hom(G, \mathbb{Z}_2)$ so we get a "perfect pairing" $\hat{\phi}_G : \mathcal{G}/\Phi(\mathcal{G}) \times G \to \mathbb{Z}_2$ and there is also a *canonical* bijection $G \cong \{T \subseteq \mathcal{G} : T$ is a closed normal subgroup of index $\leq 2\}$.

We will explain now the term "canonical" employed, starting with the following

Lemma 7.4.4.

i - Let G, G' be pre-special groups Then each continuous homomorphism $\theta : Gal(G') \to Gal(G)$ induces a $\mathbb{Z}_2$-module homomorphism $\check{\theta} : G \to G'$.

ii - The association above, $\theta \mapsto \check{\theta}$, determines a contravariant functor from the category from all pairs $(G, Gal(G))$, G a pre-special group, and continuous homomorphisms, into the category of $\mathbb{Z}_2$-modules.

Proof.

i - We have a $\mathbb{Z}_2$-homomorphism $\theta^* : Homcont(Gal(G), \mathbb{Z}_2) \to Homcont(Gal(G'), \mathbb{Z}_2)$, $\mu \mapsto \mu \circ \theta$. By Proposition 7.3.2(iii), we have $\mathbb{Z}_2$-isomorphisms $\psi_G, \psi_{G'}$. Combining the informations we define the $\mathbb{Z}_2$-homomorphism $\check{\theta} := \psi_{G'}^{-1} \circ \theta^* \circ \psi_G : G \to G'$.

ii - Note that $id^*_{\mathcal{G}} = id$, thus $\check{id}_{\mathcal{G}} = id_G$. Let $\theta' : Gal(G'') \to Gal(G')$ be a continuous homomorphism. Then we have $(\theta \circ \theta')^* = \theta'^* \circ \theta^*$, thus $(\theta \circ \theta')\check{} = \check{\theta}' \circ \check{\theta}$.

□

Remark 7.4.5. *Note that for any surjective continuous homomorphism $\theta : \mathcal{G}' \to \mathcal{G}$, we have that $\check{\theta} : G \to G'$ is an injective $\mathbb{Z}_2$-homomorphism.*

This suggest that the (sub)category of Galois groups and continuous epimorphisms is the "right" domain category of Galois groups. We have the following:

Proposition 7.4.6. *The functor described in the Lemma above restricts to a functor from the subcategory of Galois groups of standard pre-special groups (Definition above 7.3.9) and continuous epimorphisms to the category of standard pre-special groups and injective qSG-morphisms (i.e., the group homomorphisms that preserves $\equiv$, but that eventually does not preserves -1).*

Proof. Assume that G is a k-stable pre-special group and that G' is a standard pre-special group, we will prove that $\check{\theta}$ is a injective qSG-homomorphism from G to G'.

Since $\check{\theta} : G \to G'$ is a group homomorphism, it is enough to show that, for each $a, b \in G \setminus \{1\}$, $1 \in D_G < a, b > \Rightarrow 1' \in D_G < \check{\theta}(a), \check{\theta}(b) >$ and, since G, G' are k-stable pre-special group, this is equivalent to show $l(a)l(b) = 0 \in k_2(G) \Rightarrow l(\check{\theta}(a))l(\check{\theta}(b)) = 0 \in k_2(G')$. Now we have 2 cases to consider:

<u>$a = b$</u> : Since G is a k-stable pre-special group then, by Theorem 7.3.8(i), there exists $S \subseteq \mathcal{G}$ a closed normal subgroup with $\mathcal{G}/S \cong \mathbb{Z}_4$ and $S \subseteq M_a$. As $\theta : \mathcal{G}' \twoheadrightarrow \mathcal{G}$ is an *surjective* continuous homomorphism we have that the quotient map $\theta_S : \mathcal{G}'/\theta^{-1}[S] \to \mathcal{G}/S$ is an *isomorphism* so $\theta^{-1}[S] \subseteq \mathcal{G}'$ is a closed normal subgroup such that $\mathcal{G}'/\theta^{-1}[S] \cong \mathcal{G}/S \cong \mathbb{Z}_4$ and $\theta^{-1}[S] \subseteq \theta^{-1}[M_a] = M'_{\theta^\star(a)}$, where this last equality holds by the bijections in items (ii) and (iii) in Proposition 7.3.2 and the definition of $\check{\theta}$. Now, since G' is a standard pre-special group, we have $l(\check{\theta}(a))l(\check{\theta}(a)) = 0 \in k_2(G')$

<u>$a \neq b$</u> : As $\check{\theta}$ is an *injective* $\mathbb{Z}_2$-homomorphism, $\check{\theta}(a) \neq \check{\theta}(b)$. Since G is a k-stable pre-special group then, by Theorem 7.3.8(ii), there exists $D \subseteq \mathcal{G}$ a closed normal subgroup with $\mathcal{G}/D \cong \mathbb{D}_4$, $D \subseteq M_a \cap M_b$ and $M_{ab}/D \cong \mathbb{Z}_4$. As $\theta : \mathcal{G}' \twoheadrightarrow \mathcal{G}$ is an *surjective* continuous homomorphism we have that the quotient map $\theta_D : \mathcal{G}'/\theta^{-1}[D] \to \mathcal{G}/D$ is an *isomorphism* so $\theta^{-1}[D] \subseteq \mathcal{G}'$ is a closed normal subgroup such that $\mathcal{G}'/\theta^{-1}[D] \cong \mathcal{G}/D \cong \mathbb{D}_4$ and $\theta^{-1}[D] \subseteq \theta^{-1}[M_a \cap M_b] = M'_{\check{\theta}(a)} \cap M'_{\check{\theta}(b)}$. Now we check that $M'_{\check{\theta}(a)\check{\theta}(b)}/\theta^{-1}[D] \cong \mathbb{Z}_4$: as θ is an epimorphism $\theta[theta^{-1}[M_{ab}]] = M_{ab}$ so, as $M'_{\check{\theta}(a)\check{\theta}(b)} = M'_{\check{\theta}(ab)} = \theta^{-1}[M_{ab}]$ (because $\check{\theta}(a) \neq \check{\theta}(b)$ and there are exactly three maximal above $M'_{\check{\theta}(a)} \cap M'_{\check{\theta}(b)}$), we have an epimorphism $\theta_| : M'_{\check{\theta}(ab)} \twoheadrightarrow M_{ab}$ thus $ker(\theta_|) = \theta^{-1}[D] \subseteq M'_{\check{\theta}(ab)}$ and the quotient map $\theta_{|D} : M'_{\check{\theta}(ab)}/\theta^{-1}[D] \to M_{ab}/D$ is an *isomorphism* so $M'_{\check{\theta}(ab)}/\theta^{-1}[D] \cong M_{ab}/D \cong \mathbb{Z}_4$. Now, since G' is a standard pre-special group, we have $l(\check{\theta}(a))l(\check{\theta}(b)) = 0 \in k_2(G')$.

□

7.4.3 Towards a galoisian cohomology for SG-theory

Let G be a standard pre-special group. Since $\mathcal{G} = \mathrm{Gal}(G)$ is a profinite group, the Galois Cohomology is available for this subclass of pre-special groups. In particular, there is the graded cohomology ring $H^*(G) := H^*(\mathcal{G}, \{\pm 1\})$ where $\mathcal{G}$ act trivially on $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Therefore, at least some parts of Milnor's scenario for containing 3 graded rings related to quadratic forms theory of fields (with $char \neq 2$) is available for (standard) special groups: $W_*(G), k_*(G)$, and $H^*(G)$.

The result above just provides the initial step to establish cohomological methods in SG-theory.

Theorem 7.4.7. *As in the field case, consider $\mathbb{Z}_2 \cong \{\pm 1\}$ as a discrete $Gal(G)$-module endowed with the trivial action, i.e., $\sigma.a = a$, for all $\sigma \in Gal(G)$ and $a \in \mathbb{Z}_2$. Then $H_*(G) := H_*(Gal(G), \mathbb{Z}_2)$, is an Igr, endowed with the cup product. Moreover, there is a canonical isomorphism of pointed 2-groups $(G, -1) \cong (H^1(G), (-1))$.*

Proof. We write $\mathcal{G} := Gal(G)$. Just recall that:

$H^0(\mathcal{G}, \mathbb{Z}_2) = (\mathbb{Z}_2)^{\mathcal{G}} = Fix(\mathbb{Z}_2) = \mathbb{Z}_2$, since $\mathcal{G}$ is acting trivially on $\mathbb{Z}_2$.

For $H^1(\mathcal{G}, \mathbb{Z}_2) := CrossedHom(\mathcal{G}, \mathbb{Z}_2)/principalCrossedHom(\mathcal{G}, \mathbb{Z}_2)$, since $\mathcal{G}$ is acting trivially on $\mathbb{Z}_2$, we get

$$\begin{aligned}
principalCrossedHom(\mathcal{G},\mathbb{Z}_2) &:= \ \mathrm{Im}(\overline{\partial}_1)\\
&:= \{x:\mathcal{G}\to\mathbb{Z}_2 : x=\overline{\partial}_1 a \text{ for some } a\in\mathbb{F}_2\}\\
&= \{x:\mathcal{G}\to\mathbb{Z}_2 : \text{ there exist } \mathbb{F}_2\in\mathbb{F}_2 \text{ such that } x(\sigma)=\sigma a-a \text{ for all } \sigma\in\mathcal{G}\}\\
&= \{x:\mathcal{G}\to\mathbb{Z}_2 : \text{ there exist } a\in\mathbb{F}_2 \text{ such that } x(\sigma)=0 \text{ for all } \sigma\in\mathcal{G}\}\\
&= \{0\};
\end{aligned}$$

and

$$\begin{aligned}
CrossedHom(\mathcal{G},\mathbb{Z}_2) &:= \ \mathrm{Ker}(\overline{\partial}_2)\\
&:= \{x:\mathcal{G}\to\mathbb{Z}_2 : x \text{ is continuous and } x(\sigma\tau)=\sigma x(\tau)+x(\sigma) \text{ for all } \sigma,\tau\in\mathcal{G}\}\\
&= \{x:\mathcal{G}\to\mathbb{Z}_2 : x \text{ is continuous and } x(\sigma\tau)=x(\tau)+x(\sigma) \text{ for all } \sigma,\tau\in\mathcal{G}\}\\
&= Homcont(\mathcal{G},\mathbb{Z}_2).
\end{aligned}$$

Therefore $H^1(\mathcal{G},\mathbb{Z}_2)=Homcont(\mathcal{G},\mathbb{Z}_2)/\{0\}\cong Homcont(\mathcal{G},\mathbb{Z}_2)=Homcont(Gal(G),\mathbb{Z}_2)$.

On the other hand, by Proposition 7.3.2(iii) $\psi_G : G \overset{\cong}{\to} Homcont(Gal(G),\mathbb{Z}_2)$ as $\mathbb{Z}_2$-modules and, $-1\in G$ corresponds to a open subgroup of $Gal(G)$ with index ≤ 2, that corresponds to (-1) in $Homcont(Gal(G),\mathbb{Z}_2)$

□

It is natural ask if the Igr $H^*(Gal(G),\{\pm1\})$ is in the subcategory Igr_h: this depends of an analysis and more explicit description of $H^2(Gal(G),\{\pm1\})$. In particular, we will need to analyze the relationship between the equations $l(a)l(b)=0\in k_2(G)$ and $(a)\cup(b)=0\in H^2(Gal(G),\mathbb{Z}_2)$, for $a,b\in G$, in a standard pre-special group G. Related to this question is the existence of a Milnor like canonical arrow from the mod 2 k-theory graduated ring of G to the graduated ring of cohomology of G: $h(G):k_*(G)\to H^*(G)$.

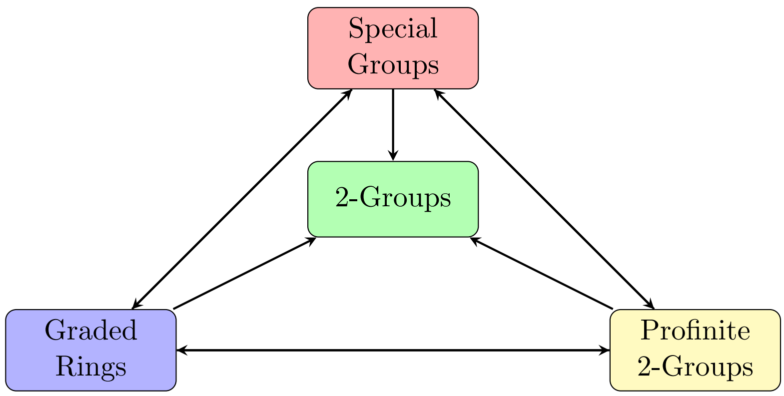
These generalizes some results in [2] to the context of (pre)special groups where they prove that the cohomology ring $H^*(Gal(F^{(3)}|F),\mathbb{Z}_2)$ contains the cohomology ring $H^*(Gal(F^s|F),\mathbb{Z}_2)$ as its subring generated by cup products of level 1 elements. Therefore, it could be interesting also analyze the properties of the subIgr generated in level 1 of the Igr $H^*(Gal(G),\{\pm1\})$, that is possibly a member of the subclass Igr_+.

Chapter 8

Conclusion and Further Works

After all, we return to our initial diagram

new-conclusion



In this present work, our main results concerns to the relation between special groups and graded rings, with much contribution of the theory of multirings/hyperfields. In fact, we established the result of Arason-Pfister Hauptsatz for every special group (Theorem 6.3.2), as an application of "multialgebraic methods" here introduced.

In Chapter 7 we started the investigation of the relations between special groups and profinite 2-groups, towards completing the initial diagram above.

After that, we glance at these roads to follow:

1. We intend to analyze further the introduced notions of formally real semigroups, formally real multirings and quadratic multirings.

2. With Example 2.5.15 as a prototype, specialize the study of quadratic multirings where every element is the product of a non-zero divisor and an idempotent. This could give some hint about the structure of invertible elements in real semigroups, which until today is not known to be a reduced special group in general.

3. In [25] is constructed a von Neumann hull functor from multiring category and that, when restricted to in semi-real rings, it commutes with real semigroup functor. This allows us to obtain some quadratic forms properties of a semi-real ring by looking to its von Neumann regular hull. It would be interesting to determine what kind of property in the von Neumann hull of a quadratic multiring return to the original structure.

4. The definition and analysis of the structure of Witt ring of more general quadratic structures (non only obtained from special groups): this subject have already appeared in Section 4 of Chapter 2, in connection with [37].

5. Extension of the K-theory framework to more general multirings (for example, to VN-multirings) with quadratic flavour.

6. Compare graded K-theory with graded Witt ring for VN-real semigroups as in the field case (Milnor [52]) and special groups (Dickmann-Miraglia [28]).

7. In the hyperfield case, investigate the extension of the concept of Galois group to hyperfields, comparing the Galois cohomology ring and analyse the existence of some canonical arrow from K-theory to this cohomology ring, in an attempt to recover the Milnor's Conjecture available in the classic algebraic quadratic forms context ([57], [20], [21]).

8. The next steps in the program of study algebraic extensions of superfields are a development of Galois theory and Galois cohomology theory, envisaging application to other mathematical theories as abstract structures of quadratic forms and real algebraic geometry ([24],[17],[18]): some parts of this program are under development in [16] and [14].

9. In the vein of the previous item, we will pursue, in particular, further developments of the theory of quadratic extensions of hyperfields and superfields, envisaging the description of Galois groups of special hyperfields "from below". We intend apply this description to obtain further information on the graded cohomology ring of a special group and provide a more complete development of cohomological methods in SG-theory, applying this to obtain a possible obstruction for every reduced SG to satisfy Marshall's conjecture.

10. Since the theory of superfields/hyperfields and the abstract theories of quadratic forms of Special Groups [28] and of Real Semigroups [33] are (or can be seen as) first-order theories, we wonder about other possible model-theoretic results in these theories. In connection with this, we plan to develop an order theory of superfields and analyze some candidates for notions of real closed superfields in such a way that we may address the questions: (i) the class of real closed superfields admits quantifiers elimination or is model-complete (according to a convenient choice of language)?; (ii) any reasonably ordered superfield admits an essentially unique real closure?

11. It could be interesting describe and explore an alternative notion of algebraically closed multifield based on an alternative notion of of root of a polynomial, taking in account factorizations, for example, if $p(x) \in (x-b)q(x)$ for some $q(x)$, then b can be seem as a root of $p(x)$: by Theorem 7 in [6], this in fact *coincide* with the other notion of root of a polynomial $p(x) \in F[x]$ whenever F is a hyperfield.

12. In [55] was started the development of a identity theory and a universal algebra like theory for multi structures. However, a full model theory of multi structures, in the vein of Chapter 1 of [26], should be an object of interest (as the present work suggests) and it is seems to be unknown.

13. Examples 3.6.16 and 3.7.7 reveals the necessity of some computational implementation in order to ease and accelerate the calculations with algebraic extensions of superfields: in [13], we start a proposal towards this subject.

Bibliography

[1] Jiří Adámek, J Adamek, J Rosicky, et al. *Locally presentable and accessible categories*, volume 189. Cambridge University Press, 1994.

[2] A. Adem, D. B. Karagueuzian, and J. Mináč. On the cohomology of Galois groups determined by Witt rings. *Advances in Mathematics*, (148):105—-160, 1999.

[3] Madeline Al Tahan, Sarka Hoskova-Mayerova, and Bijan Davvaz. Some results on (generalized) fuzzy multi-hv-ideals of hv-rings. *Symmetry*, 11(11):1376, 2019.

[4] R Ameri, M Eyvazi, and S Hoskova-Mayerova. Advanced results in enumeration of hyperfields. *Aims Mathematics*, 5(6):6552–6579, 2020.

[5] R Ameri, A Kordi, and S Hoskova-Mayerova. Multiplicative hyperring of fractions and coprime hyperideals. *Analele Universitatii" Ovidius" Constanta-Seria Matematica*, 25(1):5–23, 2017.

[6] Reza Ameri, Mansour Eyvazi, and Sarka Hoskova-Mayerova. Superring of polynomials over a hyperring. *Mathematics*, 7(10):902, 2019.

[7] J. Arason and A. Pfister. Beweis des Krullschen Durschnittsatzes fur den Wittring. *Inventiones Mathematicae*, 12:173–176, 1971.

[8] Francis Borceux. *Handbook of categorical algebra: volume 1, Basic category theory*, volume 1. Cambridge University Press, 1994.

[9] Herivelto Borges and Eduardo Tengan. *Algebra Comutativa em Quatro Movimentos-Projeto Euclides*. Rio de Janeiro: IMPA, 2015.

[10] Marcelo E Coniglio, Aldo Figallo-Orellano, and Ana C Golzio. Non-deterministic algebraization of logics by swap structures. *arXiv preprint arXiv:1708.08499*, 2017.

[11] B Davvaz and T Musavi. Codes over hyperrings. *Matematicki Vesnik*, 68(1):26–38, 2016.

[12] Kaique Matias de Andrade Roberto. Multirings and the chamber of secrets: relationships between abstract theories of quadratic forms. Master's thesis, Universidade de São Paulo, 2019.

[13] Kaique Matias de Andrade Roberto, Ana Luiza da Conceição Tenório, Hugo Rafael de Oliveira Ribeiro, and Hugo Luiz Mariano. Algebraic Extensions of Superfields: some calculations. *in preparation*, 2023.

[14] Kaique Matias de Andrade Roberto, Ana Luiza da Conceição Tenório, Hugo Rafael de Oliveira Ribeiro, and Hugo Luiz Mariano. Galois Theory of Hyperfields, I. *in preparation*, 2023.

[15] Kaique Matias de Andrade Roberto, Hugo Rafael de Oliveira Ribeiro, and Hugo Luiz Mariano. On algebraic extensions and algebraic closures of superfields. *Preliminary version in https://arxiv.org/pdf/2208.08537. Submitted*, 2022.

[16] Kaique Matias de Andrade Roberto, Hugo Rafael de Oliveira Ribeiro, and Hugo Luiz Mariano. Quadratic extensions of special hyperfields and the general Arason-Pfister Hauptsatz. *Preliminary version in https://arxiv.org/abs/2210.03784. Submitted*, 2022.

[17] Kaique Matias de Andrade Roberto, Hugo Rafael de Oliveira Ribeiro, and Hugo Luiz Mariano. Quadratic structures associated to (multi) rings. *Categories and General Algebraic Structures*, 16(1):105–141, 2022.

[18] Kaique Matias de Andrade Roberto and Hugo Luiz Mariano. K-theories and free inductive graded rings in abstract quadratic forms theories. *Categories and General Algebraic Structures*, 17(1):1–46, 2022.

[19] Kaique Matias de Andrade Roberto and Hugo Luiz Mariano. On superrings of polynomials and algebraically closed multifields. *Journal of Pure and Applied Logic*, 9(1):419–444, 2022.

[20] Kaique Matias de Andrade Roberto and Hugo Luiz Mariano. Galois groups of pre special hyperfields, I. *in preparation*, 2023.

[21] Kaique Matias de Andrade Roberto and Hugo Luiz Mariano. Inductive Graded Rings associated to Quadratic Multirings. *in preparation*, 2023.

[22] Arileide Lira de Lima. *Les groupes speciaux. Aspects algebriques et combinatoires de la theorie des espaces d'ordres abstraits.* PhD thesis, Université Paris VII, France, 1996.

[23] Hugo Rafael de Oliveira Ribeiro. *Anel de Witt para semigrupos reais, envoltória von Neumann e B-pares.* PhD thesis, Universidade de São Paulo, Brazil, 2021.

[24] Hugo Rafael de Oliveira Ribeiro, Kaique Matias de Andrade Roberto, and Hugo Luiz Mariano. Functorial relationship between multirings and the various abstract theories of quadratic forms. *São Paulo Journal of Mathematical Sciences*, 16:5–42, 2022.

[25] Hugo Rafael de Oliveira Ribeiro and Hugo Luiz Mariano. von Neumann regular hyperrings and applications to real reduced multirings. *arXiv preprint arXiv:2101.06527. Submitted*, 2022.

[26] Razvan Diaconescu. *Institution-independent model theory.* Springer Science & Business Media, 2008.

[27] Maximo Dickmann and Francisco Miraglia. On quadratic forms whose total signature is zero mod 2^n: Solution to a problem of M. Marshall. *Inventiones mathematicae*, 133(2):243–278, 1998.

[28] Maximo Dickmann and Francisco Miraglia. *Special groups: Boolean-theoretic methods in the theory of quadratic forms.* Number 689 in Memoirs AMS. American Mathematical Society, 2000.

[29] Maximo Dickmann and Francisco Miraglia. Lam's conjecture. In *Algebra Colloquium*, pages 149–176. Springer-Verlag, 2003.

[30] Maximo Dickmann and Francisco Miraglia. Algebraic k-theory of special groups. *Journal of Pure and Applied Algebra*, 204(1):195–234, 2006.

[31] Maximo Dickmann and Francisco Miraglia. Quadratic form theory over preordered von Neumann-regular rings. *Journal of Algebra*, 319(4):1696–1732, 2008.

[32] Maximo Dickmann and Francisco Miraglia. *Faithfully quadratic rings*. Number 1128 in Memoirs AMS. American Mathematical Society, 2015.

[33] Maximo Dickmann and Alejandro Petrovich. Real semigroups and abstract real spectra. i. *Contemporary Mathematics*, 344:99–120, 2004.

[34] D. P. Ellerman. Sheaves of structures and generalized ultraproducts. *Annals of Mathematical Logic*, 7(2):163–195, 1974.

[35] Ryszard Engelking. *General Topology*. Heldermann Verlag, 1989.

[36] Michael D. Fried and Moshe Moshe Jarden. *Field Arithmetic*. Springer, 2008.

[37] Pawel Gladki and Krzysztof Worytkiewicz. Witt rings of quadratically presentable fields. *Categories and General Algebraic Structures*, 12(1):1–23, 2020.

[38] Ana Claudia Golzio. A brief historical survey on hyperstructures in algebra and logic. *South American Journal of Logic*, 2018.

[39] Kenneth Hoffman and Ray Kunze. *Linear algebra*. Englewood Cliffs, New Jersey, 1971.

[40] Werner Hürlimann. Cooper and lam's conjecture for generalized bell ternary quadratic forms. *Journal of Number Theory*, 158:23–32, 2016.

[41] Jaiung Jun. Algebraic geometry over hyperrings. *Advances in Mathematics*, 323:142–192, 2018.

[42] Bruno Kahn. La conjecture de Milnor (d'apres V. Voevodsky). *Astérisque*, 245:379–418, 1997.

[43] Tsit-Yuen Lam. *Introduction to quadratic forms over fields*, volume 67. American Mathematical Soc., 2005.

[44] Saunders Mac Lane. *Categories for the working mathematician*, volume 5. Springer Science & Business Media, 2013.

[45] Hugo Luiz Mariano, Hugo Rafael de Oliveira Ribeiro, and Kaique Matias de Andrade Roberto. *Uma Jornada pelas Teorias Algébricas de Formas Quadráticas*. Editora da Física, 2021.

[46] Murray Marshall. *Abstract Witt rings*. Kingston, Ont.: Queen's University, 1980.

[47] Murray Marshall. Real reduced multirings and multifields. *Journal of Pure and Applied Algebra*, 205(2):452–468, 2006.

[48] Murray A Marshall. *Spaces of orderings and abstract real spectra*. Lecture Notes in Mathematics 1636, Springer, 1996.

[49] Ch G Massouros. Theory of hyperrings and hyperfields. *Algebra and Logic*, 24(6):477–485, 1985.

[50] Christos G Massouros and Gerasimos G Massouros. On join hyperrings. In *Proceedings of the 10th International Congress on Algebraic Hyperstructures and Applications, Brno, Czech Republic*, pages 203–215, 2009.

[51] Geronimos G Massouros and Christos G Massouros. Homomorphic relation on hyperingoinds and join hyperrings. *Ratio Mathematica*, 13(1):61–70, 1999.

[52] John Milnor. Algebraic k-theory and quadratic forms. *Inventiones mathematicae*, 9(4):318–344, 1970.

[53] Ján Minác and Michel Spira. Witt rings and galois groups. *Annals of mathematics*, pages 35–60, 1996.

[54] Anastase Nakassis. Recent results in hyperring and hyperfield theory. *International Journal of Mathematics and Mathematical Sciences*, 11, 1988.

[55] Cosmin Pelea and Ioan Purdea. Multialgebras, universal algebras and identities. *Journal of the Australian Mathematical Society*, 81(1):121–140, 2006.

[56] Luis Ribes and Pavel Zalesskii. *Profinite groups*. Springer, 2000.

[57] Kaique Matias de Andrade Roberto and Hugo Luiz Mariano. Inductive graded rings, hyperfields and quadratic forms. *arXiv preprint arXiv:2307.01674*, 2023.

[58] Oleg Viro. Hyperfields for Tropical Geometry I. Hyperfields and dequantization. *arXiv preprint arXiv:1006.3034*, 2010.

[59] A Wadsworth. Merkurjev's elementary proof of Merkurjev's theorem. In *Applications of Algebraic K-theory to Algebraic Geometry and Number Theory, Parts I, II*, volume 55, pages 741–776, Boulder, Colorado, 1983. American Mathematical Society, Contemporary Mathematics.

Index