Lecture Notes in Mathematics 1636

Murray A. Marshall

Spaces of Orderings and Abstract Real Spectra

Springer

Murray A. Marshall

Spaces of Orderings and Abstract Real Spectra

Springer

Author

Murray A. Marshall
Department of Mathematics and Statistics
University of Saskatchewan
Saskatoon
Canada S7N 5E6

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Marshall, Murray A.:
Spaces of orderings and abstract real spectra / Murray A. Marshall. - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1996
(Lecture notes in mathematics ; 1636)
ISBN 3-540-61729-9
NE: GT

Mathematics Subject Classification (1991): 12D15, 12J20, 14P10

ISSN 0075-8434
ISBN 3-540-61729-9 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready TEX output by the author
SPIN: 10479861 46/3144-543210 - Printed on acid-free paper

Table of Contents

Introduction

Spaces of orderings, introduced by the Author in the series of papers [53–56] [58], provide an abstract framework for studying orderings on fields and the reduced theory of quadratic forms over fields. All the main results of the theory, e.g., the isotropy theorem [10] [13] [26] [76], the representation theorem for the Witt ring [10] [26], and the structure theory for finite chain length spaces and fans [14] [15] [31], hold for spaces of orderings.

Spaces of orderings also occur naturally in other more general settings. In [32] and [85] (also see [59]) it is proved that orderings on skew fields satisfy the axioms for spaces of orderings. This has been extended to ternary fields (also called planar ternary rings); see [40]. In [42] (also see [87]) the maximal orderings on a semi-local ring are shown to form a space of orderings.

The axioms for a spaces of orderings have also been generalized in various ways, to quaternionic schemes [57] [70] (also see [35]) (an attempt to axiomatize the non-reduced theory of quadratic forms over fields), and to spaces of signatures of higher level [59] [73] [75] (an attempt to axiomatize Becker's orderings and signatures of higher level on fields).

Recently, a new sort of generalization has been found which is global in nature and really quite interesting. In [23] and [5], Bröcker and Andradas, Bröcker, and Ruiz generalize the space of orderings axioms $O_1 - O_4$, defining more general objects called abstract real spectra (also called spaces of signs in [5]), and show that these provide an abstract framework for studying orderings on a commutative ring. Any abstract real spectrum has prime ideals, and each prime ideal has associated to it a so-called residue space which is, in fact, a space of orderings. Various local-global properties can be proved. For example, the main results on minimal generation of constructible sets (in particular, the results on minimal generation of basic open sets) [21] [22] [52] [62–65] [80] hold in any abstract real spectrum.

These present notes evolved gradually, starting out initially as a long paper presenting new results in the theory of abstract real spectra. At a certain point it was decided that the material was important enough that it deserved a proper presentation to make it accessible to a wider audience. This led to the inclusion of introductory material on orderings on fields and rings as well as introductory material on spaces of orderings. At the same time as this was being done, more structure results for abstract real spectra were being obtained and new much simpler axioms were discovered and the equivalence of these axioms with Bröcker's original axioms was proved. Finally, near the end, it was pointed out by several people that these notes would be used as a standard reference not only for abstract real spectra, but also for the older theory of spaces of orderings. At this point additional material on spaces of orderings was included to make it more or less complete in this regard also.

It is also worth mentioning that, as the final touches were being applied to this manuscript, it was discovered that orderings on general noncommutative rings also satisfy the axioms for abstract real spectra [71]. The precise meaning of this result remains to be determined, but it does indicate that the abstract concept has some wider application. This application to noncommutative rings is not discussed here.

The goal of these notes then, is to introduce the reader to spaces of orderings and abstract real spectra and, at the same time, to develop enough of the associated field theory and commutative ring theory to provide motivation. An attempt is made to keep the presentation self-contained and at a reasonable level for the beginner but, at same time, the reader is expected to know elementary facts about ordered fields and valuations, and elementary commutative ring theory.

Spaces of orderings are introduced in Chap. 2. We start with the simple axioms for spaces of orderings (we call them AX2, AX2, AX3) given in the general context of spaces of signatures of higher level in [59]. The idea on which these axioms are based can be found implicitly already in [57] [70]. These axioms very natural and elegant, and also they have the advantage of being easily verified in the field situation. In this way, the presentation is self-contained, not depending on quadratic form theory [46] [79].

The results on fans and the representation theorem and the stability index (see [55]) are presented in detail in Chap. 3. Considerable effort is made to explain what these results mean in the field case; see Sect. 3.5 and 3.6. The deeper results on existence of P-structures, structure of connected components, structure of spaces of orderings of finite chain length, and the isotropy theorem (see [56]) are presented in Chap. 4. The proofs in the field case are easier and also quite enlightening, so are covered first in Sect. 4.4. Note however that the deeper results in Chap. 4 are not needed until later, at the end of Chap. 7 (in Sect. 7.7) and in Chap. 8.

In Chap. 6, we give a detailed exposition of the basic theory of abstract real spectra. The axioms we use are also referred to as AX1, AX2, AX3 (see Sect. 6.1) since they generalize directly our axioms for a space of orderings. Like the axioms for spaces of orderings, they are very natural and elegant and are easily verified in the ring situation. There are other axioms as well which are natural enough, and these are also considered. In Sect. 6.7 we consider certain alternate axioms called (α), (β), (γ), (δ) which generalize the axioms $O_1 - O_4$ given in [53–56, 58]. In the last chapter, in Sect. 8.2 we consider Bröcker's axioms [5] [23]. These also generalize $O_1 - O_4$ but in a different way. One of the main contributions of these notes is to show (and it is highly non-trivial) that these various definitions of abstract real spectra are, in fact, equivalent. This provides strong evidence that the concept is the right one (or at least close to the right one).

The most important application of the theory to date is in the "geometric case" to minimal generation of semi-algebraic sets in real algebraic varieties, and this is really quite beautiful. This is mentioned briefly here, in Chap. 7, in the general context of minimal generation of constructible sets. The focus here is always on the abstract treatment; i.e., we work with constructible sets in abstract real spectra. The reader should see [3] [5] [22] [27] [52] [80] for more concrete treatments of minimal generation of semi-algebraic sets. For the minimal generation of basic open sets, the treatment in [27] [52] is certainly the most elementary. Also, see [4] and [5] for the application to minimal generation of semi-analytic sets.

It is worthwhile making a few additional comments about Chap. 8. Abstract real spectra of finite chain length are classified in Sect. 8.5. This allows one to build a lot of abstract examples. In fact, we get "too many" examples. In Sect. 8.6 we give an additional property of real spectra in the concrete (commutative) ring situation which does not hold in general in the abstract situation. In Sect. 8.7 we give an abstract characterization of those abstract real spectra of finite chain length which are realized as real spectra of rings. The work of Delzell and Madden [33] shows that an abstract real spectrum can also fail to be realized as the real spectrum of a ring for purely topological reasons. This is discussed in Sect. 8.8.

Thus the situation with abstract real spectra is in marked contrast with the corresponding situation for spaces of orderings. There is no known example of a space of orderings which is not realized as the space of orderings of a field. On the other hand, there are many examples of abstract real spectra, even finite abstract real spectra, which are not realized as real spectra of (commutative) rings. This suggests that more axioms may be required, but it is not clear what these should be. At the same time, to complicate matters, the newly discovered examples coming from noncommutative rings still have to be investigated.

The Author wishes to thank Ludwig Bröcker for explaining his idea of abstract real spectra in various conversations over the course of several years. His preprint [23] and the joint work [5] by Andradas, Bröcker, and Ruiz were very useful. Thanks are also due to Michel Coste, Max Dickmann, and Claus Scheiderer for providing useful comments. Also, closer to home, thanks are due to Leslie Walter, Mahdi Zekavat, and Yufei Zhang for their help in reading the manuscript and locating misprints and points that needed further clarification and improvement.

Finally, before we start, here are a few words about notation which may be helpful.

The unexplained notation is more or less standard. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ denote the positive integers, the integers, the rationals, the reals, and the complex numbers respectively.

$\mathbb{Z}_2$ denotes the integers modulo 2. If G is a group of exponent 2, $\dim_2(G)$ denotes the dimension of G viewed as a vector space over $\mathbb{Z}_2$.

$|A|$ denotes the cardinality of the set A. For sets A and B,

$$A \backslash B := \{x \mid x \in A,\ x \notin B\}.$$

A^B denotes the power set, i.e., the set of all functions from B to A. If f, g are mappings, $f \circ g$ denotes the composite mapping. $f|_Y$ denotes the restriction of f to a subset Y. If S is a set of mappings,

$$S|_Y = \{f|_Y \mid f \in S\}.$$

The closure of a set Y in a topological space is denoted by $\overline{Y}$.

For k a field, $k[t_1, ..., t_n]$ denotes the ring of polynomials and $k(t_1, ..., t_n)$ the field of rational functions. $\operatorname{trdeg}(F : k)$ denotes the transcendence degree of a field extension F of k.

All rings are assumed to be commutative with 1. For A a ring, $A[t_1, ..., t_n]$ denotes the polynomial ring. $(f_1, ..., f_k)$ denotes the ideal in A generated by $f_1, ..., f_k$. $k(\mathfrak{p})$ denotes the residue field of A at a prime $\mathfrak{p}$, i.e., the field of quotients of the domain $A/\mathfrak{p}$. $S^{-1}A$ denotes the localization of A at a multiplicative set S. $A_\mathfrak{p}$ denotes localization of A at a prime $\mathfrak{p}$, i.e., at the multiplicative set $A \backslash \mathfrak{p}$. If G is a group, $A[G]$ denotes the group ring with coefficients in A.

1. Orderings on Fields

In Sect. 1.1 we introduce some of the basic terminology and recall Lang's homomorphism theorem and its application to the solution of Hilbert's 17th problem. We also give a variation of Lang's homomorphism theorem which will be useful later in our study of dimension and stability index. Sect. 1.2 contains basic facts about groups of exponent 2 and their character groups. In Sect. 1.3 we present the fundumental relationship between orderings and real places. In Sect. 1.4 we give some examples.

1.1 Lang's Homomorphism Theorem

An *ordering* on a field k is a subset $P \subseteq k$ closed under addition and multiplication, i.e., $P + P \subseteq P$, $PP \subseteq P$, such that $P \cup -P = k$, and $P \cap -P = \{0\}$. A field k is said to be *formally real* if it has an ordering. An *ordered field* is a pair (k, P) where k is a field and P is an ordering on k. The theory of ordered fields developed by Artin and Schrier is covered in basic algebra texts. Artin used properties of ordered fields in his solution of Hilbert's 17th problem.

Suppose P is an ordering of k. For any $a \in k$, either $a \in P$ or $-a \in P$. Since P is closed under multiplication, this means $a^2 = (-a)^2 \in P$. Since P is also closed under addition, this means P contains all finite sums $\sum a_i^2$, $a_i \in k$. For example, $1 = 1^2 \in P$ so P contains all positive integers (so, in particular, k has characteristic 0).

k^2 denotes the set of squares of elements of k, i.e., $k^2 := \{a^2 \mid a \in k\}$. Σk^2 denotes the set of sums of squares of elements of k, i.e., the set of finite sums $\sum a_i^2$, $a_i \in k$. Σk^2 is closed under addition and multiplication. A *preordering* in k is any subset $T \subseteq k$ such that $T + T \subseteq T$, $TT \subseteq T$, $k^2 \subseteq T$. Example: Every ordering is a preordering. Σk^2 is a preordering. Σk^2 is the unique smallest preordering of k.

Theorem 1.1.1 *If T is a preordering in a field k of characteristic $\neq 2$, and $a \in k$, $a \notin T$, then there exists an ordering P of k with $T \subseteq P$, $a \notin P$ (so k has characteristic 0).*

This is a useful result. It implies, for example, (taking $T = \Sigma k^2$, $a = -1$) that k is formally real iff $-1 \notin \Sigma k^2$.

Proof. Using the fact that T is a preordering in k, one checks that $T' := T - aT = \{s - at \mid s, t \in T\}$ is also a preordering in k.

Claim 1: $-1 \notin T'$. For, if $-1 = s - at$, $s, t \in T$, then $at = 1 + s$. If $1 + s = 0$ then $-1 = s \in T$ so $a = (\frac{a+1}{2})^2 - (\frac{a-1}{2})^2 = (\frac{a+1}{2})^2 + (-1)(\frac{a-1}{2})^2 \in T$, a contradiction. If $1 + s \neq 0$ then $t \neq 0$ so $a = \frac{1+s}{t} = (\frac{1}{t})^2(t)(1+s) \in T$, also a contradiction.

Now use Zorn's lemma to pick P any preordering of k maximal subject to the conditions $P \supseteq T'$, $-1 \notin P$.

Claim 2: P is an ordering. For, if $b \in k$, and $b \notin P$, then $P - bP$ is a preordering and, as in Claim 1, $-1 \notin P - bP$ and $P \subseteq P - bP$ so, by maximality of P, $P = P - bP$, i.e., $-b \in P$. This proves $P \cup -P = k$. If $b \in P \cap -P$, $b \neq 0$, then $-1 = (\frac{1}{b})^2(b)(-b) \in P$, a contradiction. This proves $P \cap -P = \{0\}$.

Finally, since $a \notin T$ and $0 = 0^2 \in T$, we know $a \neq 0$. Since $-a \in P$, and $P \cap -P = \{0\}$, this means $a \notin P$. Thus P has the required properties. □

It is assumed that the reader knows something about real closed fields and real closures.

Lang's work on ordered fields was motivated by the earlier work of Artin. His famous homomorphism theorem was developed to explain and simplify Artin's solution of Hilbert's 17th problem.

Theorem 1.1.2 *(Lang's homomorphism theorem) Suppose (k, Q) is an ordered field with real closure R and suppose D is a finitely generated k-algebra which is an integral domain and that the ordering Q extends to an ordering in the quotient field of D in some way. Then*

(1) There exists a k-algebra homomorphism $\phi : D \to R$.

(2) More generally, if $a_1, \dots, a_m \in D$ are positive in this extended ordering then there exists a k-algebra homomorphism $\phi : D \to R$ such that $\phi(a_i) > 0$, $i = 1, \dots, m$.

Lang's homomorphism theorem, properly viewed, is just a weak version of Tarski's transfer principle. The proof given below illustrates this fact:

Proof. Let F be the quotient field of D, let P be the fixed extension of Q to F, and let R' be the real closure of the ordered field (F, P). Since D is a finitely generated k-algebra which is a domain, $D \cong \frac{k[x_1,\dots,x_n]}{\mathfrak{p}}$ for some prime ideal $\mathfrak{p} \subseteq k[x_1, \dots, x_n]$. By the Hilbert Basis Theorem (e.g., see [8]), the ideal $\mathfrak{p}$ is finitely generated, say $\mathfrak{p} = (g_1, \dots, g_s)$, $g_i \in k[x_1, \dots, x_n]$, $i = 1, \dots, s$. Finding a k-algebra homomorphism $\phi : D \to R$ just amounts to finding a point $(b_1, \dots, b_n) \in R^n$ such that $g_i(b_1, \dots, b_n) = 0$, $i = 1, \dots, s$. We know there exists such a point in R'^n, namely the point $(x_1 + \mathfrak{p}, \dots, x_n + \mathfrak{p})$, so the existence of $(b_1, \dots, b_n)$ follows from Tarski's transfer principle. This proves (1).

(2) can also be deduced from the transfer principle, but it can also be deduced from (1) as follows: Since $a_i > 0$, $\sqrt{a_i} \in R'$, $i = 1, ..., m$. Let $D' = D[\frac{1}{\sqrt{a_1}}, ..., \frac{1}{\sqrt{a_m}}] \subseteq R'$. Applying (1), we obtain a k-algebra homomorphism $\phi : D' \to R$. Thus $\sqrt{a_i} = a_i \frac{1}{\sqrt{a_i}} \in D'$ and $\phi(\sqrt{a_i})\phi(\frac{1}{\sqrt{a_i}}) = \phi(1) = 1$ so $\phi(\sqrt{a_i}) \neq 0$. Thus $\phi(a_i) = (\phi(\sqrt{a_i}))^2 > 0$, $i = 1, ..., m$. □

For the reader not familiar with the transfer principle, other proofs of Lang's homomorphism theorem are available (e.g., the proof in [49]), but these proofs are also complicated. Rather than read these other proofs, the beginner is probably better off to read the elementary proof of quantifier elimination given in [12]. Some knowledge of model theory is helpful here, but not absolutely necessary. Once quantifier elimination is established, the transfer principle (and consequently, Lang's homomorphism theorem) follow as immediate corollaries. Quantifier elimination is a standard tool in real algebraic geometry, so one needs it in any case if one wants to pursue this area of study.

Corollary 1.1.3 *(Solution of Hilbert's 17th problem) Suppose (k, Q) is an ordered field and R is some real closed extension of (k, Q) (so $R^2 \cap k = Q$ where $R^2 := \{a^2 \mid a \in R\}$). Suppose $f \in k[x_1, ..., x_n]$ satisfies $f(a_1, ..., a_n) \geq 0$ for all $(a_1, ..., a_n) \in R^n$. Then f is expressible as $f = \sum_{i=1}^{s} r_i f_i^2$ for some $f_1, ..., f_s \in k(x_1, ..., x_n)$, $r_1, ..., r_s \in Q$.*

Proof. Let T denote the set of finite sums $\sum_{i=1}^{s} r_i f_i^2$, $f_1, ..., f_s \in k(x_1, ..., x_n)$, $r_1, ..., r_s \in Q$. This is a preordering in the rational function field $k(x_1, ..., x_n)$. If $f \notin T$ then, by 1.1.1, we have an ordering P of $k(x_1, ..., x_n)$ with $P \supseteq T$ such that $f \notin P$. Clearly $P \supseteq Q$ so $P \cap k = Q$, i.e., P extends Q. Applying Lang's homomorphism theorem (2) to the polynomial ring $k[x_1, ..., x_n]$, we get a k-algebra homomorphism $\phi : k[x_1, ..., x_n] \to R$ such that $\phi(f) < 0$. Letting $a_i = \phi(x_i)$, $i = 1, ..., n$, we see that $\phi(f) = f(a_1, ..., a_n)$. Thus $f(a_1, ..., a_n) < 0$. □

From the point of view of these notes, Lang's homomorphism theorem is central and, at the same time, peripheral. It is required (only) to motivate the definition of real spectra and to understand the application of the results on minimal generation of constructible sets (in Chap. 7) to real algebraic geometry.

Also, the following version of Lang's homomorphism theorem will be useful, later on, to understand the meaning of the stability index (Sect. 3.6) and dimension (Sect. 7.3) in the concrete setting of real algebraic geometry.

Theorem 1.1.4 *Suppose (k, Q) is an ordered field, F is a finitely generated field extension of transcendence degree $d \geq 1$ over k which has an ordering extending Q, and $D \subseteq F$ is any finitely generated k-algebra of transcendence* *degree d over k. Then there exists a discrete valuation ring B in F with $D \subseteq B$ such that the residue field $\overline{F}$ of B is a finitely generated field extension of transcendence degree $d-1$ over k which has an ordering extending Q, and the image of D under the mapping $B \to \overline{F}$ is a finitely generated k-algebra of transcendence degree $d-1$ over k.*

Proof. By Noether normalization [8, p. 169], there exists a transcendence basis $x_1, ..., x_d$ in D such that D is integral over $k[x_1, ..., x_d]$. Let $k_1 = k(x_1, ..., x_{d-1})$, so $\text{trdeg}(F : k_1) = 1$, and let $E =$ the integral closure of $k_1[x]$ in F, where $x = x_d$. E is a Dedekind domain [8, Chap. 9] and is finitely generated as a k_1-algebra (since it is even finitely generated as a $k_1[x]$-module; see [8, Prop. 5.17, p. 64]). Let P be a fixed ordering on F extending Q and let R_1 be a real closure of k_1 at the induced ordering $P_1 = P \cap k_1$. According to Lang's homomorphism theorem, there exists a k_1-algebra homomorphism $\alpha : E \to R_1$. Let $\mathfrak{p} = \ker(\alpha)$. Then $\mathfrak{p}$ is a maximal ideal of E so the local ring $E_\mathfrak{p}$ is a discrete valuation ring in F [8, Th. 9.3, p. 95]. Take $B = E_\mathfrak{p}$. Since $k[x_1, ..., x_d] \subseteq E$ and E is integrally closed in F, it follows that $D \subseteq E \subseteq E_\mathfrak{p}$. The residue field of $E_\mathfrak{p}$ is $\overline{F} = E_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \cong E/\mathfrak{p} \cong \alpha(E) \subseteq R_1$. This is a finite extension of $k_1[x]/(f)$ where $(f) = \mathfrak{p} \cap k_1[x]$ which, in turn, is a finite extension of $k_1 = k(x_1, ..., x_{d-1})$. Thus $x_1, ..., x_{d-1}$ is a transcendence basis of $\overline{F}$ over k. Since $x_1, ..., x_{d-1}$ are in the image of D, the proof is complete. □

1.1 Characters on groups of exponent 2

We need some elementary facts about groups of exponent 2 and their character groups.

A group of *exponent* 2 is a (necessarily abelian) group G satisfying $a^2 = 1$ $\forall\, a \in G$. A *character* on a group G of exponent 2 is a group homomorphism $x : G \to \{-1, 1\}$. The *character group* of a group G of exponent 2 is $\chi(G) := \text{Hom}(G, \{-1, 1\})$, the set of all characters on G, with the group operation defined pointwise, i.e., $(xy)(a) := x(a)y(a)$ for all $a \in G$.

Any group G of exponent 2 is a direct sum of κ cyclic groups of order 2, where κ is some cardinal number, and the character group $\chi(G)$ is the direct product of κ cyclic groups of order 2 (same κ). In particular, if κ is finite, then $\chi(G) \cong G$ (non-canonically). Perhaps the easiest way to understand this is to write the operation on G as $+$ so the condition that G has exponent 2 is that $2a = 0$ $\forall a \in G$, i.e., a group of exponent 2 is just a vector space over the 2-element field $\mathbb{Z}_2 = \frac{\mathbb{Z}}{2\mathbb{Z}}$. Viewed in this way, the cardinal number κ is just the dimension of G (we denote this dimension by $\dim_2(G)$), and $\chi(G)$ is just the dual space of G. Note: If κ is infinite, then the dimension of $\chi(G)$ is strictly greater than κ.

If G is a group of exponent 2, then $\chi(G)$ has a natural topology making it into a topological group. The topology is just the weakest such that the mappings $x \mapsto x(a)$, $a \in G$, are continuous, giving $\{-1,1\}$ the discrete topology. Saying that $\chi(G)$ is a topological group just means that the topology is Hausdorff and the mappings $(x,y) \mapsto xy$, $x \mapsto x^{-1}$ on $\chi(G)$ are continuous. Of course, since the exponent is 2, $x^{-1} = x$ so the second mapping is just the identity.

Proposition 1.2.1 *For any group G of exponent 2:*

(1) $\chi(G)$ is compact.

(2) For each subgroup H of G, $\chi(G/H)$ is a closed subgroup of $\chi(G)$.

(3) Conversely, if S is any closed subgroup of $\chi(G)$ then $S = \chi(G/H)$ where $H = \cap_{x\in S} \ker(x)$.

Note: We are identifying characters of G/H with characters of G containing H in their kernel.

Proof. (1) Denote by $\{-1,1\}^G$ the set of all functions from G to $\{-1,1\}$ with the product topology, giving $\{-1,1\}$ the discrete topology. Then $\chi(G) \subseteq \{-1,1\}^G$ and the topology on $\chi(G)$ is the induced topology. Since $\{-1,1\}^G$ is compact by Tychonoff's theorem, it suffices to check that $\chi(G)$ is closed in $\{-1,1\}^G$. Suppose $x \in \{-1,1\}^G$ is in the closure of $\chi(G)$. For each $a, b \in G$, the set

$$U = \{y \in \{-1,1\}^G \mid y(a) = x(a), y(b) = x(b), y(ab) = x(ab)\}$$

is a neighbourhood of x in $\{-1,1\}^G$. Thus $U \cap \chi(G) \neq \emptyset$, say $y \in U \cap \chi(G)$. Then $y(ab) = y(a)y(b)$ so $x(ab) = y(ab) = y(a)y(b) = x(a)x(b)$. This proves x is a character of G, so $x \in \chi(G)$.

(2) $\chi(G/H)$ is compact by (1) so it is closed in $\chi(G)$.

(3) It is clear that $S \subseteq \chi(G/H)$. Replacing G by G/H, we are reduced to the case where $H = \{1\}$. Thus we are assuming $S \subseteq \chi(G)$ is a closed subgroup such that $\cap_{x\in S} \ker(x) = \{1\}$, and we want to show $S = \chi(G)$.

It suffices to handle the case where G is finite. Suppose K is any finite subgroup of G and denote by $S|_K$ the set of restrictions $x|_K$, $x \in S$. This is a subgroup of $\chi(K)$ and $\cap_{x\in S} \ker(x|_K) = \{1\}$. Thus, if we know the result in the finite case, then $S|_K = \chi(K)$. This means that, for each $y \in \chi(G)$ and each finite subgroup K of G, there exists $x \in S$ such that $x|_K = y|_K$. Since S is closed in $\chi(G)$, this implies $S = \chi(G)$.

So suppose G is finite (so the topology is discrete). Let $\{x_1, ..., x_n\}$ be a subset of S chosen minimal such that $\cap_{i=1}^n \ker(x_i) = \{1\}$. Consider the chain of subgroups

$$G \supseteq \ker(x_1) \supseteq \ker(x_1) \cap \ker(x_2) \supseteq \dots \supseteq \cap_{i=1}^n \ker(x_i) = \{1\}.$$

For $j = 1, ..., n$, $\ker(x_j)$ has index 2 in G and $\cap_{i=1}^{j-1} \ker(x_i) \not\subseteq \ker(x_j)$ by the minimal choice of the subset $\{x_1, ..., x_n\}$. Thus $(\cap_{i=1}^{j-1} \ker(x_i)) \cdot \ker(x_j) = G$ so

$$\frac{\cap_{i=1}^{j-1}\ker(x_i)}{\cap_{i=1}^{j}\ker(x_i)} \cong \frac{(\cap_{i=1}^{j-1}\ker(x_i))\cdot\ker(x_j)}{\ker(x_j)} = \frac{G}{\ker(x_j)}.$$

This means $\cap_{i=1}^{j}\ker(x_i)$ has index 2 in $\cap_{i=1}^{j-1}\ker(x_i)$, $j = 1, ..., n$, so $\{1\} = \cap_{i=1}^{n}\ker(x_i)$ has index 2^n in G, i.e., $|G| = 2^n$. Thus, by counting, we see that the natural injection $G \hookrightarrow \prod_{i=1}^{n} G/\ker(x_i)$ is surjective so we get elements $a_1, ..., a_n$ in G such that $x_i(a_j) = -1$ if $i = j$ and 1 otherwise. Clearly $a_1, ..., a_n$ are a $\mathbb{Z}_2$-basis of G, i.e., every element $a \in G$ is expressible uniquely as $a = \prod_{i=1}^{n} a_i^{e_i}$, $e_i \in \{0,1\}$. Also it is clear that $x_1, ..., x_n$ is just the dual basis of $\chi(G)$. Since $x_1, ..., x_n$ are in S, this means $S = \chi(G)$. □

A topological space X is called a *Boolean space* if it is compact and Hausdorff and the clopen (i.e., both closed and open) sets form a basis for the topology. For example, if G is a group of exponent 2 then $\chi(G)$ is a Boolean space. Boolean spaces are also characterized as compact Hausdorff spaces which are totally disconnected (i.e., the connected components are singleton sets). This is a consequence of the following general result which we record now for future use:

Lemma 1.2.2 *For any compact topological space X which is normal (i.e., disjoint closed sets can be separated), the connected component of any $x \in X$ is the intersection of all clopen sets in X containing x.*

Note: We are not assuming X is Hausdorff. If X is Hausdorff then compact implies normal.

Proof. Let $x \in X$ and let $Z \subseteq X$ be the intersection of all clopen sets containing x. Clearly the connected component of x is contained in Z. If we show that Z is connected, it will follow that Z is the connected component of x and we will be done. Suppose this is false so we have non-empty closed sets Z_1, Z_2 in Z with $Z_1 \cup Z_2 = Z$, $Z_1 \cap Z_2 = \emptyset$. Z is closed in X since it is the intersection of clopen sets, so Z_1, Z_2 are closed in X. Since X is normal, there exist disjoint open sets U_1, U_2 in X with $U_i \supseteq Z_i$, $i = 1, 2$. Consider the closed sets $X \backslash U_1$, $X \backslash U_2$. Then $(X\backslash U_1) \cap (X \backslash U_2) \cap Z = \emptyset$ so by compactness, $(X\backslash U_1) \cap (X\backslash U_2) \cap Y = \emptyset$ for some clopen set Y in X with $Z \subseteq Y$. Y decomposes as a disjoint union of two non-empty open sets $Y = (U_1 \cap Y) \cup (U_2 \cap Y)$. This means $U_1 \cap Y$ and $U_2 \cap Y$ are clopen in Y (and hence in X). Say $x \in U_1 \cap Y$. Then $U_1 \cap Y$ is a clopen set containing x and $Z \not\subseteq U_1 \cap Y$ which contradicts the definition of Z. □

1.3 Orderings and Real Places

Elementary results in the model theory of real closed fields, e.g., the transfer principle, tend to emphasize points of similarity between ordered fields, but two ordered fields can be quite different in important aspects. To understand these differences one has to go to the arithmetic of the field, specifically, to the associated real places.

In these notes the focus is not on a single ordering so much but rather on the set of all orderings on a field k. In the final analysis, orderings on k come from the unique ordering on the field of real numbers via the real places $\alpha : k \to \mathbb{R} \cup \{\infty\}$. This was noticed first by Krull and Baer, and we explain this now in detail; also see [48].

First we recall some terminology. A *valuation ring* in a field k is a subring $B \subseteq k$ such that for all $a \in k^* := k\backslash\{0\}$, either $a \in B$ or $\frac{1}{a} \in B$. Any valuation ring B is a local ring with $\mathfrak{m} = \{a \in k^* \mid \frac{1}{a} \notin B\} \cup \{0\}$ as its unique maximal ideal and $U = \{a \in k^* \mid a, \frac{1}{a} \in B\} = B\backslash\mathfrak{m}$ as its unit group. The field $\overline{k} = B/\mathfrak{m}$ is called the *residue field* of B. A *place* from k to some other field k' is a ring homomorphism $\alpha : B \to k'$ where B is a valuation ring in k with kernel $= \mathfrak{m} =$ the maximal ideal of B (so $\alpha : B \to k'$ factors uniquely as $\alpha = \overline{\alpha} \circ p$ where $p : B \to \overline{k} = B/\mathfrak{m}$ is the homomorphism to the residue field and $\overline{\alpha} : \overline{k} \hookrightarrow k'$ is some embedding). Normally, we extend the place α to a function $\alpha : k \to k' \cup \{\infty\}$ (where ∞ is a symbol not in k') by defining $\alpha(a) = \infty$ if $a \in k\backslash B$. A valuation ring B in k is said to be *trivial* if $B = k$ (so $\mathfrak{m} = \{0\}$). A place is said to be *trivial* if the associated valuation ring is trivial, i.e., a trivial place $\alpha : k \to k' \cup \{\infty\}$ is just an embedding $\alpha : k \hookrightarrow k'$. We say a place $\alpha : k \to k' \cup \{\infty\}$ is *real* if $k' = \mathbb{R}$, the usual field of real numbers. (This terminology is not standard. Most people require only that k' is formally real.)

Notes. (1) Suppose B, B' are valuation rings in k with maximal ideals $\mathfrak{m}, \mathfrak{m}'$ respectively. Then $B' \subseteq B \Leftrightarrow \mathfrak{m} \subseteq \mathfrak{m}'$ and, in this case, $\mathfrak{m}$ is a prime ideal of B' and $\frac{B'}{\mathfrak{m}}$ is a valuation ring in $\overline{k} = \frac{B}{\mathfrak{m}}$ with maximal ideal $\frac{\mathfrak{m}'}{\mathfrak{m}}$ and residue field $\frac{B'}{\mathfrak{m}}/\frac{\mathfrak{m}'}{\mathfrak{m}} \cong \frac{B'}{\mathfrak{m}'}$. Moreover, $B' \leftrightarrow \frac{B'}{\mathfrak{m}}$ defines a one-to-one correspondence between valuation rings in k contained in B and valuation rings in $\overline{k}$.

(2) Of course, if B' is a discrete valuation ring then $\{0\}, \mathfrak{m}'$ are the only prime ideals of B' so, if $B' \subseteq B$, then either $\mathfrak{m} = \{0\}$ (so $B = k$) or $\mathfrak{m} = \mathfrak{m}'$ (so $B = B'$).

(3) If $\alpha : k \to k' \cup \{\infty\}$ is a place and $\alpha^{-1}(k') \subseteq B$, then α factors as $\alpha = \overline{\alpha} \circ p$ where $p : B \to \overline{k} = \frac{B}{\mathfrak{m}}$ is the natural homomorphism and $\overline{\alpha}$ is some (necessarily unique) place from $\overline{k}$ to k'. This is clear from (1).

Suppose now that P is an ordering on k. We say P is *archimedian* if for each $a \in k$ there exists an integer $n \geq 1$ (depending on a) such that $n - a, n + a \in P$. If P is archimedian, there is a unique embedding $\alpha : k \hookrightarrow \mathbb{R}$

such that $P = \alpha^{-1}(\mathbb{R}^2)$. Here $\mathbb{R}^2 := \{a^2 \mid a \in \mathbb{R}\}$, the unique ordering on $\mathbb{R}$. For $a \in k$, $\alpha(a) = \inf\{r \in \mathbb{Q} \mid r-a \in P\} = \sup\{r \in \mathbb{Q} \mid a-r \in P\}$ where $\mathbb{Q} =$ the field of rational numbers. In this case, the real place associated to P is just the trivial place $\alpha : k \hookrightarrow \mathbb{R}$. On the other hand, if P is non-archimedian, set $B_P = \{a \in k \mid n-a, n+a \in P \text{ for some integer } n \geq 1\}$. It is easy to check that B_P is a valuation ring in k and that $\mathfrak{m}_P := \{a \in k \mid \frac{1}{n} - a, \frac{1}{n} + a \in P \text{ for all positive integers } n\}$ is the maximal ideal of B_P. Also, P induces an ordering $\overline{P}$ on the residue field $\overline{k} := B_P/\mathfrak{m}_P$ given by $\overline{P} = \{a + \mathfrak{m}_P \mid a \in B_P \cap P\}$ and $\overline{P}$ is archimedian, so we get a unique embedding $\overline{\alpha} : \overline{k} \hookrightarrow \mathbb{R}$ such that $\overline{\alpha}^{-1}(\mathbb{R}^2) = \overline{P}$. Composing $\overline{\alpha}$ with the natural homomorphism from B_P to $\overline{k}$ gives a real place $\alpha : k \to \mathbb{R} \cup \{\infty\}$ given by

$$\alpha(a) = \begin{cases} \infty & \text{if } a \notin B_P \\ \overline{\alpha}(a + \mathfrak{m}_P) & \text{if } a \in B_P. \end{cases}$$

Note: If P is archimedian then $B_P = k$, $\mathfrak{m}_P = \{0\}$, $\overline{k} = k$, and $\overline{\alpha} = \alpha$.

Notation. We denote the real place $\alpha : k \to \mathbb{R} \cup \{\infty\}$ constructed in this way from the ordering P by $\lambda(P)$.

Conversely, suppose $\alpha : k \to \mathbb{R} \cup \{\infty\}$ is any real place. Let $B = \{a \in k \mid \alpha(a) \neq \infty\}$. Thus B is a valuation ring of k with maximal ideal $\mathfrak{m} = \{a \in k \mid \alpha(a) = 0\}$. Let U denote the unit group of B, i.e., $U = B \backslash \mathfrak{m}$ and let $U^+ = \{a \in U \mid \alpha(a) > 0\}$. U^+ is a subgroup of U and $-1 \notin k^{*2}U^+$. (If $-1 = a^2 b$, $a \in k^*$, $b \in U^+$, then $a \in U$ so, applying α, $-1 = \alpha(a)^2\alpha(b) > 0$, a contradiction.) There are, in general, many orderings P such that $\lambda(P) = \alpha$, but they are all obtained by a simple process. Pick any subgroup $P^* \subseteq k^*$ containing $k^{*2}U^+$ such that $-1 \notin P^*$.

Claim 1. $P := P^* \cup \{0\}$ is a preordering in k. (In particular, $k^2U^+ = k^{*2}U^+ \cup \{0\}$ is a preordering in k.) Clearly $PP \subseteq P$. Showing $P + P \subseteq P$ is less trivial. Suppose $a, b \in P$. We want to show $a + b \in P$. This is clear if $a = 0$ or $b = 0$, so we can assume $a, b \in P^*$. Either $\frac{a}{b} \in B$ or $\frac{b}{a} \in B$. Interchanging a, b if necessary, we can assume $\frac{b}{a} \in B$. We claim $1 + \frac{b}{a} \in U^+$. For otherwise, applying α, we get $\alpha(\frac{b}{a}) \leq -1$ so $-\frac{b}{a} \in U^+ \subseteq P^*$ which is a contradiction because P^* is a group, $\frac{b}{a} \in P^*$, $-1 \notin P^*$. Thus $a + b = a(1 + \frac{b}{a}) \in P^*U^+ \subseteq P^*P^* \subseteq P^*$. This proves $P + P \subseteq P$, so P is a preordering.

Claim 2. Suppose, in addition, that P^* is maximal subject to the condition $-1 \notin P^*$. Then $P = P^* \cup \{0\}$ is an ordering in k and $\lambda(P) = \alpha$. If $a \in k^*$, $a \notin P$, then, since $k^{*2} \subseteq P^*$, $P^* \cup aP^*$ is a subgroup of k^* and clearly $P^* \subsetneq P^* \cup aP^*$ so $-1 \in P^* \cup aP^*$. Since $-1 \notin P^*$, this means $-1 \in aP^*$, i.e., $a \equiv -1 \bmod P^*$. This proves $P^* \cup -P^* = k^*$, so $P \cup -P = k$. Also, $P^* \cap -P^* = \emptyset$ so $P \cap -P = \{0\}$. This proves P is an ordering.

If $a \notin B$, then $\frac{1}{a} \in \mathfrak{m}$. Thus $\alpha(\frac{1}{n} \pm \frac{1}{a}) = \frac{1}{n} > 0$ so $\frac{1}{n} \pm \frac{1}{a} \in U^+ \subseteq P$. This proves $\frac{1}{a} \in \mathfrak{m}_P$ so $a \notin B_P$. This proves $B_P \subseteq B$. Suppose $a \in B$. Then $\alpha(a) \neq$