Spring 4-4-2013

The Level of Fields and Division Rings

Alex Martin
alexmartin8907@gmail.com

THE LEVEL OF FIELDS AND DIVISION RINGS

by

Alex Martin

B.A., Northwestern University, 2011

A Research Paper
Submitted in Partial Fulfillment of the Requirements for the
Master of Science Degree

Department of Mathematics
in the Graduate School
Southern Illinois University Carbondale
May, 2013

RESEARCH PAPER APPROVAL

THE LEVEL OF FIELDS AND DIVISION RINGS

By

Alex Martin

A Research Paper Submitted in Partial

Fulfillment of the Requirements

for the Degree of

Masters of Science

in the field of Mathematics

Approved by:

Dr. Robert Fitzgerald, Chair

Dr. Jerzy Kocik

Dr. Philip Feinsilver

Graduate School
Southern Illinois University Carbondale
April 2013

TABLE OF CONTENTS

INTRODUCTION

The main focus of this paper will be to construct a division ring R of arbitrary level where the level is the smallest natural number n such that -1 is the sum of n square-products in R. To start, we will examine the somewhat analagous case of the level of a (commutative) field F with the help of some basic results in the area of quadratic forms. We will then shift our attention to the notion of orderings on division rings, and actually construct a classic class of examples of ordered division rings. In the final chapter, we will, as previously stated, construct a division ring of arbitrary level, and provide a proof that this division ring is as we claim.

CHAPTER 1

QUADRATIC FORMS AND THE LEVEL OF FIELDS

The material for Chapter 1 is adapted from [1]

1.1 QUADRATIC FORMS

Before we begin working with division rings, it would be helpful to first introduce some analagous results in the field case. We would like to eventually introduce Pfister's Level Theorem which states that the level of a field is either ∞ or a power of 2, that is, either -1 is not a sum of squares or is a sum of 2^n squares (but not fewer) where $n \in \mathbb{N}$. Before doing so, we should first examine some useful preliminary results on quadratic forms.

To start, we should formally introduce the notion of level with the following two definitions.

Definition. For any integer $m \geq 1$, we write $D(m) = D_F(m)$ for the set $D_F(m\langle 1\rangle)$ (where $m\langle 1\rangle$ is the diagonal quadratic form $a_1^2 + a_2^2 + \cdots a_m^2$ with $a_i \in F$) which consists of all nonzero elements of F that are sums of m squares in F. If necessary, we take $D(0)$ to be the empty set, and set $D(\infty) = \cup_{m\in\mathbb{N}} D(m)$, the set of all sums of squares. Thus, we have an ascending chain $D(0) \subseteq F^2 = D(1) \subseteq D(2) \subseteq \ \cdots$.

Definition. We say that $a \in \dot{F}$ (where $\dot{F} := F - \{0\}$) has length n (written $len(a) = len_F(a) = n$) if $a \in D_F(n) \setminus D_F(n-1)$. If $a \in \dot{F} \setminus D_F(\infty)$ (that is, a is not a sum of squares), we write $len(a) = \infty$. The *level* of a field F, denoted by $s(F)$, is defined to be $len(-1)$. In other words, $s(F)$ is the smallest natural number n such that -1 is a sum of n squares in F.

We want to show that $1 + x_1^2 + \cdots + x_n^2$ cannot be a sum of n squares in $F(x_1, \ldots, x_n)$, and (similarly) $x_0^2 + x_1^2 + \cdots + x_n^2$ cannot be a sum of n squares in $F(x_0, x_1, \ldots, x_n)$. This result is a consequence of the Second Representation Theorem, and proving these results requires a hefty amount of work that comes in the form of a few preliminary results. To start, let us introduce the Cassels-Pfister Theorem.

Theorem 1.1.1. *Let γ be a (regular) quadratic form over F, and let $p(x) \in F[x] \cap D_{F(x)}(\gamma)$. Then,*

1. *$p(x)$ is already represented by γ over $F[x]$, and*

2. *if $e \in F$ is such that $p(e) \neq 0$, then $p(e) \in D_F(\gamma)$.*

Before we start the proof of this theorem, we should introduce some new terminology.

Definition. Let γ be a quadratic form over the field F. We say that γ is *isotropic* over F if there exists some $a_i \in F$ with at least one $a_i \neq 0$ such that $\gamma(a_1, \ldots, a_n) = 0$. We say that γ is *anisotropic* otherwise. We will take the following as fact for the upcoming proof: If γ is isotropic over F, γ would contain the subform $\langle 1, -1 \rangle (= x^2 - y^2)$.

Proof. It is easy to see that (1) $\Rightarrow$ (2) by a simple substitution so we will only need to show that the first conclusion holds. Let us assume that γ is a diagonal form $\langle a_1, \ldots, a_n \rangle$ $(a_i \in \dot{F})$. We should consider both the isotropic and anisotropic cases for γ. If γ is isotropic over F, γ would contain the subform $\langle 1, -1 \rangle$ (as in the previous definition.) From the identity

$$p(x) = [(p(x) + 1)/2]^2 - [(p(x) - 1)/2]^2 \in F[x]$$

we quickly see that (1) holds.

Now consider the case in which γ is anisotropic. By the hypothesis, we have

$$p(x) = a_1(f_1(x)/f_0(x))^2 + \cdots + a_n(f_n(x)/f_0(x))^2, \tag{1.1}$$

where $f_0, \ldots, f_n \in F[x]$, with $f_0 \neq 0$. We assume that equation (1.1) is chosen so that $\deg f_0$ is minimal. We wish to show that $\deg f_0$ must be zero.

For the sake of contradiction, let us assume that $\deg f_0 > 0$. Now consider the diagonal form $\langle -p(x), a_1, \ldots, a_n \rangle$ over a field $E = F(x)$, and associate with it the symmetric bilinear form B. To reach our desired contradiction, we want to produce an isotropic vector $h = (h_0, \ldots, h_n)$ where $h_i \in F[x]$ and $h_0 \neq 0$ with $\deg h_0 < \deg f_0$. To construct this particular h, we first divide all the f_i $(0 \leq i \leq n)$ by f_0:

$$f_i = f_0 g_i + r_i, \quad \text{where } r_i = 0 \text{ or } \deg r_i < \deg f_0.$$

Note that, for $i = 0$, we have $g_0 = 1$, $r_0 = 0$, and $g_i, r_i \in F[x]$. We now have the following three vectors in E^{n+1}:

$$f = (f_0, \ldots, f_n), \quad g = (g_0, \ldots, g_n), \quad \text{and} \quad r = (r_0, \ldots, r_n),$$

which are all related by the vector equation $f = f_0 g + r$. If $r = 0$, then f_0 divides all the f_i in equation (1.1) and we would arrive at a new solution with $f_0 = 1$. Therefore, let us assume that $r \neq 0$.

Before we construct h, we should first recall the notion of a bilinear form. A *bilinear form* on a vector space V is a function $B : V \times V \to F$ (where F is our desired field of scalars) which is linear in each argument, that is,

1. $B(u + v, w) = B(u, w) + B(v, w)$

2. $B(u, v + w) = B(u, v) + B(u, w)$

3. $B(\lambda u, v) = B(u, \lambda v) = \lambda B(u, v)$

where $u, v, w \in V$ and $\lambda \in F$.

With this notion of a bilinear form in mind, we may now construct our desired h. We set

$$h = \alpha f + \beta g = (h_0, \ldots, h_n) \quad (\alpha, \beta \in F[x]),$$

subject to the condition

$$0 = B(h, h) = \beta[2\alpha B(f, g) + \beta B(g, g)].$$

where the function B is a bilinear form. This equation is satisfied by $\alpha := B(g,g)$ and $\beta = -2B(f,g)$. With these choices of α and β, we have

$$h_0 = B(g,g)f_0 - 2B(f,g) = B(f_0g - 2f, g) = -B(f+r, g).$$

Thus,

$$f_0h_0 = -B(f+r, f-r) = B(r,r) = \sum_{i=1}^{n} a_i r_i(x)^2 \neq 0,$$

since $\gamma = \langle a_1, \ldots, a_n \rangle$ is anisotropic over F. Hence, we have $h_0 \neq 0$ and $\deg h_0 < \deg f_0$, as desired. □

As a consequence, we have the following corollary:

Corollary 1.1.2. *Let γ be a quadratic form over F, and let $X = (x_1, \ldots, x_s)$ be a set of (commuting) independent indeterminates over F. Let $p(X) \in F(X)$ and $e = (e_1, \ldots, e_s) \in F^s$ be such that $p(e)$ is defined and not equal to zero. Then*

$$p(X) \in D_{F(X)}(\gamma) \Rightarrow p(e) \in D_F(\gamma).$$

Proof. With the assumption that $p(e) \neq 0$, we can write $p(X)$ in the form $f(X)/g(X)$, where $f, g \in F[X]$ with $g(e) \neq 0$ and $f(e) \neq 0$. By our hypothesis, γ represents $p(X)$, and therefore, γ also represents $f(X)g(X) = p(X)g(X)^2$ over $F(X)$. If we can show that γ represents $f(e)g(e)$ over F, then γ will also represent $[f(e)g(e)]/g(e)^2 = f(e)/g(e) = p(e)$ over F. Because of this, we can assume that $p(X)$ is a polynomial in the indeterminates $x_1, \ldots, x_s$.

We now proceed by induction on s. The base case $s = 1$ is just part (2) of Theorem 1.1.1. For $s > 1$, we can view γ as a form over $F' = F(x_1, \ldots, x_{s-1})$. Since γ represents $p(x_1, \ldots, x_s)$ over $F'(x_s)$, γ represents $p(x_1, \ldots, x_{s-1}, e_s)$ over F' by part (2) of Theorem 1.1.1. By the inductive hypothesis, it follows quickly that γ represents $p(e_z \ldots, e_{s-1}, e_s) = p(e)$ over F. □

The Theorem 1.1.1 and Corollary 1.1.2 are crucial to the proof of the Second Representation Theorem (which will be subsequently stated) which we need in order to arrive at our desired result on sums of squares.

Theorem 1.1.3. *Let* $\gamma = \langle a_1, \ldots, a_n \rangle = a_1x_1^2 + \cdots a_nx_n^2$ *be an anisotropic form over* F*, where* $n \geq 1$*. Let* $\varphi = \langle a_2, \ldots, a_n \rangle = a_2x_2^2 + \cdots a_nx_n^2$*, and* $d \in \dot{F}$*. Then, for a single indeterminate* x*,*

$$d \in D_F(\varphi) \Longleftrightarrow a_1x^2 + d \in D_{F(x)}(\gamma).$$

Proof. Let us first assume that $d \in D_F(\varphi)$, and consider $\gamma = \langle a_1 \rangle \perp \varphi$ as an orthogonal decomposition over $F(x)$. The first part of the decomposition, namely $\langle a_1 \rangle$, represents a_1x^2 over $F(x)$. The second part, namely φ, represents d which is already over F. Thus, γ represents $a_1x^2 + d$, as desired.

Conversely, let us assume that $a_1x^2 + d \in D_{F(x)}(\gamma)$. By Theorem 1.1.1, there exists an equation

$$\mathrm{a}_1x^2 + d \in D_{F(x)}(\gamma) = a_1f_1(x)^2 + \cdots + a_nf_n(x)^2, \quad \text{where } f_i \in F[x]. \quad (1.2)$$

We know that γ is anisotropic over F, and the left-hand side in equation (1.2) is of degree 2. Examining the leading coefficients of all the f_i's, we see that $\deg f_i \leq 1$ for all i. With this in mind, we write $f_1(x) = a + bx$, where $a, b \in F$. Let $c \in F$ be a solution for one of the equations $a + bx = \pm x$. Substituting c into equation (1.2), we get the following:

$$a_1c^2 + d = a_1(\pm c)^2 + a_2f_2(c)^2 + \cdots + a_nf_n(c)^2.$$

Subtracting the term a_1c^2 from each side, we see that $d \in D_F(\varphi)$, as desired. □

The following is the first of two direct consequences of the Second Representation Theorem.

Corollary 1.1.4. *Let $n \geq 1$, and let F be a field in which -1 is not a sum of $n-1$ squares (e.g., F can be a formally real field, that is, a field in which -1 is not a sum of squares). If $d \in \dot{F}$ and $x^2 + d$ is a sum of n squares in $F(x)$, then d is a sum of $n-1$ squares in F.*

Extending Corollary 1.1.4 by induction on n, we finally arrive at our desired result in the form of the following corollary which is a key result for the final theorem of this paper.

Corollary 1.1.5. *For F as in Corollary 1.1.4, $1 + x_1^2 + \cdots + x_n^2$ cannot be a sum of n squares in $F(x_1, \ldots, x_n)$. Similarly, $x_0^2 + x_1^2 + \cdots + x_n^2$ cannot be a sum of n squares in $F(x_0, x_1, \ldots, x_n)$.*

1.2 SUMS OF SQUARES AND THE LEVEL OF A FIELD

In this section, we will wrap up our work with fields with the conclusion that the level of a field F happens to be either a power of 2 or ∞ (in which case -1 is not a sum of squares in F). This result comes in the form of Pfister's Level Theorem. Before we arrive at this conclusion, we should first examine a few other results on sums of squares in a field F.

We will need the following lemma prior to introducing the next theorem.

Lemma 1.2.1. *Let $m = 2^n$ and $c = c_1^2 + \cdots + c_m^2$, where $c_i \in F$. Then there exists an $m \times m$ matrix $S \in \mathbb{M}_m(F)$ with first row $c_1, \ldots, c_m$ such that $S \cdot S^t = S^t \cdot S = c \cdot I_m$ (where "t" denotes the transpose).*

Proof. There are two cases of c to consider, namely, $c = 0$ and $c \neq 0$. For $c = 0$, we first assume that all $c_i = 0$. In this case, we can choose S to be the zero matrix, and we quickly arrive at the desired conclusion. Now, for $c \neq 0$, assume (without loss of generality) that $c_1 \neq 0$, and consider the row matrix $(c_1, \ldots, c_m) = R$. If we set $S = c_1^{-1} \cdot R^t \cdot R$, we see that S does indeed have its first row equal to the row matrix R. Furthermore,

$$S \cdot S^t = c_1^{-2} \cdot R^t \cdot RR^t \cdot R = 0,$$

since $R \cdot R^t = c = 0$. Through a similar computation, we see that $S^t \cdot S = 0$. Thus, our conclusion holds for $c = 0$.

We now assume that $c \neq 0$ and proceed with an inductive argument on n. We begin by splitting the set $c_1, \ldots, c_m$ into two equal parts. Next, re-label the elements in these two equal parts as $a_1, \ldots, a_{2^{n-1}}$ and $b_1, \ldots, b_{2^{n-1}}$, respectively. Now, write $a = \sum a_i^2$ and $b = \sum b_i^2$, so $s = a + b$. Notice that a and b cannot both be zero since we assumed that $c \neq 0$. Without loss of generality, let us assume that $a \neq 0$. By our inductive hypothesis, there exist square matrices A, B of size 2^{n-1}, such that

$$A \cdot A^t = A^t \cdot A = a \cdot I_{2^{n-1}} \quad \text{and} \quad B \cdot B^t = B^t \cdot B = b \cdot I_{2^{n-1}}.$$

Furthermore, A has first row $(a_1, \ldots, a_{2^{n-1}})$ and B has first row $(b_1, \ldots, b_{2^{n-1}})$. Now, we use A and B to construct our S in the following way:

$$S = \begin{pmatrix} A & B \\ -a^{-1} A^t \cdot B^t \cdot A & A^t \end{pmatrix} \in \mathbb{M}_m(F).$$

It is easy to see that S has first row equal to $(c_1, \ldots, c_m)$. Through simple matrix computations, we see that $S \cdot S^t = S^t \cdot S = c \cdot I_m$, as desired. □

With Lemma 1.2.1 at hand, we are able to introduce the following theorem concerning sums of squares.

Theorem 1.2.2. *Let $m = 2^n$ and $u_1, \ldots, u_m, v_1, \ldots, v_m \in F$. Then there exist $w_2, \ldots, w_m \in F$ such that*

$$(u_1^2 + \cdots + u_m^2) \cdot (v_1^2 + \cdots + v_m^2) = (u_1 v_1 + \cdots + u_m v_m)^2 + w_2^2 + \cdots + w_m^2.$$

In particular, if $\sum u_i v_i = 0$, then $\left(\sum u_i^2 \right) \cdot \left(\sum v_i^2 \right)$ is a sum of $m - 1$ squares.

Proof. Let $u = \sum u_i^2$ and $v = \sum v_i^2$. By Lemma 1.2.1, there exists $U, V \in \mathbb{M}_m(F)$ such that

$$U \cdot U^t = U^t \cdot U = u \cdot I_m, \quad V \cdot V^t = V^t \cdot V = v \cdot I_m.$$

Furthermore, we know that the first row of U must be $(u_1, \dots, u_m)$, and the first row of V must be $(v_1, \dots, v_m)$. Therefore,

$$(uv) \cdot I_m = u \cdot V \cdot V^t = V \cdot (U^t \cdot U) \cdot V^t = W \cdot W^t, \quad \text{where} W = V \cdot U^t.$$

Notice that if $(w_1, w_2, \dots, w_m)$ is the first row of W, then $uv = w_1^2 + w_2^2 + \cdots + w_m^2$. Since $W = V \cdot U^t$, it is clear that we have $w_1 = u_1 v_1 + \cdots + u + m v_m$ which brings us to our desired conclusion. □

Before we finally introduce Pfister's Level Theorem, recall that the level of a field, written $s(F)$, is equal to ∞ if and only if -1 is not a sum of squares in F. In the case where F is not formally real, $s(F)$ is the smallest natural number n such that -1 is a sum of n squares in F.

Theorem 1.2.3. *Let F be a field. Then $s(F)$ is either ∞ or a power of 2.*

Proof. Let $s(F) = s \in \mathbb{N}$, and let $2^k \leq s < 2^{k+1}$. Write

$$-1 = a_1^2 + \cdots + a_{2^k}^2 + a_{2^k+1}^2 + \cdots + a_s^2.$$

By transposition, we see that

$$-(1 + a_{2^k+1}^2 + \cdots + a_s^2) = (a_1^2 + \cdots + a_{2^k}^2) \neq 0$$

Otherwise, we would have the following:

$$-1 = a_{2^k+1}^2 + \cdots + a_s^2$$

which is a sum of $s - 2^k < 2^k \leq s$ many squares, a contradiction. Notice that $a_1^2 + \cdots + a_{2^k}^2$ and $1 + a_{2^k+1}^2 + \cdots + a_s^2$ are both in $D(2^k)$. Since $D(2^k)$ is a group, by Theorem 1.2.2 we see (from the following calculation) that $-1 \in D(2^k)$. From before,

$$-(1 + a_{2^k+1}^2 + \cdots + a_s^2) = (a_1^2 + \cdots + a_{2^k}^2)$$

Through simple arithmetic, we get

$$-1 = \frac{a_1^2 + \cdots + a_{2^k}^2}{1 + a_{2^k+1}^2 + \cdots + a_s^2} = \frac{(a_1^2 + \cdots + a_{2^k}^2)(1 + a_{2^k+1}^2 + \cdots + a_s^2)}{(1 + a_{2^k+1}^2 + \cdots + a_s^2)^2}$$

which is in $D(2^k)$. Thus, $s(F) = s = 2^k$, as desired. □

With the completion of this proof, we see that the level of a field F is indeed either ∞ or a power of 2. From here on, we will be abandoning fields and shifting our work to the noncommutative case of division rings. One might think the same result on levels might hold for division rings. However, we will see that this is not the case.

CHAPTER 2

NONCOMMUTATIVE RINGS

The material in Chapter 2 is adapted from [2]

2.1 ORDERINGS AND PREORDERINGS IN RINGS

In this section, we introduce the notions of ordering and preordering in a ring. For a ring R to be ordered, there must be a transitive total ordering "$<$" given on R such that, for all elements $a, b, c \in R$, we have

$$a < b \Rightarrow a + c < b + c,$$

$$0 < a, 0 < b \Rightarrow 0 < ab.$$

We define the *positive cone* of the ordering "$<$" to be $P := \{c \in R : 0 < c\}$. It is clear that P has the following three properties:

$$\begin{aligned} &(a) \quad P + P \subseteq P \\ &(b) \quad P \cdot P \subseteq P \\ &(c) \quad P \cup (-P) = R \setminus \{0\}. \end{aligned} \tag{2.1}$$

Conversely, if we are given a set P satisfying these three axioms, then, defining a total ordering on R by: $a < b \Leftrightarrow (b - a) \in P$, it follows quickly that R becomes an ordered ring under "$<$". It is for this reason that we refer to a set P satisfying (2.1) as an *ordering* on R. Standard examples of ordered rings include $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ with their usual orderings.

Proposition 2.1.1. *Let P be an ordering on a ring $R \neq 0$. Then $P \cap (-P) = \emptyset$, $1 \in P$, and R is a domain with characteristic zero.*

Proof. If $a \in P \cap (-P)$, then $0 = a + (-a) \in P + P \subseteq P$, contradicting property (c) from (2.1). Next, note that one of ± 1 belongs to P, so $1 = 1^2 = (-1)^2 \in P \cdot P \subseteq P$. From this, it follows further that, for any $n \in \mathbb{N}$, $n \cdot 1 = 1 + \ldots + 1 \in P$. Therefore, $charR = 0$. Finally, if $b, c \in R \setminus \{0\}$, then for suitable choices of the signs, $(\pm b)(\pm c) \in P \cdot P \subseteq P$, and so $bc \neq 0$. This shows that R is a domain. □

While Proposition 2.2.1 gives us a set of necessary conditions for the existence of an ordering on a ring R, it is important to note that these conditions are not sufficient to ensure the existence of such an ordering. This issue gives rise to the following question: What is a necessary and sufficient condition for the existence of an ordering on a ring R? This question has been answered in the case where R is a field. In 1927, Emil Artin and Otto Schreier showed that a field R is orderable iff R is *formally real*.

Definition. A ring R is *formally real* if -1 is not a sum of squares in R.

It is important to note that this is a necessary condition for the existence of an ordering on R with the following reasoning: If $a \neq 0$, then either $a \in P$ or $-a \in P$ by (2.1)(c). Hence, $a^2 = a \cdot a = (-a)(-a) \in P$ by (2.1)(b). Thus, sums of squares are in P by (2.1)(a), and therefore, by Proposition 2.1.1, $-1 \in -P$ which means $-1 \notin P$.

The rest of the Artin-Schreier Theorem ensures that this condition of a ring R being formally real is indeed sufficient for R to have an ordering. We will state a generalization of the Artin-Schreier Theorem to possibly noncommutative rings later in this section. For now, we will extend the idea of an ordering to that of a preordering in a ring R.

Definition. A *preordering* in a ring R is a subset $T \subseteq R \setminus \{0\}$ satisfying the following two properties:

1. $T + T \subseteq T$
2. For $a_1, \ldots, a_m \in R \backslash \{0\}$ and $t_1, \ldots, t_n \in T$, the product of $a_1, a_1, \ldots, a_m, a_m, t_1, \ldots, t_n$, taken in any order, lies in T.

Since we will be frequently referring to property (2) from the above definition, we will introduce the following notation: For arbitrary elements $a_1, \ldots, a_m \in R$ and nonnegative integers $i_1, \ldots, i_m$, we write $per(a_1^{i_1} \cdots a_m^{i_m})$ to mean a product of the following $i_1 + \cdots + i_m$ factors: $\{\ a_1, \ldots, a_1, \ldots, a_m, \ldots, a_m\ \}$ where each a_k is taken i_k times. These factors may be permuted in any way. Using this notation, property (2) from the above definition may be expressed in the form: $per(a_1^2 \cdots a_m^2 t_1 \cdots t_n) \in T$, for any $a_1, \ldots, a_m \in R \setminus \{0\}$ and $t_1, \ldots, t_n \in T$.

We may now extend Proposition 2.1.1 to preorderings. The proof of the following proposition follows similarly to that of Proposition 2.1.1.

Proposition 2.1.2. *Let T be a preordering on a ring $R \neq 0$. Then $T \cap -T = \emptyset, 1 \in T$, and R is a domain with characteristic zero.*

Considering the fact that $axa = (-a)x(-a)$, we see that any ordering in R is, in fact, always a preordering. Extending this to a more general scenario, we see that the intersection of an arbitrary, non-empty family of orderings is also a preordering.

Before moving forward, we should introduce some new notation. Let $T \subseteq R \setminus \{0\}$ be any preordering, and let $b \in R$ be any nonzero element. We define T_b to be the set of all sums of elements of the form $per(b^i a_1^2 \cdots a_m^2 t_1 \cdots t_n)$ where $a_1, \ldots, a_m \in R \setminus \{0\}, t_1, \ldots, t_n \in T$, and $i, m, n \geq 0$.

With this new terminology at our disposal, we may introduce the following lemma.

Lemma 2.1.3. *The following are equivalent:*

1. *T_b is not a preordering in R*
2. *There exists an equation $t' + bt = 0$ where $t, t' \in T$*
3. *There exists an equation $t'' + t'b = 0$ where $t', t'' \in T$.*

Proof. If (2) holds, then $t'b + btb = 0$, so (3) holds with $t'' := btb \in T$. Similarly, we have (3) $\Rightarrow$ (2). Since (2) $\Rightarrow$ (1) is clear, we are left only with the proof of (1) $\Rightarrow$ (2). It is easy to see that the set T_b satisfies the two conditions required of a preordering.

Therefore, T_b fails to be a preordering if and only if $0 \in T_b$, i.e., if and only if there exists an equation

$$0 = \sum per(b^i a_1^2 \cdots a_m^2 t_1 \cdots t_n),$$

where, in each term, $a_1, \ldots, a_m \in R \setminus \{0\}$ and $t_1, \ldots, t_n \in T$. Take note that:

1. for even i, $per(b^i a_1^2 \cdots a_m^2 t_1 \cdots t_n) \in T$, and

2. for odd i, $b \cdot per(b^i a_1^2 \cdots a_m^2 t_1 \cdots t_n) \in T$,

since T is a preordering. If we group the terms in (2.2) according to the parity of i, we have an equation $0 = t + r$ where $t \in T$ and $br \in T$. Multiplying by b, we get $bt + t' = 0$, where $t' = br \in T$. □

With Lemma 2.1.3, we can now characterize the orderings among the preorderings.

Theorem 2.1.4. *A preordering $T \subseteq R \setminus \{0\}$ is an ordering iff T is maximal as a preordering.*

Proof. First assume T is an ordering. If there exists a preordering $T' \supsetneqq T$, then, for $a \in T' \setminus T$, we have $-a \in T \subseteq T'$ and so

$$0 = a + (-a) \in T' + T' \subseteq T',$$

which is a contradiction. Thus, T is a maximal preordering. Conversely, assume T is a maximal preordering. If T is not an ordering, then there exists an element b such that $b, -b \notin T$. Since T_b satisfies the definition of preordering and $T_b \supsetneqq T$, Lemma 2.1.3 implies that there exists an equation $t_1 + bt_2 = 0$, where $t_1, t_2 \in T$. Applying the same argument to $-b$, we get a similar equation $t_3 - bt_4 = 0$, where $t_3, t_4 \in T$. But then for $t_5 := (bt_2)(bt_4) \in T$, we get $t_1 t_3 + t_5 = 0$, which is a contradiction. □

Let us define $T(R)$ to be the set of all sums of terms of the form $per(a_1^2 \cdots a_m^2)$ where $a_i \in R \setminus \{0\}$. As before, it is easy to check that $T(R)$ is indeed a preordering. We may now define a ring R to be *formally real* is $0 \notin T(R)$. If R is formally real, then $T(R)$ is a preordering in R. We will call this the *weak preordering* of R since it is contained in every preordering of R.

Now, as promised, we introduce the complete generalization of the Artin-Schreier Theorem.

Theorem 2.1.5. *For any ring $R \neq 0$, the following are equivalent:*

1. *R is formally real.*
2. *R has a preordering.*
3. *R has an ordering.*

Proof. (3) $\Rightarrow$ (1) and (1) $\Rightarrow$ (2) are clear. For (2) $\Rightarrow$ (3), fix a preordering T in R. By Zorn's Lemma, T can be enlarged into a maximal preordering T_1. By Theorem 2.1.4, T_1 is an ordering for R. $\square$

In the theory of formally real fields, it is well known that any preordering T in a field F is the intersection of all the orderings containing T. In the case when $T = T(F)$, this says that an element $a \in F \setminus \{0\}$ is a sum of squares in F if and only if a is positive in each ordering of the formally real field F. We now wish to see how these results can be generalized from fields to arbitrary rings.

For any preordering T in a ring, we have the following equations:

$$\{\ \text{a}\in R : at \in T \text{ for some } t \in T\}$$

$$= \{\ \text{a}\in R : t'a \in T \text{ for some } t' \in T\}$$

$$= \{\ \text{a}\in R : ab^2 \in T \text{ for some } b \neq 0\}$$

$$= \{\ \text{a}\in R : b'^2a \in T \text{ for some } b' \neq 0\}.$$

In fact, if $at = t'$ where $t, t' \in T$, then $t'a = ata \in T$, and also $at^2 = t't \in T$. We will denote the set in (2.3) by $\tilde{T}$, and call it the *division closure* of T. It is clear that $0 \notin \tilde{T}$ and $T \subseteq \tilde{T}$. It is easy to check that $\tilde{T}$ is indeed a preordering of R. There is no need to check this since the following characterization of $\tilde{T}$ shows that $\tilde{T}$ is indeed a preordering.

Theorem 2.1.6. *For any preordering $T \subseteq R \setminus \{0\}$, the division closure $\tilde{T}$ of T is equal to the intersection T' of all the orderings of R containing T.*

Proof. For any ordering $P \supseteq T$, we have $\tilde{P} \supseteq \tilde{T}$. Since clearly $\tilde{P} = P$, this implies that $T' \supseteq \tilde{T}$. To complete the proof, we will show that, for any $a \neq 0$, $a \notin \tilde{T}$ implies that $a \notin P$ for some ordering $P \supseteq T$ (since this would mean $a \notin T'$). Consider T_{-a} (similar to the previously defined T_b). Since $a \notin \tilde{T}$, we know that T_{-a} is a preordering in R. This is evident from our previous work with T_b. As we saw before, T_{-a} can be enlarged into an ordering P of R. But then $P \supseteq T$, and $-a \in T_{-a} \subseteq P$ implies that $a \notin P$. □

The following are two immediate consequences of Theorem 2.1.6.

Corollary 2.1.7. *A preordering $T \subseteq R \setminus \{0\}$ is an intersection of orderings if and only if T is "division closed" in the sense that, for $a \in R$ and $t \in T$, $at \in T$ implies that $a \in T$.*

Corollary 2.1.8. *In a formally real ring R, a nonzero element $a \in R$ is totally positive (i.e., positive in all orderings of R) if and only if there exists $b \in R \setminus \{0\}$ such that ab^2 belongs to the weak preordering $T(R)$.*

In general, the weak preordering $T(R)$ need not be division-closed, so the totally positive element a above need not belong to $T(R)$.

2.2 ORDERED DIVISION RINGS

We now wish to specialize the notion of ordering structures to division rings. Many of the results from Section 2.1 take on a simpler form in the case of division rings. We will begin by introducing some new notation. Throughout this section, we let D denote a division ring, and let D^* denote its multiplicative group of nonzero elements. If P is an ordering in D, then clearly P is a subgroup of D^*. It is also interesting to note that with the total ordering induced from D, P is itself a multiplicative ordered group. The ordering cone for this group is $\{a \in P : a > 1\}$. Since $[D^* : P] = 2$, P is a normal subgroup of D^*. The following proposition shows that similar results hold for preorderings as well.

Proposition 2.2.1. *A set $T \subseteq D^*$ in a division ring D is a preordering if and only if $T + T \subseteq T, T \cdot T \subseteq T$, and $D^{*2} \subseteq T$. If T is a preordering, then $t \in T \Rightarrow t^{-1} \in T$, and T contains the commutator group $[D^*, D^*]$. In particular, T is a normal subgroup of D^*, and $D^*/\,T$ is an abelian group of exponent 2.*

Proof. For the first conclusion of the proposition, it is clear that part (2) of the definition of preordering from Section 2.1 implies the two properties $T \cdot T \subseteq T$ and $D^{*2} \subseteq T$. Conversely, assume these properties hold, and consider $x = per(a_1^2 \cdots a_m^2 t_1 \cdots t_n)$ where $a_1, \ldots, a_m \in D^*$ and $t_1, \ldots, t_n \in T$. Using the relation, $aba = (ab)^2(b^{-1})^2 b$, we can rewrite x as a product $c_1 \cdots c_r$, where each c_i is either a nonzero square or is an element of T. Hence, $x \in T$. Next, we note that $aba^{-1}b^{-1} = a^2(a^{-1}b)^2(b^{-1})^2$, so $[D^*, D^*] \subseteq T$. From this, the other conlusions follow easily. □

For future reference, we shall refer to any element of the form $a_1^2 \cdots a_m^2$ as a *square-product*. From Proposition 2.2.1, any commutator in D is a square-product, and any element $per(a_1^2 \cdots a_m^2)$ is also a square-product. In Section 2.1, we defined the set $T(D)$ to be the set of sums of elements of the form $per(a_1^2 \cdots a_m^2)$ where m is arbitrary, and the a_i's are nonzero. For a division ring D, $T(D)$ is then the set of sums of nonzero square-products. By definition, D is formally real if and only if $0 \notin T(D)$. Since all the nonzero square-products form a subgroup of D^*, we see that D is formally real if and only if $-1 \notin T(D)$. This result in conjuction with Theorem 2.1.5 brings us to our next result.

Theorem 2.2.2. *A division ring D can be ordered if and only if -1 is not a sum of square-products in D.*

If D is a field, any square-product is just a square. If D is a division ring but not a field, then a square-product need not necessarily be a perfect square, that is, a^2b^2 does not necessarily equal $(ab)^2$. If D is not formally real, we can write -1 as a sum of square-products, but not necessarily as a sum of squares. Later in this section, we will work through the construction of such an example.

Recall that, for a preordering $T \subseteq D^*$ and any element $b \in D$, we have defined T_b to be the set of all sums of elements of the form $per(b^i a_1^2 \cdots a_m^2 t_1 \cdots t_n)$ where $a_1, \ldots, a_m \in R \setminus \{0\}, t_1, \ldots, t_n \in T$, and $i, m, n \geq 0$. Notice that T_b is essentially $T + bT (= T + Tb)$ in the case of division rings. Also notice that since T is a subgroup of D^*, it is clearly division-closed (as we defined in Section 2.1.) Combining Lemma 2.1.3 and Corollary 2.1.7, we arrive at the following theorem.

Theorem 2.2.3. *Let T be any preordering in a division ring D. Then T is the intersection of all the orderings containing T. For $b \in D$, $T_b = T + bT$ is a preordering of D if and only if $b \notin -T$.*

Corollary 2.2.4. *Assume $charD \neq 2$. Then an element $s \in D^*$ is totally positive (i.e., positive with respect to all orderings of D) if and only if a is a sum of square-products.*

Proof. If D is formally real, the conclusion follows by applying Theorem 2.2.3 to the weak preordering $T(D)$, which consists of all sums of square-products. Now assume D is not formally real. Then, vacuously, any $a \in D^*$ is totally positive.

Since $charD \neq 2$, we can write

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

By Theorem 2.2.2, -1 is a sum of square-products, so a is also a sum of square-products. □

At this point, it would be helpful to introduce an important class of examples of ordered division rings. We will also take some time to work through the construction since it is in no way trivial.

2.3 EXAMPLE OF AN ORDERED DIVISION RING

Before beginning the construction, we should first work through some facts on subsets of a totally ordered set G. Recall that a subset $S \subseteq G$ is *well-ordered* if every nonempty subset of S has a least element.

Lemma 2.3.1. *Let $(G, <)$ be a totally ordered set. For any subset $S \subseteq G$, the following statements are equivalent:*

1. *S is well-ordered*
2. *S satisfies the descending chain condition (i.e., any sequence $s_1 \geq s_2 \geq s_3 \geq \cdots$ in S is eventually constant).*
3. *Any sequence $\{s_1, s_2, s_3, \ldots\}$ in S contains a subsequence $\{s_{n(1)}, s_{n(2)}, s_{n(3)}, \ldots\}$ (where $n(1) < n(2) < n(3) < \cdots$) such that $s_{n(1)} \leq s_{n(2)} \leq s_{n(3)} \leq \cdots$.*

Proof. Since (3) $\Rightarrow$ (2) and (2) $\Rightarrow$ (1) are both obvious, it is enough to show that (1) $\Rightarrow$ (3). Let $\{s_1, s_2, s_3, \ldots\}$ be a sequence in a well-ordered subset S of G. Choose $n(1)$ so that $s_{n(1)} = min\{s_i : i \geq 1\}$. Then choose $n(2) > n(1)$ so that $s_{n(2)} = min\{s_i : i > n(1)\}, \ldots,$ etc. This produces a nondecreasing subsequence $s_{n(1)} \leq s_{n(2)} \leq \cdots$, as desired. □

Lemma 2.3.2. *Let S and T be well-ordered subsets of a totally ordered set $(G, <)$. Then $S \cup T$ is well-ordered. If $(G, <)$ is an ordered group, then*

$$U := S \cdot T = \{st : s \in S, t \in T\}$$

is also well-ordered. Moreover, for any $u \in U$, there exists only an finite number of ordered pairs (s, t) with $s \in S$ and $t \in T$ such that $u = st$.

Proof. Since the proof of the first conclusion is trivial, we will omit it. For the second conclusion, assume for the sake of contradiction that U is not well-ordered. By Lemma 2.3.1, there would exist a strictly decreasing sequence $s_1t_1 > s_2t_2 > \cdots$ where $s_i \in S, t_i \in T$. After replacing $\{s_1, s_2, \ldots\}$ by a subsequence, we may assume (since S is well-ordered) that $s_1 \leq s_2 \leq \cdots$. If $t_i \leq t_{i+1}$ for some i, we would have $s_it_i \leq s_{i+1}t_1 \leq s_{i+1}t_{i+1}$, which is a contradiction. Thus, it must be that $t_1 > t_2 > t_3 > \cdots$. But this contradicts the fact that T is well-ordered. This justifies the second conclusion of Lemma 2.3.2. The proof of the third conclusion follows similarly. □

With these two lemmas at hand, we may now begin the Mal'cev-Neumann construction of Laurent series rings. Let us begin by fixing a base ring R and an ordered group $(G, <)$. We assume that G is multiplicatively written. Let the positive cone of the ordering on G be defined as follows:

$$P = \{x \in G : x > 1\}$$

We fix a group homomorphism ω from G to $Aut(R)$, where $Aut(R)$ is the group of automorphisms of the ring R. We will denote the image of $g \in G$ under ω by ω_g.

The Mal'cev-Neumann ring $A = R((G, \omega))$ consists of certain formal sums

$$\alpha = \sum_{g \in G} \alpha_g g$$

where the α_g's are elements of R. It is useful to think of such formal series $\alpha = \sum_{g \in G} \alpha_g g$ as a function $\alpha : G \to R$ defined by $\alpha(g) = \alpha_g$ for all $g \in G$. For each such α, we define the *support* of α by $supp(\alpha) := \{g \in G : \alpha_g \neq 0\}$.

We are now in a position to give an actual definition for the previously mentioned Mal'cev-Neumann ring $A = R((G, \omega))$. The definition is as follows:

$$A = R((G, \omega)) = \{\alpha = \sum \alpha_g g : supp(\alpha) \subseteq G \text{ is well-ordered}\}$$

Formal addition and multiplication in A are defined as follows:

$$\sum_{g \in G} \alpha_g g + \sum_{g \in G} \beta_g g = \sum_{g \in G} (\alpha_g + \beta_g) g, \tag{2.2}$$

$$\left(\sum_{g \in G} \alpha_g g \right) \cdot \left(\sum_{h \in G} \beta_h h \right) = \sum_{u \in G} \left(\sum \alpha_g \omega_g(\beta_h) \right) u, \tag{2.3}$$

where the last sum is over all (g, h) such that $gh = u$. Combining the fact that we can restrict g and h to $supp(\alpha)$ and $supp(\beta)$, respectively, and the fact that both supports are well-ordered in G, we see that the last sum in (2.3) is finite by Lemma 2.3.2. Also, since

$$supp(\alpha + \beta) \subseteq supp(\alpha) \cup supp(\beta),$$

$$supp(\alpha\beta) \subseteq supp(\alpha) \cdot supp(\beta),$$

the supports on the left-hand side are both well-ordered by Lemma 2.3.2. Thus, we see that addition and multiplication are well-defined in A.

With this observation, we see that it is straightforward to check that $(A, +, \cdot)$ is a ring. The subring A, which consists of all finite sums $\alpha = \sum \alpha_g g$ (i.e., sums of finite support), turns out to be the twisted group ring $R * G$ which we will denote as $R[G, \omega]$. Furthermore, we identify R with the subring $R \cdot 1 \subseteq A$, and identify G with the subgroup $1 \cdot G$ of invertible elements in A. If we find ourselves in the case where ω is the trivial homomorphism, we will denote the untwisted ring of Laurent series by $R((G))$.

The method with which we multiply two series α and β as in (2.3) comes from the distributive law and the twist law $g \cdot r = \omega_g(r) g$, where $r \in R$ and $g \in G$. When dealing with the special case where G is an infinite cyclic group $\{x^n : n \in \mathbb{Z}\}$ ordered by the positive cone $P = \{x^n : n > 0\}$, the homomorphism

$$\omega : \quad G \to Aut(R)$$

is specified by a single automorphism $\sigma := \omega_x$. In this situation, the twist law is simply $x \cdot r = \sigma(r)x$ (for $r \in R$), and

$$A = R((\langle x \rangle, \omega)) = \{\sum_{i=n}^{\infty} \alpha_i x^i : \quad \alpha_i \in R, n \in \mathbb{Z}\}$$

is Hilbert's twisted Laurent series ring $R((x, \sigma))$. Note that the well-ordered subsets of $\mathbb{Z}$ are just the non-empty subsets which have a lower bound.

We now wish to show that the above construction is indeed a division ring. This naturally brings us to the following theorem:

Theorem 2.3.3. *Assume R is a division ring, and $(G, <)$ and ω are as above. Then $A = R((G, \omega))$ is also a division ring.*

The proof of Theorem 2.3.3 relies heavily on the following lemma on ordered groups (G, P).

Lemma 2.3.4. *Let S be a well-ordered subset of P in the ordered group (G, P). Let $S^n = \{s_1 \cdots s_n : s_i \in S\}$ for $n \geq 1$, and let $S^\infty = \cup_{n \geq 1} S^n \subseteq P$. Then*

1. *S^∞ is well-ordered, and*

2. *any $u \in S^\infty$ lies in only finitely many S^n's.*

It is clear from Lemma 2.3.2 and a simple induction argument that each $S^n (n \geq 1)$ is well-ordered. It is not so obvious that conclusion (1) in Lemma 2.3.4 is true. This is due to the fact that an infinite union of well-ordered subsets of G is not necessarily well-ordered.

Before we prove Lemma 2.3.4, it is necessary to introduce some new terminology. Given the ordered group (G, P), we say that two elements s and t in P are *relatively archimedean* (written $s \sim t$) if $s \leq t^m$ and $t \leq s^n$ for some positive integers m, n. It is simple to check that "$\sim$" is an equivalence relation on P.

We denote the equivalence class of $s \in P$ by $[s]$. We will refer to $[s]$ as the *archimedean class of s*. Given two archimedean classes $[r]$ and $[s]$, we define $[r] < [s]$ if $r^n < s$ for all

$n \geq 1$. It is easy to see that "$<$" is well-defined independently of the choice of the class representative, and it gives a total ordering on the set of all the archimedean classes of G. As is usually the case, $[r] \leq [s]$ will mean either$[r] < [s]$ or $[r] = [s]$.

Furthermore, for any elements $s_1, \ldots, s_n \in P$, we always have

$$[s_1 \cdots s_n] = [\max\{s_1, \ldots, s_n\}].$$

If $s_i = \max\{s_1, \ldots, s_n\}$, then $s_1 \cdots s_n \leq s_i^n$ and $s_i \leq s_1 \cdots s_n$ (since all $s_j > 1$). This shows that $s_i \sim s_1 \cdots s_n$, and so $[s_1 \cdots s_n] = [s_i]$.

With this in mind, we will begin the lengthy proof of Lemma 2.3.4.

Proof. We begin by proving conclusion (1). For the sake of contradiction, let us assume that S^∞ is not well-ordered. Then there exists a strictly decreasing sequence $u_1 > u_2 > \cdots$ in S^∞, say $u_i = s_{i1}s_{i2} \cdots s_{in_i}$, where $s_{ij} \in S$. We claim that the sequence of archimedean classes $[u_1] \geq [u_2] \geq \cdots$ is eventually constant. To see this, let

$$s_i = \max\{s_{i1}, \ldots, s_{in_i}\} \in S.$$

From the previous observation, $[u_i] = [s_i]$ so we have $[s_1] \geq [s_2] \geq \cdots$. Since $\{s_1, s_2, \ldots\} \subseteq S$ has a smallest element, say s_{i0}, the sequence $[s_1] \geq [s_2] \geq \cdots$ must stabilize after i_0 terms, as claimed.

Let $U = \min\{[u_i] : i \geq 1\} = [s_{i0}]$. By choosing a different strictly decreasing sequence in S^∞, say $u_1' > u_2' > \cdots$, we arrive at another archimedean class U'. Since any such class is the class of an element in S, we may assume that our initial $u_1 > u_2 > \cdots$ has been chosen such that U is as small as possible. Once we eliminate a finite number of the u_i's, we may assume that $U = [u_i] = [s_i]$ for all $i \geq 1$.

Now consider the nonempty set $\{s \in S : [s] = U\}$. This has a least element. We will denote this least element by s_U. Since $[s_U] = [u_1]$, there exists an integer $m \geq 1$ such that $u_1 \leq s_U^m$. Furthermore, we assume that our sequence $u_1 > u_2 > \cdots$ (subject to all the previous conditions) has been chosen so that the m we took above is as small as possible.

Our u_i can take on any of following four forms:

$$\{s_i, v_i s_i, s_i w_i, v_i s_i w_i\}$$

where $v_i, w_i \in S^\infty$. Only a finite number of the u_i's can be of the first type. If this is not the case, we would have a strictly decreasing sequence in S, which is not possible. Therefore, there must exist a sequence of the u_i's of one of the other three types. We will proceed under the assumption that our sequence of u_i's is of the fourth type. (The other two types are actually much simpler, and can be dealt with in a similar manner.)

Once we pass to a subsequence, we may assume that $u_i = v_i s_i w_i$ for all i. Let $B = \{v_i : i \geq 1\}, C = \{w_i : i \geq 1\}$, and let $D = \{s_i : i \geq 1\} \subseteq S$. If B and C are both well-ordered, we have that (by a double application of Lemma 2.3.2) BDC is also well-ordered. We see that $u_1 > u_2 > \cdots$ in BDC gives a contradiction. Therefore, let us assume that B is not well-ordered. Once we replace the v_i's by a subsequence, we may assume that $v_1 > v_2 > \cdots$ in $B \subseteq S^\infty$. Earlier, we saw that

$$V := \min\{[v_i] : i \geq 1\}$$

exists, and, since $v_i \leq u_i$, we have $V \leq U$. Since we chose U to be minimal, we get $V = U$ which implies that $s_V = s_U$. As before, let us assume that $[v_1] = [v_2] = \cdots$. From

$$v_1 s_U \leq v_1 s_1 \leq v_1 s_1 w_1 = u_1 \leq s_U^m, v_1 s_U \leq v_1 s_1 \leq v_1 s_1 w_1 = u_1 \leq s_U^m,$$

we see that it must be the case that $m \leq 2$. Otherwise, we would have $v_1 \leq 1$ which is not possible. If we can cancel the s_U's in the above equation, we arrive at $v_1 \leq s_U^{m-1} = s_V^{m-1}$. This is a contradiction to the minimality of m and, therefore, S^∞ is well-ordered.

We now wish to show that conclusion (1) implies conclusion (2). Let us begin by assuming that there is a counterexample to (2). Let us call this counterexample u. Since S^∞ is well-ordered by (1), there exists a least counterexample $u \in S^\infty$. For $1 \leq i < \infty$, we write $u = s_{i1} s_{i2} \cdots s_{in_i}$ where $2 \leq n_1 < n_2 < \cdots$, and $s_{ij} \in S$. Since

$$u = s_{i1} \cdots (s_{i2} \cdots s_{in_i}) \in S \cdot S^\infty,$$

and both S and S^∞ are well-ordered, Lemma 2.3.2 implies that there is an element $v \in G$ such that

$$s_{i2} \cdots s_{in_i} = v$$

for infinitely many i's. Clearly, this v lies in infinitely many S^n's, but $s_{i1} > 1$ for all i implies that $v < u$. This is a contradiction to the minimality of our counterexample u. □

The following is an important consequence of Lemma 2.3.4. It is important to note that we make no assumption on R in the following corollary.

Corollary 2.3.5. *Let*

$$\alpha \in \sum \alpha_g g \in A = R((G, \omega))$$

be such that $S := supp(\alpha)$ *lies in* P. *Then for any* $a_0, a_1, \ldots \in R$, *the sum* $a_0 + a_1\alpha + a_2\alpha^2 + \cdots$ *gives a well-defined element of* A.

Proof. Since $supp(\alpha^n) \subseteq S^n$, each $g \in G$ can lie in $supp(\alpha^n)$ only for finitely many n's by part (2) of Lemma 2.3.4. Therefore, it makes sense to take the sum

$$\gamma = a_0 + a_1\alpha + a_2\alpha^2 + \cdots$$

Furthermore, $supp(\gamma)$ is well-ordered since it lies in

$$\{1\} \cup_{n\geq 1} S^n = \{1\} \cup S^\infty.$$

Thus, γ is an element of A. □

With Lemma 2.3.4 and Corollary 2.3.5 at our disposal, we may finally give a proof of Theorem 2.3.3

Proof. Let us assume that R is a division ring and consider a nonzero element $\beta = \sum \beta_g g \in A$. Let g_0 be the least element in $supp(\beta)$. Then $\beta_{g_0}^{-1}\beta g_0^{-1} = 1 - \alpha$ where $\alpha \in A$ has $supp(\alpha) \in P$. By Corollary 2.3.5,

$$\gamma = 1 + \alpha + \alpha^2 + \cdots$$

is a well-defined element of A. Through a simple calculation, we see that γ is an inverse of $1-\alpha$. Thus, $1-\alpha$ is a unit in A, and so $\beta = \beta_{g_0}(1-\alpha)g_0$ is also a unit in A. □

With the completion of the proof of Theorem 2.3.3, we see that $R((G,\omega))$ is indeed a division ring. We are now ready to introduce the notion of ordering with regard to our construction.

As before, let R be an ordered ring, and let P_0 be an ordering on R. Also, let $(G,<)$ be a multiplicative ordered group, and let $\omega : G \to Aut(R)$ be a homomorphism from G to the group of automorphisms of R. Recall that we denote the Mal'cev-Neumann Laurent series ring as $A = R((G,\omega))$ with formal addition and multiplication as defined in equations (2.2) and (2.3), respectively. Recall, as well, the twist law for formal multiplication defined by $g \cdot r = \omega_g(r)g(g \in G, r \in R)$ where ω_g denotes the image of g under ω.

Proposition 2.3.6. *Assume that, for each $g \in G, \omega_g$ is an order-preserving automorphism of (R, P_0), i.e., $\omega_g(P_0) = P_0$. Let*

$$P = \{\alpha = \sum_{g \in G} \alpha_g g : \alpha_{g_0} \in P_0 \textit{ for } g_0 = \textit{least element in supp}(\alpha)\}.$$

Then P is an ordering for $A = R((G,\omega))$. If (R, P_0) is an ordered division ring, then so is (A, P).

Proof. To show that P is an ordering for A, we simply need to check the three axioms for an ordering hold. In other words, we should check that conditions (a), (b), and (c) from equation (2.1) in section 2.1 hold for this particular P. Since conditions (a) and (c) are obvious, we need only check that condition (b) holds.

Let $\alpha = \sum \alpha_g g$ and $\beta = \sum \beta_h h$ be in P. Let g_0 be the least element of *supp* (α), and let h_0 be the least element of *supp* (β). Then $g_0 h_0$ is the least element of *supp* $(\alpha\beta)$. This element appears in $\alpha\beta$ with coefficient $\alpha_{g_0}\omega_{g_0}(\beta_{h_0})$. Since $\alpha_{g_0}, \beta_{h_0} \in P_0$ and ω is an order-preserving automorphism, we see that $\alpha_{g_0}\omega_{g_0}(\beta_{h_0}) \in P_0$. Therefore, $\alpha\beta \in P$. Thus, P is an ordering on A.

By a simple application of Theorem 2.3.3 in combination with the previous part of this proof, we see that the final conclusion of Proposition 2.3.6 holds. That is, if (R, P_0) is an ordered division ring, then so is (A, P). □

It is useful to note that we can think of G as being embedded in A by identifying $g \in G$ with $1 \cdot g$. By doing so, we see that $G \subseteq P$. We also see that if $g > 1$ in the ordering of G, then $1 - g \in P$. Therefore, we have that $g < 1$ in the ordering of A. If we let $R = \mathbb{Q}$ with its usual ordering P_0, and let ω be the trivial homomorphism, we get the following corollary to Proposition 2.3.6.

Corollary 2.3.7. *Any ordered group $(G, <)$ can be embedded, in an order-reversing way, as a subgroup of the multiplicative ordered group of positive elements in an ordered division ring A. If G is commutative, A may be chosen to be an ordered field.*

With the previous results and our construction of the Mal'cev-Neumann Laurent series ring, we can easily introduce Hilbert's original examples of noncommutative ordered division rings. Let (R, P_0) be an ordered field, and let $G = \langle x \rangle$ be an infinite cyclic group with the ordering cone $\{x^n : n \geq 1\}$. Let σ be any order-preserving automorphism of (R, P_0), and let

$$\omega : G \to Aut(R)$$

be defined by $\omega_x = \sigma$. The resulting Laurent series division ring $A = R((x, \sigma))$, with multiplication induced by $xr = \sigma(r)x$ where $r \in R$, has a natural ordering P which extends P_0. Note that if σ is not the trivial homomorphism, then (A, P) is a noncommutative ordered division ring.

It would be helpful to examine a specific example of this idea. Let $R = Q((y))$ with the ordering P_0 being constructed from the usual ordering of Q by a similar method used in Proposition 2.3.6. That is,

$$P_0 = \{\sum_{i=n}^{\infty} a_i y^i : n \in Z, a_n > 0 \in \mathbb{Q}\}$$

As for our desired σ, let us take the order-preserving automorphism of $\mathbb{Q}$ induced by $y \mapsto 2y$. Our result, namely the noncommutative ordered division ring $(\mathbb{Q}((y))((x, \sigma)), P)$, is Hilbert's original example of a noncommutative ordered division ring.

It is more useful to us to consider a variation of Hilbert's example. Instead of letting $R = \mathbb{Q}((y))$, we shall consider a formally real field k (instead of $\mathbb{Q}$) with $R = k((y))$. Recall that a formally real field is one in which -1 is not a sum of squares. Fixing an element $c \in k^*$, we let σ be the automorphism of R defined by $\sigma(y) = cy$ where $\sigma|k =$ *the identity.* With our new division ring $A = k((y))((x; \sigma))$, we have the following proposition.

Proposition 2.3.8. *Let $H_i \in A$.*

1. *Whenever $\sum_i H_i^2 = 0$ in A, we have $H_1 = H_2 = \cdots = 0$. In particular, -1 is not a sum of squares in A.*

2. *If c has the form $-(1 + c_1^2 + \cdots + c_r^2)$ in k, then -1 is a sum of $r + 1$ square-products in A. In this case, A is not formally real.*

Before moving on to the proof, it might be helpful to point out that this proposition allows us to construct division rings in which -1 is a sum of square-products, but not a sum of squares.

Proof. Notice that, in (2), we have $xy = \sigma(y)x = cyx$, so

$$c = xyx^{-1}y^{-1} = x^2(x^{-1}y)^2(y^{-1})^2.$$

If $c = -(1 + c_1^2 + \cdots + c_r^2)$, then

$$-1 = x^2(x^{-1}y)^2(y^{-1})^2 + c_1^2 + \cdots + c_r^2$$

which is a sum of $r + 1$ square-products. For (1), assume that $\sum_i H_i^2 = 0$ where the H_i's are not all zero and $c \in k^*$ is arbitrary. Write $H_i = h_i x^m + \cdots$, where m is chosen such that some $h_i \in k((y))$ is nonzero. Then

$$\sum_i H_i^2 = \sum_i (h_i x^m + \cdots)(h_i x^m + \cdots) = \left(\sum_i h_i \sigma^m(h_i) \right) x^{2m} + \text{higher terms.} \qquad (2.4)$$

Now write $h_i = a_i y^n + \cdots$, where n is chosen such that some $a_i \in k$ is nonzero. Then

$$\sum_i h_i \sigma^m(h_i) = \sum_i (a_i y^n + \cdots)(a_i c^{mn} y^n + \cdots) = \left(\sum_i a_i^2 c^{mn}\right) y^{2n} + \text{higher terms}.$$

This is a nonzero element in $k((y))$ since $\sum_i a_i^2 \neq 0$ in k. Thus, by equation (2.4), $\sum_i H_i^2 \neq 0$ in A. $\square$

With addition of Proposition 2.3.8, it would be useful to introduce a new definition.

Definition. For a non-formally real division ring D, the *level*, $s(D)$, of D is defined to be the smallest integer s such that -1 is a sum of s square-products in D.

Recall from Chapter 1 that $s(D)$ must be a power of 2 in the case where D is a field, and it can be shown that any power of 2 is the level of some non-formally real field. The following theorem shows that the level of a non-formally real division ring does not hold to this requirement. Instead, the level can be any positive integer. The following theorem is stated simply for motivation for the final chapter where we will recall some useful information and restate the theorem in a slightly different way.

Theorem 2.3.9. *In Proposition 2.3.8 (2), assume that $-c = 1 + c_1^2 + \cdots + c_r^2 \in k$ is not a sum of squares of r elements in k. Then $-1 = x^2(x^{-1}y)^2(y^{-1})^2 + c_1^2 + \cdots + c_r^2$ is a shortest representation of -1 as a sum of square-products in A, i.e., $s(A) = r + 1$.*

CHAPTER 3

THE LEVEL OF DIVISION RINGS

The main focus of this chapter will be to work through a paper by Winfried Scharlau and Angelika Tschimmel [3] which analyzes the level of division rings. We should first recall some of our previous work with (commutative) fields before continuing further.

Recall that we define a commutative field K to be formally real if -1 is not a sum of squares in K. In the case where K is not formally real, we define (as before) the level $s(K)$ of the field K to be the smallest natural number n such that -1 is the sum of n squares in K. Recall that Pfister's Level Theorem (Theorem 1.2.3) states that the level of a field must be either ∞ or a power of 2.

When dealing with a (noncommutative) division ring, we may replace the idea of sums of squares with sums of square-products (as we defined earlier). With this in mind, we call a division ring K formally real if -1 is not a sum of square-products. If K is not formally real, we define the level $s(K)$ to be the smallest natural number n such that -1 is the sum of n square-products in K.

As the main result of this chapter, we now construct a division ring of arbitrary level. This construction is similar to the example that was introduced in Section 2.3.

Let k be a (commutative) field and let $k((y))$ be the field of formal power series over k in the indeterminate y. Let z be another indeterminate, and consider the set

$$k((y))((z)) = \{Y_m z^m + Y_{m+1} z^{m+1} + \cdots | m \in \mathbb{Z}, Y_i \in k((y))\}$$

of formal right Laurent series with principal part in the indeterminate z over $k((y))$. We use the same addition rules as were introduced in equation (2.2) from Section (2.3). We will also use a similar method of multiplication as was introduced in equation (2.3) in the same section. Instead of employing the twist function ω_g as in equation (2.3) (where $g \cdot r = \omega_g(r) g$) , we will introduce the following commutation rule: Let $a \in k$ (where

$a \neq 0, 1)$ be a fixed twist element. We define multiplication in $k((y))((z))$ precisely as was defined in equation (2.3) from Section (2.3) with the commutation rule

$$zy = ayz.$$

In particular,

$$z^j y^i = a^{ij} y^i z^j \quad \text{for} \quad i, j \in \mathbb{Z}.$$

We have already shown in Section 2.3 that $k((y))((z))$ is a division ring (i.e., division ring), and let us denote this division ring by K_a. Let Z be an element in $k((y))((z))$ such that

$$Z = Y_m z^m + Y_{m+1} z^{m+1} + \cdots \quad \text{with} \quad Y_m = \alpha_s y^s + \alpha_{s+1} y^{s+1} + \cdots, \quad \alpha_s \neq 0.$$

We shall call $\alpha_s \in k$ the lowest coefficient of Z. By our commutation rule, we see that the lowest coefficient of a square-product is an element of $k^{*2} \cup ak^{*2}$. Notice also that a is a square-product as seen in the following equation:

$$zy = ayz \Rightarrow a = z^2 (z^{-1} y)^2 y^{-2}.$$

Before introducing the main theorem, it would be useful to preemptively prove a few results on products of sums of squares.

Let F be a field of characteristic not equal to 2. Let $D(k)$ denote the collection of sums of k squares in F.

Proposition 3.0.10. *If $m \leq n$, then $D(m) \subset D(n)$.*

Proof. Let $a_i \in F$. Then

$$a_1^2 + \cdots + a_m^2 = a_1^2 + \cdots + a_m^2 + 0^2 + \cdots 0^2,$$

where $(n - m)$ zeroes are added. $\square$

The following is a corollary to Theorem 1.2.2 which states, in short, that $D(2^t) \cdot D(2^t) \subset D(2^t)$.

Corollary 3.0.11. *Let a, b be positive integers. Then $D(a) \cdot D(b) \subset D(a+b-1)$.*

Proof. We induct on $M := a + b$. As $a, b \geq 1$, the base case is for $M = 2$. Here $a = b = 1$ and

$$D(a) \cdot D(b) \subset D(1) \cdot D(1) \subset D(1) \subset D(a+b-1).$$

Now suppose $M > 2$. We can assume $a \leq b$. Find t with $2^{t-1} < a \leq 2^t$, and write $b = k2^t + s$, with $0 \leq s < 2^t$. We must consider two cases for k, that is, $k = 0$ and $k > 0$. Now suppose $M > 2$. We can assume $a \leq b$. Find t with $2^{t-1} < a \leq 2^t$, and write $b = k2^t + s$, with $0 \leq s < 2^t$. We must consider two cases for k, that is, $k = 0$ and $k > 0$.

First, consider $k = 0$. Here, $b = s < 2^t$. Note that $b \geq a \geq 2^{t-1} + 1$ so that $a + b - 1 \geq 2^t + 1$. We have

$$D(a) \cdot D(b) \subset D(2^t) \cdot D(2^t) \subset D(2^t) \subset D(a+b-1).$$

For $k > 0$, we have $s < 2^t \leq b$, and

$$\begin{aligned} D(a) \cdot D(b) \subset D(a) \cdot [D(k2^t) + D(s)] &\subset D(2^t) \cdot D(k2^t) + D(a) \cdot D(s) \\ &\subset D(k2^t) + D(a+s-1) \\ &= D(a + k2^t + s - 1) \\ &= D(a+b-1), \end{aligned}$$

where in the second line we used Pfister's result for the first term and induction for the second term. □

Corollary 3.0.12. *Let n be a positive integer and $0 \leq m < n$. Then*

$$D(m+1) \cdot D(n-m) \subset D(n).$$

Proof. Take $a = m + 1$ and $b = n - m$. Then $a + b - 1 = n$. □

With these helpful results, we are now able to introduce the main result of the paper.

Theorem 3.0.13. *Let k be the rational function field $\mathbb{R}(x_1, \ldots, x_n)$, and let*

$$-a = 1 + x_1^2 + \cdots + x_n^2.$$

That is, we choose $-a$ for the Cassels polynomial $1 + x_1^2 + \cdots + x_n^2$. Then $s(K_a) = n + 1$.

Proof. We have that $-a = 1 + x_1^2 + \cdots + x_n^2$. By a simple algebraic manipulation, we arrive at the equation

$$-1 = a + x_1^2 + \cdots + x_n^2$$

Earlier, we showed that a is a square-product. Therefore, $s(K_a) \leq n + 1$ since -1 is the sum of at most $n + 1$ square-products by the above equation. Now, assume there exists square-products $Z_1, \ldots, Z_n$ such that

$$-1 = Z_1 + \cdots + Z_n.$$

Consider the lowest coefficient of $Z_1 + \cdots + Z_n$, that is, the sum of the lowest coefficients of some of the Z_i. We note that this sum is equal to 0 or -1.

Now, notice that the lowest coefficient of the Z_i are elements of $k^{*2} \cup ak^{*2}$. Therefore, for some $0 \leq m \leq n$, we can define the quadratic form q over k to be

$$q = \langle 1, \ldots, 1, a, \ldots, a \rangle = m \times \langle 1 \rangle \perp (n - m) \times \langle a \rangle.$$

By our claim, we hope to have $q = 0$ or -1. We claim next that when q represents 0, q also represents -1. To show this, let us assume that q represents 0, and say $b_1 \neq 0$. Then

$$\begin{aligned}
0 &= b_1^2 + \cdots + b_m^2 + ac_1^2 + \cdots + ac_{n-m}^2 \\
-b_1^2 &= b_2^2 + \cdots + b_m^2 + ac_1^2 + \cdots + ac_{n-m}^2 \\
-1 &= \left(\frac{b_2}{b_1}\right)^2 + \cdots + \left(\frac{b_m}{b_1}\right)^2 + a\left(\frac{c_1}{b_1}\right)^2 + \cdots + a\left(\frac{c_{n-m}}{b_1}\right)^2 \\
-1 &= 0^2 + \left(\frac{b_2}{b_1}\right)^2 + \cdots + \left(\frac{b_m}{b_1}\right)^2 + a\left(\frac{c_1}{b_1}\right)^2 + \cdots + a\left(\frac{c_{n-m}}{b_1}\right)^2
\end{aligned}$$

Thus, if q represents 0, then q also represents -1.

We see now that in either case, q represents -1. Let us examine this representation further. Doing so will bring us to a contradiction which will complete the proof.

Let us consider $q = -1$. So

$$-1 = b_1^2 + \cdots + b_m^2 + ac_1^2 + \cdots + ac_{n-m}^2$$

$$-1 - b_1^2 - \cdots - b_m^2 = ac_1^2 + \cdots + ac_{n-m}^2$$

$$1 + b_1^2 + \cdots + b_m^2 = -a(c_1^2 + \cdots + c_{n-m}^2)$$

Multiplying both sides by $(c_1^2 + \cdots + c_{n-m}^2)$, we get

$$(1 + b_1^2 + \cdots + b_m^2)(c_1^2 + \cdots + c_{n-m}^2) = -a(c_1^2 + \cdots + c_{n-m}^2)^2$$

Now, let $d = (c_1^2 + \cdots + c_{n-m}^2)^2$. By a simply algebraic manipulation, we get

$$(1 + b_1^2 + \cdots + b_m^2)\left(\left(\frac{c_1}{d}\right)^2 + \cdots + \left(\frac{c_{n-m}}{d}\right)^2\right) = -a$$

Thus, $-a$ is a product of the sum of $(m+1)$ squares and the sum of $(n-m)$ squares. By Corollary 3.0.12, $-a$ is a sum of n squares. This is a contradiction to Corollary 1.1.5 in Section 1.1. Hence, $s(K_a) = n + 1$, as desired. □

REFERENCES

[1] Lam, T.Y., *Introduction to Quadratic Forms Over Fields*, American Mathematical Society, Rhode Island, 2005.

[2] Lam, T.Y., *A First Course in Noncommutative Rings*, Springer-Verlag New York Inc., New York, 1991.

[3] Scharlau, W., Tschimmel, A., *On the Level of Skew-Fields*, Archiv der Mathematik, **40** (1983), 314–315.

VITA

Graduate School
Southern Illinois University

Alex Martin Date of Birth: January 31, 1989

705 West College Street, Carbondale, Illinois 62901

alexmartin8907@gmail.com

Northwestern University
Bachelor of Arts, Mathematics, June 2011

Research Paper Title:
The Level of Fields and Ordered Division Rings

Major Professor: Dr. R. Fitzgerald