

MINIMAL GENERATION OF CONSTRUCTIBLE SETS IN THE REAL SPECTRUM OF A RING

Murray A. Marshall

I. THE REAL SPECTRUM OF A COMMUTATIVE RING

1. Preorderings, semi-preorderings
2. Orderings and semi-orderings
3. Semi-orderings and valuations
4. Nullstellensatz, positivstellensatz
5. Compactness
6. Description of closure
7. The Hörmander-Lojasiewicz inequality
8. Basic constructible sets

II. CONSTRUCTIBLE SETS AND SEMI-ALGEBRAIC SETS

1. The basic correspondence
2. Finiteness theorem
3. Dimension

III. ORDERINGS, VALUATIONS, AND QUADRATIC FORMS

1. Quadratic forms
2. Baer-Krull-Springer theorem
3. Criterion for T -isotropy

IV. MINIMAL GENERATION OF CONSTRUCTIBLE SETS

1. Pfister forms
2. The stability index
3. Complexity of basic open sets
4. Complexity of basic closed sets
5. Bröcker's t -invariant
6. Complexity of general constructible sets

V. APPLICATION TO REAL ALGEBRAIC GEOMETRY

1. Behaviour of stability under field extension
2. Application to finitely generated algebras

These notes provide a short self-contained introduction to Ludwig Bröcker's theory of complexity of constructible sets in the real spectrum of a ring and to the associated theory of complexity of semi-algebraic sets in real algebraic varieties. The theory has only just recently evolved to the point where this sort of presentation is possible [12], [13], [20], [21], [22], [24], the main breakthrough being due to Ludwig Bröcker and Claus Scheiderer in 1987.

This material is accessible to anyone familiar with elementary commutative algebra, as presented in [2], say, and the theory of real closed fields (including quantifier elimination and the transfer principle), as in [5, Chapters 1 and 5], say.

A basic difference between the real spectrum and the ordinary (prime) spectrum of a ring is seen vividly by looking at the field case. The prime spectrum of a field is a trivial object (just a single point) but the real spectrum of a field can be highly non-trivial. Thus the reader should not be surprised to find that about half of the presentation is field theory. The main tool to be developed here is the interrelationship between orderings, valuations, and quadratic forms [4], [6], [17], [23]; see Part III.

The presentation is divided into five parts. Parts I and II introduce the reader to the real spectrum, and establish the relationship between constructible sets and semi-algebraic sets. Most of this material is found in [3], [5], [16], [18], but in a slightly different form. Parts I and III, when taken together, contain the prerequisites to Part IV which is the heart of the subject. In Part IV one learns (in summary) that the complexity of constructible sets depends only on certain "stability indices" of the residue fields and further, that these indices can be computed by valuation theory. Part V gives the application to semi-algebraic sets.

In the interests of brevity, many important parts of the theory are not included (e.g., the application to complexity of semi-analytic sets [1]). The Author decided that the goal of making available a short self-contained introduction should override other considerations. In any case, the book by Andradas, Bröcker, and Ruiz which is scheduled to appear soon will make up for these

deficiencies.

The Author wishes to thank the organizers for inviting him to present this material at the XII Escola de Álgebra, Diamantina, Brasil, 1992. The Author also wishes to thank Leslie Walter for her contribution to these notes.

This latest version of these notes grew out of a seminar given at the University of Saskatchewan in 1993. It contains an introduction which was not present in some of the earlier versions, and the order in which topics are presented has been changed.

1. Introduction

Let K be a field, $F \subseteq K$ any subfield. Denote the polynomial ring $F[X_1, \dots, X_N]$ by $F[X]$ for short. Let V be an algebraic set in K^N defined over F , so V has the form

$$V = \{x \in K^N : h_i(x) = 0, i = 1, \dots, k\}$$

for some polynomials $h_1, \dots, h_k \in F[X]$, $k \geq 0$. Recall: algebraic sets are also called algebraic varieties.

In algebraic geometry one usually assumes K is algebraically closed (e.g., $K = \mathcal{O}$) and one is interested in subsets of V defined by polynomial equations $f = 0$ and polynomial inequalities $f \neq 0$, $f \in F[X]$. These are studied by looking at the F -algebra

$$A = \frac{F[X]}{(h_1, \dots, h_k)}.$$

Each point $x \in V$ determines a ring homomorphism $A \rightarrow K$, $f \mapsto f(x)$. This has image $F[x] \subseteq K$ and kernel $p_x := \{f \in A : f(x) = 0\}$. Thus $A/p_x \cong F[x]$, so the *residue field* at x , i.e., the field of quotients of the domain A/p_x , is isomorphic to the finitely generated field extension $F(x) \subseteq K$. $\text{Spec } A$ denotes the (prime) *spectrum* of A , i.e., the set of prime ideals of A . Since p_x is a prime ideal for each $x \in V$, we have a mapping

$$\Psi : V \rightarrow \text{Spec } A, x \mapsto p_x.$$

Various properties of V are reflected by properties of $\text{Spec} A$. For example, if $f \in A$, the set of solutions of the equation $f = 0$ in $\text{Spec} A$ is (by definition) the set

$$\{p \in \text{Spec} A : f \in p\}.$$

In real algebraic geometry, on the other hand, one assumes K is real closed (e.g., $K = \mathbb{R}$) and one is interested in subsets of V defined by polynomial equations $f = 0$ and inequalities $f > 0$, $f \in F[X]$. These are the so-called *semi-algebraic sets* (more precisely, *semi-algebraic sets defined over F*). To study these one needs the *real spectrum* of A . This is denoted by $\text{Sper} A$. The key here is to observe that, for $x \in V$, the residue field $F(x)$ is ordered by the natural ordering $P_x := F(x) \cap K^2$ induced by $F(x) \subseteq K$. Motivated by this, one defines the *real spectrum* of A to be the set of all pairs (q, Q) , where $q \subseteq A$ is a prime ideal and Q is an ordering on the residue field at q (= the quotient field of the domain A/q). Thus, we have a mapping

$$\Phi : V \rightarrow \text{Sper} A, \quad x \mapsto (p_x, P_x).$$

Now various properties of V , including “real” properties, are reflected by properties of $\text{Sper} A$. For example, for $f \in A$, it makes sense to talk about the set of solutions of the inequality $f > 0$ in $\text{Sper} A$. In this way, we have a certain class of subsets of $\text{Sper} A$, called *constructible sets*, corresponding to the semi-algebraic sets in V .

It turns out that, to get an accurate reflection of the properties of V , the real spectrum is a bit too large. Let P denote the ordering on F induced by K , i.e., $P = F \cap K^2$. Then we have a certain subset $X_T \subseteq \text{Sper} A$ corresponding to the preordering $T := \sum A^2 P$. This terminology will be explained later. In concrete terms, X_T consists of all pairs (q, Q) as above, but with Q extending P . For each $x \in V$, P_x extends P , so we have

$$\Phi : V \rightarrow X_T \subseteq \text{Sper} A, \quad x \mapsto (p_x, P_x).$$

Of course, if F is uniquely ordered, then $X_T = \text{Sper} A$, so there is no need for this extra adjustment.

Remark Actually, the proof that X_T “accurately reflects” properties of V is quite complicated: it uses Tarski’s transfer principle for real closed fields; see Theorems 2.1 and 2.4 below.

Hopefully, the above discussion will serve to motivate the reader to learn more about the real spectrum and to understand how this knowledge can be applied to study problems in real algebraic geometry.

The special problem we have in mind (and the main problem being considered in these notes) is the problem of minimal generation of semi-algebraic sets. This is described nicely in Bröcker’s survey article [12]. We conclude this introduction by giving a partial description of this problem.

We continue to assume that K is real closed. If one is given a subset of V of the form

$$S = \{x \in V : f_i(x) = 0, i = 1, \dots, n\}, \quad f_1, \dots, f_n \in A,$$

then one can ask for the minimum number of equations required to describe S . The answer is trivial: $S = \{x \in V : f(x) = 0\}$, where $f = \sum_{i=1}^n f_i^2$, so S can be described by a single polynomial equation. Similarly, the set

$$S = \{x \in V : f_i(x) \neq 0, i = 1, \dots, n\}$$

can be described by a single inequality: $S = \{x \in V : f(x) \neq 0\}$, where $f = \prod_{i=1}^n f_i$.

On the other hand, if one replaces $=, \neq$ by $>$ or \geq , the question is highly non-trivial. For example, what is the minimal number of inequalities $f > 0$ required to describe a *basic open set*

$$S = \{x \in V : f_i(x) > 0, i = 1, \dots, n\}, \quad f_1, \dots, f_n \in A?$$

Examples

- (1) The triangle in \mathbb{R}^2 defined by the three inequalities $x > 0, y > 0, 1 > x+y$ can be described equally well by two inequalities $xy > 0, (x+y-1)(x+y) < 0$.

- (2) The half-line in \mathbb{R} defined by $x^2 > 2, x > 0$ can be described by a single inequality $x > \sqrt{2}$ over \mathbb{R} but, over \mathbb{Q} , two inequalities are required.

The reader might guess that the number of inequalities required is bounded above by the dimension d of V . After all, in Example (1), $V = \mathbb{R}^2$ is 2-dimensional, and, in Example (2), $V = \mathbb{R}$ is 1-dimensional. On the other hand, in Example (2), if $F = \mathbb{Q}$, then two inequalities are required (since the polynomials in question are required to have coefficients in F).

It turns out that the bound is $d + \bar{s}_P + \delta_P$, where \bar{s}_P, δ_P are certain invariants of the ordered field (F, P) ; see Theorem 5.6 (1) below. If (F, P) is real closed, then $\bar{s}_P = \delta_P = 0$. On the other hand, if $F = \mathbb{Q}$, then $\bar{s}_P = 0, \delta_P = 1$. This explains the slightly bigger bound required in Example (2) in case $F = \mathbb{Q}$.

This is a very nice result but, at the same time, it is perhaps somewhat surprising since, intuitively, it is not clear why such a bound should even exist. e.g., consider the following:

Question. In \mathbb{R}^2 , how does one go about describing the interior of a given convex polygon using just two polynomial inequalities?

From the viewpoint of algebraic geometry, Theorem 5.6 is the main theorem proved in these notes. The reader will observe that Theorem 5.6 has four parts (all equally interesting) and that we have only looked at one of these parts here. But hopefully this is enough to give the reader some idea of what these notes are about.

As one might expect, the proof of Theorem 5.6 is also interesting. This proof is carried out entirely in the context of constructible sets, working in the subset $X_T \subseteq \text{Sper } A$ discussed above (i.e., $T = \sum A^2 P$), and is then transferred back to V via the mapping $\Phi : V \rightarrow X_T$. Actually, most of this theory of minimal generation of constructible sets holds for any ring A , commutative with 1, and any preordering $T \subseteq A$; see Part IV. It is only in Part V that specialization is made to the case where A is a finitely generated F -algebra, and $T = \sum A^2 P$.

I THE REAL SPECTRUM OF A COMMUTATIVE RING

1. Preorderings, semi-preorderings

Throughout, A denotes a ring (always assumed to be commutative with 1). For a prime $p \subseteq A$, $F(p)$ denotes the *residue field* of A at p , i.e., the quotient field of the domain A/p .

Note

- (1) Primes in a localization $\Sigma^{-1}A$ (where $\Sigma \subseteq A$ is a multiplicative set) have the form $\Sigma^{-1}p$ where $p \subseteq A$ is prime, $p \cap \Sigma = \emptyset$, and, in this situation, $F(\Sigma^{-1}p) \cong F(p)$.
- (2) Similarly, primes in a factor ring A/I have the form $\bar{p} = p/I$ where $p \subseteq A$ is a prime containing I , and $F(\bar{p}) \cong F(p)$.

A subset $T \subseteq A$ is called a *preordering* if $T + T \subseteq T$, $TT \subseteq T$, and $A^2 \subseteq T$. (Here, $A^2 := \{a^2 : a \in A\}$). T is called *proper* if $-1 \notin T$. $\sum A^2$ denotes the set of all finite sums $a_1^2 + \dots + a_n^2$, $a_1, \dots, a_n \in A$, $n \geq 1$. This is a preordering. Moreover, $\sum A^2 \subseteq T$ holds for any preordering $T \subseteq A$.

Note. If A has a proper preordering then $-1 \notin \sum A^2$ (so, in particular, $\text{Char } A = 0$). Conversely, if $-1 \notin \sum A^2$, then $\sum A^2$ itself is a proper preordering in A .

More generally, a subset S of A will be called a *semi-preordering* if $S + S \subseteq S$, $A^2S \subseteq S$, and $1 \in S$. S is said to be *proper* if $-1 \notin S$. Note: Since $1 \in S$ and $A^2S \subseteq S$, $\sum A^2 \subseteq S$ holds for any semi-preordering S . A preordering is just a semi-preordering which happens to be closed under multiplication.

If $p \subseteq A$ is a prime and $S \subseteq A$ is a semi-preordering,

$$S(p) := \left\{ \frac{\bar{t}}{\bar{a}^2} : t \in S, a \in A \setminus p \right\} \subseteq F(p).$$

(Here, $\bar{} : A \rightarrow A/p \subseteq F(p)$ denotes the natural homomorphism). One checks easily that $S(p)$ is a semi-preordering of $F(p)$.

If $S \subseteq A$ is a preordering, then the semi-preordering $S(p) \subseteq F(p)$ is actually a preordering. This is easy to check. Also, if $S = \sum A^2$, then $S(p) = \sum F(p)^2$.

Theorem 1.1. (Bröcker) *If $S \subseteq A$ is a proper semi-preordering then there exists a prime $p \subseteq A$ such that the semi-preordering $S(p) \subseteq F(p)$ is proper.*

Proof. Let $A[\frac{1}{2}] := \{\frac{a}{2^k} : a \in A, k \geq 0\}$ (localization of A at the multiplicative set generated by 2) and let $S[\frac{1}{2}] := \{\frac{t}{2^k} : t \in S, k \geq 0\}$. $S[\frac{1}{2}]$ is easily checked to be a semi-preordering in $A[\frac{1}{2}]$. Moreover, $S[\frac{1}{2}]$ is proper. (If $-1 \in S[\frac{1}{2}]$, then $-2^k = t \in S$ for some $k \geq 0$ so $-1 = (2^k - 1) + t \in S$.) Thus, replacing A by $A[\frac{1}{2}]$ and S by $S[\frac{1}{2}]$, we can assume $\frac{1}{2} \in A$. Thus we are free to use the identity

$$(*) \quad x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2, \quad x \in A.$$

Also, by Zorn's Lemma, we can assume S is maximal (proper) with respect to inclusion. Look at $p := S \cap -S$. This is an additive group (since $S + S \subseteq S$) and $A^2 p \subseteq p$ (since $A^2 S \subseteq S$). Using (*) one deduces that $Ap \subseteq p$, i.e., p is an ideal. The main step in the proof is to show that p is prime.

Claim: $a^2 \in p \Rightarrow a \in p$. For suppose $a^2 \in p$, $a \notin p$. Replacing a by $-a$ if necessary, we can suppose $a \notin S$. Consider the semi-preordering $S' := S + \sum A^2 a$. By maximality of S , $-1 \in S'$ so $-1 = t + as$, $t \in S, s \in \sum A^2$. Let $c := as$. Thus $c^2 = a^2 s^2 \in p$ (since $a^2 \in p$), so $1 + 2c = (1 + c)^2 + (-c^2) \in S$. Since $c + t = -1$, this means $-1 = (1 + 2c) + 2t \in S$, a contradiction. This proves the claim.

Suppose now that $a, b \in A, ab \in p$. We want to show $a \in p$ or $b \in p$. By the claim, it suffices to show that one of a^2, b^2 is in p . Suppose $a^2 \notin p$ (so $a^2 \notin -S$). Thus, by maximality of S , $-1 \in S - \sum A^2 a^2$, say $-1 = t - a^2 s$, $t \in S, s \in \sum A^2$. Then $-b^2 = b^2 t - (ab)^2 s \in S$ so $b^2 \in p$. This completes the proof that p is prime.

Suppose $-1 \in S(p)$. Then $-1 = \frac{t}{2^k}$ for some $t \in S$, $a \in A \setminus p$. Clearing fractions, $-a^2 \in S$ so $a^2 \in p$, i.e., $a \in p$, a contradiction. This completes the proof. \square

Later, in Part IV, §3, we use the full strength of Theorem 1.1. But, for now, we will be applying Theorem 1.1 only in the case where $S \subseteq A$ is a preordering.

2. Orderings and semi-orderings

Suppose F is a field of characteristic 0 and $T \subseteq F$ is a preordering. If $a \in T$, $a \neq 0$, then $\frac{1}{a} = (\frac{1}{a})^2 a \in T$. This implies that $T^* := T \setminus \{0\}$ is a subgroup of the multiplicative group $F^* := F \setminus \{0\}$. Since $F^2 \subseteq T$, the factor group F^*/T^* has exponent 2. Note also that if $s = -t$, $s, t \in T^*$, then $-1 = s/t \in T^*$. Thus, if T is proper, then $T \cap -T = \{0\}$. This can also be deduced from the fact that $T \cap -T$ is an ideal; see the proof of Theorem 1.1.

Orderings on fields were considered by Hilbert and later, in more detail, by Artin and Schreier. A subset $P \subseteq F$ (F a field) is called an *ordering* if P is a proper preordering and $P \cup -P = F$. Thus, for an ordering P , the factor group F^*/P^* has order 2.

$\text{Sper } F$ denotes the set of all orderings of F . This is called the *real spectrum* of F . If $T \subseteq F$ is a preordering, $X_T := \{P \in \text{Sper } F : P \supseteq T\}$. Thus, for example, if $T = \sum F^2$, then $X_T = \text{Sper } F$.

Theorem 1.2. (Artin) *For any proper preordering $T \subseteq F$, $X_T \neq \emptyset$ and, moreover, $T = \cap \{P : P \in X_T\}$.*

Proof. We begin by proving the following *Claim*: if $a \notin T$ then the preordering $T - aT$ is proper. For otherwise $-1 = s - at$ for some $s, t \in T$ so $at = 1 + s$. This is not zero (since $-1 \notin T$) so $t \neq 0$. Thus $a = (1 + s)/t \in T$, contradicting our assumption. This proves the claim.

To prove $X_T \neq \emptyset$, use Zorn's Lemma to pick a maximal proper preordering $P \supseteq T$. If $a \in F$ and $a \notin P$ then, by the claim (applied to the preordering P) $P - aP$ is proper so, by the maximal choice of P , we must have $P = P - aP$ and consequently $-a \in P$. This proves $F = P \cup -P$ so P is an ordering. Thus $P \in X_T$, so $X_T \neq \emptyset$.

To prove $T = \cap \{P : P \in X_T\}$, it suffices to show that if $a \in F \setminus T$, then

$\exists P \in X_T$ with $a \notin P$. But, by the claim, $T - aT$ is proper, so $X_{T-aT} \neq \emptyset$ by what we have already proved. Any $P \in X_{T-aT}$ satisfies $-a \in P$ and consequently $a \notin P$ (since $P \cap -P = \{0\}$) \square

Semi-orderings on fields were introduced by Prestel. We will need these later, in proving the Isotropy Theorem in Part III. A subset $S \subseteq F$, is called a *semi-ordering* if S is a proper semi-preordering (i.e., $S + S \subseteq S$, $F^2 S \subseteq S$, $1 \in S$, $-1 \notin S$) and $S \cup -S = F$. Thus, an ordering is just a semi-ordering which happens to be closed under multiplication.

Note. If $S \subseteq F$ is a semi-preordering, then $S \cap -S$ is an ideal of F (see the proof of Theorem 1.1) so $S \cap -S = \{0\}$ if S is proper.

We restrict our attention here to semi-preorderings, etc., on F satisfying $TS \subseteq S$ for some preordering $T \subseteq F$. These will be referred to as *T-semi-preorderings*, etc. (Of course, there is no loss of generality in this: we can always take $T = \sum F^2$.) Note: Since $1 \in S$, $T \subseteq TS \subseteq S$ for any T -semi-preordering S . In particular, a T -ordering is just an element of X_T .

Theorem 1.3. *Any T-semi-preordering is the intersection of the T-semi-orderings containing it.*

Proof. One verifies, if S is a T -semi-preordering and $a \notin S$, then $S - aT$ is proper T -semi-preordering. The result follows from this, exactly as in the proof of Artin's Theorem. \square

For the rest of this section and the next, fix a T -semi-ordering $S \subseteq F$ and denote by $<$ the associated linear ordering on $(F, +)$ (so $a < b$ just means $b - a \in S, b \neq a$). Since we are not assuming $SS \subseteq S$, it is necessary to exercise caution in dealing with $<$.

Lemma 1.4. *For any $a, b \in F$*

$$(1) \quad 0 < a \Rightarrow 0 < a^{-1}$$

$$(2) \quad 0 < a < b \Rightarrow a^2 b < ab^2$$

$$(3) \ 0 < a < b \Rightarrow b^{-1} < a^{-1}$$

$$(4) \ 0 < a < b \text{ and } b \in T \Rightarrow a^2 < b^2$$

$$(5) \ 0 < a < b \text{ and } a \in T \Rightarrow a^2 < b^2$$

Proof.

$$(1) \ a^{-1} = (a^{-1})^2 a.$$

$$(2) \ ab^2 - a^2b = b^2((b-a)^{-1} + a^{-1})^{-1}.$$

(3) follows from (2), multiplying each side by $a^{-2}b^{-2}$.

(4) By (2) $a^2b < ab^2$ and $b^{-1} \in T$ so scaling, we get $a^2 < ab$. Also, $a < b$ and $b \in T$ so scaling by b , we get $ab < b^2$.

(5) Similar to (4). □

Lemma 1.5. *If S is Archimedean (i.e., $0 < a \Rightarrow a < n$ for some $n \in \mathbb{N}$) then S is an ordering.*

Proof. Suppose $a < b$. Then $\exists n \in \mathbb{N}$ such that $0 < (b-a)^{-1} < n$ so by (3), $0 < n^{-1} < b-a$. Choose $m \in \mathbb{Z}$ so that $m-1 \leq na < m$. Then $m < nb$. (Otherwise, $1 - n(b-a) = (m-nb) + (na - (m-1)) \in S$ so $n(b-a) \leq 1$ and therefore $b-a \leq n^{-1}$, a contradiction.) Thus $na < m < nb$, so $a < m/n < b$. This proves \mathcal{Q} is dense. Now suppose $a, b \in S^*$. We must show $ab \in S$. We can assume $a < b$. Then $0 < b-a < b+a$ so $\exists r \in \mathcal{Q}$ with $0 < b-a < r < b+a$. Since $r \in T$, we can apply parts (4) and (5) to obtain $(b-a)^2 < r^2 < (b+a)^2$. Thus $ab = \frac{(b+a)^2 - (b-a)^2}{4} \in S$. □

Remark. If $P \subseteq F$ is an Archimedean ordering, then there exists a unique embedding $\gamma_P : F \hookrightarrow \mathbb{R}$ such that $P = \gamma_P^{-1}(\mathbb{R}^2)$. This is well known.

3. Semi-orderings and valuations

The connection between orderings and valuations was noticed first by Baer and Krull. The more complicated connection between semi-orderings and valuations is due to Prestel.

We continue to assume S is a T -semi-ordering on a field F . Let $B \subseteq F$ be a valuation ring. Let $M = M_B \subseteq B$ be the maximal ideal, $B^* := B \setminus M$ the group of units of B , and let $\bar{\cdot} : B \rightarrow \bar{F} := B/M$ be the natural homomorphism. For any set $Q \subseteq F$, denote by \bar{Q} the *pushdown* of Q to \bar{F} i.e.,

$$\bar{Q} := \overline{Q \cap B} = \{\bar{a} : a \in Q \cap B\} \subseteq \bar{F}.$$

With this notation, it should be clear that \bar{S} is a \bar{T} -semi-preordering on \bar{F} and $\bar{S} \cup -\bar{S} = \bar{F}$ so \bar{S} is an semi-ordering iff $-1 \notin \bar{S}$.

Lemma 1.6. *The following are equivalent:*

- (1) $-1 \notin \bar{S}$ (so \bar{S} is a \bar{T} -semi-ordering).
- (2) $\{a \in B^* : \bar{a} \in \bar{S}\} \subseteq S$.
- (3) $(1 + M)(B^* \cap S) \subseteq S$.
- (4) $1 + M \subseteq S$.

Proof.

- (1) \Rightarrow (2). Suppose $\bar{a} \in \bar{S}$, $a \in B^*$. Then $a \in S$, since otherwise $a \in -S$ so $\bar{a} \in \bar{S} \cap -\bar{S}$ contradicting $\bar{S} \cap -\bar{S} = \{0\}$.
- (2) \Rightarrow (3) and (3) \Rightarrow (4) are clear.
- (3) \Rightarrow (1). If $-1 \in \bar{S}$ then we have $a \in S \cap B^*$ with $-1 = a + x$, $x \in M$. But then $-a = 1 + x \in S$ so $a \in S \cap -S$. \square

We say B, S are *compatible* if one of the equivalent conditions of Lemma 1.6 holds.

Note.

- (1) If S is an ordering and B, S are compatible, then the push-down of S to \bar{F} is an ordering (not just a semi-ordering).
- (2) The valuation rings of F lying over a given valuation ring B are linearly ordered by inclusion. Moreover, if $C \supseteq B$ then $M_C \subseteq M_B$ so if B is compatible with S then so is C .

Theorem 1.7. *There exists a unique smallest valuation ring B of F compatible with S . Consequently, the valuation rings of F compatible with S are linearly ordered by inclusion.*

Proof. The convex hull of \mathcal{Q} in F is

$$B = B_S := \{x \in F : \exists r \in \mathcal{Q}^+ \text{ such that } -r \leq x \leq r\}.$$

Clearly B is closed under subtraction and $\mathcal{Q} \subseteq B$. Also, using Lemma 1.4 (4), we see that $x \in B \Rightarrow x^2 \in B$. Since $xy = \frac{(x+y)^2 - (x-y)^2}{4}$, this implies B is a ring. Using Lemma 1.4 (3), it is clear that B is a valuation ring with maximal ideal

$$M = M_S := \{x \in F : -r < x < r \text{ for all } r \in \mathcal{Q}^+\}.$$

Thus, if $x \in M$ then $-1 < x < 1$ so $1+x \in S$. This proves B, S are compatible. Now let C be any valuation ring of F compatible with S . If $x \in M_C$ then $1 \pm nx \in 1 + M_C \subseteq S$ for any $n \in \mathbb{N}$ so $x \in M = M_B$. This proves $M_C \subseteq M_B$ so $B \subseteq C$. \square

Remark.

- (1) If $B \subseteq F$ is a valuation ring and $D \subseteq F$ is any subring, then BD (= the set of all products bd , $b \in B$, $d \in D$) is a valuation ring. It is the smallest valuation ring containing B and D .

- (2) Thus, by Theorem 1.7, if $D \subseteq F$ is any subring, then

$$B = B_S D = \{x \in F : -1 \leq x/d \leq 1 \text{ for some } d \in D \setminus \{0\}\}$$

(called the *convex hull* of D in F) is the smallest valuation ring in F containing D and compatible with S . This has maximal ideal

$$M = \{x \in F : -1 < dx < 1 \text{ for all } d \in D\}.$$

- (3) The pushdown $\overline{S} \subseteq \overline{F} = B_S/M_S$ is Archimedean (by definition of B_S) so, by Lemma 1.5, \overline{S} is an Archimedean ordering. Thus \exists a unique embedding $\gamma_S : \overline{F} \hookrightarrow \mathbb{R}$ with $\overline{S} = \gamma_S^{-1}(\mathbb{R}^2)$. Thus we have a real place $\lambda_S : F \rightarrow \mathbb{R} \cup \{\infty\}$ defined by composition.
- (4) Using Lemma 1.8 below, one can show that every real place $\alpha : F \rightarrow \mathbb{R} \cup \{\infty\}$ has the form $\alpha = \lambda_P$ for some (generally non-unique) $P \in \text{Sper } F$.

Lemma 1.8. *Suppose B is a valuation ring of F with maximal ideal M and residue field $\overline{F} = B/M$. Suppose $P = P^* \cup \{0\}$ where $P^* \subseteq F^*$ is a subgroup of index 2 such that the pushdown $\overline{P} := \overline{P \cap B}$ is an ordering on \overline{F} . Then P is an ordering on F .*

Proof. Since P^* has index 2, $F^2 \subseteq P$ and clearly $-1 \notin P$ (since $-1 \notin \overline{P}$). Thus it suffices to show $x, y \in P^* \Rightarrow x + y \in P^*$. By symmetry, we can suppose $x^{-1}y \in B$. Since $x + y = x(1 + x^{-1}y)$ and P^* is closed under multiplication, it suffices to show $1 + x^{-1}y \in P^*$. Thus we are reduced to the case where $x = 1$ and $y \in B \cap P$. But if $1 + y \notin P^*$, then $-(1 + y) \in P$ so, applying $- : B \rightarrow \overline{F}$, $-1 \in \overline{P}$, a contradiction. Thus $1 + y \in P^*$. This completes the proof. \square

Lemma 1.9. *Suppose F is real closed with (unique) ordering P . Then, for any P -compatible valuation ring $B \subseteq F$, the value group F^*/B^* is divisible and the residue field \overline{F} is real closed (with unique ordering \overline{P}).*

Proof. If $x \in F^*$, $n \in \mathbb{N}$, then $\pm x \in P$ so $\pm x = y^n$ for some $y \in F^*$. This proves F^*/B^* is divisible. If $x \in B^* \cap P$, $x = y^2$ for some $y \in B^*$. Thus $\bar{P} = \bar{F}^2$. If $f(t) = \sum_{i=0}^n a_i t^i$, n odd, $a_i \in B$, $a_n = 1$, then $f(t)$ has a root $y \in B$ (since F is real closed and B is integrally closed in F). Thus $\bar{y} \in \bar{F}$ is a root of $\bar{f}(t) = \sum_{i=0}^n \bar{a}_i t^i$. This proves (\bar{F}, \bar{P}) is real closed. \square

4. Nullstellensatz, positivstellensatz

The real spectrum of a ring was introduced by Coste and Roy. For a ring A (commutative with 1), an *ordering* on A is a pair $P = (p, P)$, where $p \subseteq A$ is a prime and P is an ordering on the residue field $F(p)$. $\text{Sper } A$ denotes the set of all orderings of A , i.e.,

$$\text{Sper } A := \dot{\cup}_p \text{Sper } F(p) \quad (\text{disjoint union})$$

p running through the prime ideals of A . This is called the *real spectrum* of A . If $P \in \text{Sper } A$, then $P \in \text{Sper } F(p)$ for some unique prime ideal $p \subseteq A$. p is called the *support* of P and we write $\text{Supp}(P) = p$. If $T \subseteq A$ is a preordering, we define

$$X_T := \dot{\cup}_p X_{T(p)} \quad (\text{disjoint union})$$

p running through the prime ideals of A . Note: If $T = \sum A^2$, then $T(p) = \sum F(p)^2$, so $X_T = \text{Sper } A$.

Corollary 1.10. *For any proper preordering $T \subseteq A$, $X_T \neq \emptyset$.*

Proof. Combine Theorems 1.1 and 1.2. \square

We have obvious functorial properties: Each ring homomorphism $f : A \rightarrow B$ induces a map $\text{Sper } f : \text{Sper } B \rightarrow \text{Sper } A$, $(q, Q) \mapsto (p, P)$ where $p = f^{-1}(q)$ and $P = \bar{f}^{-1}(Q)$, where $\bar{f} : F(p) \hookrightarrow F(q)$ is the embedding induced by f . Each preordering $T \subseteq A$ induces a preordering $T_B = \sum B^2 f(T) = \{\sum b_i^2 f(t_i) | b_i \in B, t_i \in T\}$ in B (T_B = the smallest preordering in B containing $f(T)$), and $\text{Sper } f$ maps X_{T_B} into X_T .

Important Examples:

- (1) If $A \rightarrow \Sigma^{-1}A$ is a localization, then $\Sigma^{-2}T := \{\frac{t}{a^2} : t \in T, a \in \Sigma\}$ is the preordering on $\Sigma^{-1}A$ induced by T . The functorial map $X_{\Sigma^{-2}T} \rightarrow X_T$ is injective and identifies $X_{\Sigma^{-2}T}$ with

$$\{P \in X_T : \text{Supp}(P) \cap \Sigma = \emptyset\}.$$

This follows from the relationship between residue fields of $\Sigma^{-1}A$ and residue fields of A . If Σ is the multiplicative set generated by some $f \in A$, then we denote $\Sigma^{-1}A$ by $A[\frac{1}{f}]$ and $\Sigma^{-2}T$ by $T[\frac{1}{f^2}]$.

- (2) If $A \rightarrow A/I$ is a factor ring then $T/I := \{t + I : t \in T\}$ is the preordering on A/I induced by T . Again, the functorial map $X_{T/I} \rightarrow X_T$ is injective and identifies $X_{T/I}$ with

$$\{P \in X_T : \text{Supp}(P) \supseteq I\}.$$

This follows from the relationship between residue fields of A/I and residue fields of A .

Notation.

- (1) If $P \in \text{Sper } F$, F a field, \geq_P denotes the associated linear ordering on F , i.e., $a \geq_P b$ means $a - b \in P$, $a >_P b$ means $a - b \in P, a \neq b$.
- (2) If $f, g \in A$ and $P \in \text{Sper } A$, we define

$$f =_P g \quad (\text{resp; } f \geq_P g, \text{ resp; } f >_P g)$$

to mean that

$$\bar{f} = \bar{g} \quad (\text{resp; } \bar{f} \geq_P \bar{g}, \text{ resp; } \bar{f} >_P \bar{g})$$

where $\bar{} : A \rightarrow A/p \subseteq F(p)$ is the natural mapping, and $p = \text{Supp}(P)$.

Note. If $P \in X_T$ then $f \geq_P 0$ holds for all $f \in T$. This is clear.

Corollaries 1.11, 1.12 which follow are abstract versions of classical results in real algebraic geometry due to Dubois and Risler and Stengle respectively. For the concrete versions of these results, see Corollaries 2.2, 2.3.

Corollary 1.11. (Nullstellensatz) *Let $T \subseteq A$ be a preordering and suppose $f \in A$ satisfies $f =_P 0$ for all $P \in X_T$. Then $-f^{2k} \in T$ holds for some integer $k \geq 0$ (and conversely).*

Proof. Consider the localization $A[\frac{1}{f}]$ of A and the preordering $T[\frac{1}{f^2}] \subseteq A[\frac{1}{f}]$ generated by T . The hypothesis implies $X_{T[\frac{1}{f^2}]} = \emptyset$. Thus, by Corollary 1.10, $-1 \in T[\frac{1}{f^2}]$. Sorting this out yields $-f^{2k} \in T$ for some integer $k \geq 0$. \square

Corollary 1.12. (Positivstellensatz) *Let $T \subseteq A$ be a preordering and suppose $f \in A$. Then*

- (1) $f >_P 0 \forall P \in X_T \Rightarrow (1 + s)f = 1 + t$ for some $s, t \in T$ (and conversely).
- (2) $f \geq_P 0 \forall P \in X_T \Rightarrow (f^{2k} + s)f = f^{2k} + t$ for some $s, t \in T$ and some integer $k \geq 0$ (and conversely).

Proof.

- (1) Look at the preordering $T - fT \subseteq A$. By the hypothesis, $X_{T-fT} = \emptyset$ and consequently, by Corollary 1.10, $-1 \in T - fT$. Also, $1 - f \in T - fT$. Thus $-(1 - f) \in T - fT$ so we have $-(1 - f) = t - fs$, i.e., $(1 + s)f = 1 + t$ for some $s, t \in T$.
- (2) Look at the preordering $T[\frac{1}{f^2}] \subseteq A[\frac{1}{f}]$, as in Corollary 1.11. Then $f >_P 0$ on $X_{T[\frac{1}{f^2}]}$ so, by (1) $\exists s_1, t_1 \in T[\frac{1}{f^2}]$ such that $(1 + s_1)f = 1 + t_1$ holds in the ring $A[\frac{1}{f}]$. Clearing fractions, this yields $(f^{2k} + s)f = f^{2k} + t$ (in A) for some $s, t \in T$ and some integer $k \geq 0$. \square

5. Compactness

For $a \in A$ let

$$\begin{aligned} Z(a) &= Z_T(a) := \{P \in X_T : a =_P 0\}, \\ U(a) &= U_T(a) := \{P \in X_T : a >_P 0\}, \\ W(a) &= W_T(a) := \{P \in X_T : a \geq_P 0\}. \end{aligned}$$

There are three natural topologies on X_T :

- (1) *the Zariski topology.* The sets $X_T \setminus Z(a) = \{P \in X_T : a \neq_P 0\} = U(a^2)$, $a \in A$, form a basis for a topology on X_T called the *Zariski topology*. This is generally not Hausdorff. Closed sets in this topology have the form

$$Z(I) = Z_T(I) := \{P \in X_T : a =_P 0 \ \forall a \in I\}$$

for some set $I \subseteq A$ (and we can take I to be an ideal if we want). If A is Noetherian and $I \subseteq A$ is an ideal, then $I = (b_1, \dots, b_k)$ for some $b_1, \dots, b_k \in A$, so $Z(I) = Z(b_1, \dots, b_k) = Z(b)$ where $b = b_1^2 + \dots + b_k^2$.

- (2) *the Harrison topology.* The sets $U(a)$, $a \in A$, form a subbasis for a topology on X_T called the *Harrison topology*. This topology is clearly finer than the Zariski topology. Again, the Harrison topology is generally not Hausdorff.
- (3) *the Tychonoff topology.* The sets $U(a), Z(a)$, $a \in A$, form a subbasis for a topology on X_T called the *Tychonoff topology*. Of course, this is finer than the Harrison topology. In the Tychonoff topology, compliments of subbasic open sets are open:

$$X_T \setminus Z(a) = U(a^2) \text{ and } X_T \setminus U(a) = W(-a) = U(-a) \cup Z(a),$$

so the Tychonoff topology is totally disconnected. The reader can check that the Tychonoff topology is Hausdorff.

Note. In the case of a field, all orderings have support 0, so $Z(a) = X_T$ or \emptyset depending on whether $a = 0$ or not. Thus, in this case, the Zariski topology is trivial, and the Harrison and Tychonoff topologies coincide.

Theorem 1.13. X_T is compact in the Tychonoff topology (and hence also in the Harrison and Zariski topologies).

Proof. According to Alexander's Theorem [15], it suffices to show that any cover of X_T by *subbasic* open sets has a finite subcover. Suppose

$$(*) \quad X_T = \cup_{i \in I} U(a_i) \cup \cup_{j \in J} Z(b_j).$$

Let $T' \subseteq A$ be the preordering generated by T and the $-a_i, i \in I$. Let $\Sigma^{-1}A$ be the localization of A at the multiplicative set Σ generated by the $b_j, j \in J$. Consider the preordering $\Sigma^{-2}T' \subseteq \Sigma^{-1}A$ induced by T' . By (*), $X_{\Sigma^{-2}T'} = \emptyset$. Thus, by Corollary 1.10, $-1 \in \Sigma^{-2}T'$ so $-c^2 = s$ for some $c \in \Sigma, s \in T'$. But $c = b_{j_1}^{k_1} \cdots b_{j_t}^{k_t}$ for some finite set $\{j_1, \dots, j_t\} \subseteq J$ and s is in the preordering generated by T and $-a_{i_1}, \dots, -a_{i_u}$ for some finite set $\{i_1, \dots, i_u\} \subseteq I$. Thus the equation $-c^2 = s$ has the form

$$-b_{j_1}^{2k_1} \cdots b_{j_t}^{2k_t} = \sum t_{e_1 \dots e_u} (-a_{i_1})^{e_1} \cdots (-a_{i_u})^{e_u}$$

(finite sum) where the coefficients $t_{e_1 \dots e_u}$ are in T and $(e_1, \dots, e_u) \in \{0, 1\}^u$. But this implies

$$X_T = \cup_{v=1}^u U(a_{i_v}) \cup \cup_{w=1}^t Z(b_{j_w}).$$

This completes the proof. □

Remark. This is almost certainly not the "best" proof of Theorem 1.13. The reader is encouraged to look at [18] for a more elementary proof which does not use Alexander's Theorem.

A subset $S \subseteq X_T$ is called *constructible* if it is clopen (= both open and closed) in the Tychonoff topology. The set of all constructible sets in X_T forms a Boolean algebra (i.e., it is closed under taking complements, finite unions, and finite intersections).

To describe constructible sets we need some additional notation. For $a_1, \dots, a_n \in A$ let

$$\begin{aligned} U(a_1, \dots, a_n) &= \bigcap_{i=1}^n U(a_i) = \{P \in X_T : a_i >_P 0, i = 1, \dots, n\} \\ W(a_1, \dots, a_n) &= \bigcap_{i=1}^n W(a_i) = \{P \in X_T : a_i \geq_P 0, i = 1, \dots, n\} \\ Z(a_1, \dots, a_n) &= \bigcap_{i=1}^n Z(a_i) = \{P \in X_T : a_i =_P 0, i = 1, \dots, n\}. \end{aligned}$$

These sets are constructible sets. The sets $U(a_1, \dots, a_n)$ (resp; $W(a_1, \dots, a_n)$) are called *basic open* (resp; *basic closed*) in X_T . Of course, basic open sets are a basis for the Harrison topology. Also, $Z(b_1, \dots, b_n) = Z(b)$ where $b = b_1^2 + \dots + b_n^2$, so sets of the form $U(a_1, \dots, a_n) \cap Z(b)$ are a basis for the Tychonoff topology.

Corollary 1.14.

- (1) *Any constructible which is Harrison open is a finite union of basic open sets.*
- (2) *Any constructible which is Harrison closed is a finite union of basic closed sets.*
- (3) *Any constructible is a finite union of sets of the form*

$$U(a_1, \dots, a_n) \cap Z(b), a_1, \dots, a_n, b \in A.$$

Proof. (1) and (3) follow from the compactness of constructible sets; see Theorem 1.13. (2) follows from (1) by taking complements, observing that the complement of $U(a)$ is $W(-a)$. \square

6. Description of closure

Because of the 3 topologies on X_T , one must use the terms *open*, *closed*, *interior*, *closure*, etc; with some care. The standard convention is the following: *When these terms are used without modifier, they always refer to the Harrison topology.*

For $S \subseteq X_T$, \bar{S} denotes the closure and $\text{z-cl}(S)$ denotes the Zariski-closure. We want to describe \bar{S} and $\text{z-cl}(S)$ in case $S \subseteq X_T$ is Tychonoff closed. We begin with $\text{z-cl}(S)$ since this is easier.

Corollary 1.15. *Suppose $S \subseteq X_T$ is Tychonoff closed. Then any minimal prime p lying over the ideal*

$$I = \cap \{ \text{Supp}(P) : P \in S \} = \{ a \in A : a =_P 0 \ \forall P \in S \}$$

has the form $p = \text{Supp}(P)$ for some $P \in S$.

Proof. If $a \in A \setminus p$, then $a \notin I$ so $\exists P \in S$ such that $a \neq_P 0$, i.e., the set $\{P \in S : a \neq_P 0\}$ is not empty. The sets of this type are Tychonoff closed and form a nested family so, by Theorem 1.13,

$$\cap_{a \in A \setminus p} \{P \in S : a \neq_P 0\} \neq \emptyset.$$

Any P in this intersection satisfies $\text{Supp}(P) \subseteq p$ so, by minimality of p , $\text{Supp}(P) = p$. □

The Zariski closure of $S \subseteq X_T$ is $\text{z-cl}(S) := Z(I)$ where I is defined as in Corollary 1.15. This is the smallest Zariski closed set in X_T containing S . According to Corollary 1.15, if S is Tychonoff closed, then

$$\text{z-cl}(S) = \{Q \in X_T : \text{Supp}(Q) \supseteq \text{Supp}(P) \text{ for some } P \in S\}.$$

The dimension of S is defined to be the (Krull) dimension of the ring A/I . Thus $\dim S = \dim \text{z-cl}(S)$ and, if S is Tychonoff closed then, by Corollary 1.15,

$$\begin{aligned} \dim S &= \dim A/I \\ &= \sup \{ \dim A/\text{Supp}(P) : P \in S \} \\ &= \sup \{ \dim A/p : S \cap X_{T(p)} \neq \emptyset \}. \end{aligned}$$

(Usual convention: $\dim A/I = -1$ if $I = A$).

If $P, Q \in \text{Sper } A$ we say Q specializes P (or P generalizes Q) and we write $Q \succ P$ (or $P \prec Q$) to indicate that $a \geq_P 0 \Rightarrow a \geq_Q 0$ (equivalently, that $a >_Q 0 \Rightarrow a >_P 0$).

Note:

- (1) If $Q \succ P$ then $\text{Supp}(Q) \supseteq \text{Supp}(P)$.
- (2) If $Q \succ P$ and $\text{Supp}(Q) = \text{Supp}(P)$, then $Q = P$.
- (3) If $Q \succ P$ and $P \succ Q$, then $P = Q$.

Analogously to Corollary 1.15, one has the following:

Corollary 1.16. *For any Tychonoff closed set $S \subseteq X_T$,*

$$\overline{S} = \{Q \in X_T : Q \succ P \text{ for some } P \in S\}.$$

Proof. (\supseteq) is clear: If $Q \succ P$, then every neighbourhood of Q contains P , so $Q \in \overline{\{P\}}$, and $\overline{\{P\}} \subseteq \overline{S}$ since $P \in S$.

(\subseteq) . Let $Q \in \overline{S}$. Then, for each $a_1, \dots, a_n \in A$ satisfying $a_i >_Q 0, i = 1, \dots, n \exists P \in S$ such that $a_i >_P 0, i = 1, \dots, n$ i.e., the Tychonoff closed set $\{P \in S : a_i >_P 0, i = 1, \dots, n\}$ is non-empty. Again, sets of this type form a nested family, so by Theorem 1.13,

$$\bigcap_{a >_Q 0} \{P \in S : a >_P 0\} \neq \emptyset.$$

Any P in this intersection satisfies $Q \succ P$. □

Corollary 1.17. *Suppose $S \subseteq X_T$ is constructible and $\dim X_T < \infty$. Then the boundary $\partial S = \partial_T S := \overline{S} \cap \overline{X_T \setminus S}$ satisfies $\dim \partial S < \dim X_T$.*

Proof. Let $I = \{a \in A : a =_P 0 \forall P \in \partial S\}$, so $\dim \partial S = \dim A/I$. Let p be a minimal prime lying over I . Then $p = \text{Supp}(P)$ for some $P \in \partial S$ (by Corollary 1.15). Thus we have $Q_1 \in S, Q_2 \in X_T \setminus S$ with $Q_i \prec P, i = 1, 2$ (by Corollary 1.16). But then one of the Q_i has support strictly smaller than p (since otherwise $Q_1 = P = Q_2$). □

Theorem 1.18. *For $P \in X_T$, the set $\overline{\{P\}} = \{Q \in X_T : P \prec Q\}$ is linearly ordered by \prec . Moreover, $\overline{\{P\}}$ has a unique maximal element.*

Proof. Suppose $P \prec Q_i, i = 1, 2$ but $Q_1 \not\prec Q_2$ and $Q_2 \not\prec Q_1$. Thus we have $a, b \in A$ satisfying $a \geq_{Q_1} 0, a <_{Q_2} 0, b \geq_{Q_2} 0, b <_{Q_1} 0$. Interchanging a, b if necessary, we can assume $a \geq_P b$. But then $a - b \geq_P 0$ and consequently $a - b \geq_{Q_2} 0$ and $b \geq_{Q_2} 0$ so $a = (a - b) + b \geq_{Q_2} 0$, a contradiction.

For the second assertion, look at $T' = \{a \in A : a \geq_Q 0 \text{ for some } Q \in X_T, Q \succ P\}$. This is a proper preordering so $\exists Q \in X_{T'}$ (Corollary 1.10). Clearly Q is the unique maximal element of $\overline{\{P\}}$. \square

Caution. $\text{Supp}(Q)$ need not be a maximal ideal.

Remark. Specializations of $P \in \text{Sper } A$ are related in a natural way to valuation rings on the residue field:

- (1) Specializations of P can be produced by the following process: let $p = \text{Supp}(P)$ and suppose B is any valuation ring on $F(p)$ containing A/p and compatible with P . Let q be the prime ideal in A defined by $q/p = M_B \cap A/p$. Then $F(q) \subseteq \overline{F} = B/M_B$ and the ordering $Q \in \text{Sper } F(q)$ defined by $Q = \overline{P} \cap F(q)$ (where \overline{P} is the pushdown of P to \overline{F}) specializes P .
- (2) Conversely, using Theorem 1.7, one can show that any specialization of P arises in this way [3]: suppose $Q \in \text{Sper } A$ is a specialization of P and let $q = \text{Supp}(Q)$. Then $q \supseteq p$, so we can look at the local ring

$$D = \{a/b : a, b \in A/p, b \notin q/p\} \subseteq F(p).$$

Let B be the smallest valuation ring in $F(p)$ containing D and compatible with P . Then it is easy to show that $M_B \cap A/p = q/p$ (so $F(q) \subseteq \overline{F}$) and that $Q = \overline{P} \cap F(q)$.

Thus Theorem 1.18 is completely "explained" by Theorem 1.7.

7. The Hörmander-Łojasiewicz inequality

In this section, we prove an abstract version of a classical inequality for semi-algebraic functions. This seems to be due to Coste. The proof given here is taken from [1].

Theorem 1.19 *Suppose $S \subseteq X_T$ is any closed constructible set and $f, g \in A$ are such that $g = 0$ on $S \cap Z(f)$. Then $\exists p \in A, p > 0$ on X_T and $m \geq 0$ such that $|g|^{2m+1} \leq p|f|$ on S . (i.e., $|\bar{g}|^{2m+1} \leq_P \bar{p}|\bar{f}|$ for each $P \in S$.)*

Proof. Since $W(b_1, \dots, b_n) = X_{T(b_1, \dots, b_n)}$ where $T(b_1, \dots, b_n)$ denotes the smallest preordering containing T and b_1, \dots, b_n , Corollary 1.14 (2) implies that there exist preorderings $T_1, \dots, T_v \supseteq T$ such that $S = X_{T_1} \cup \dots \cup X_{T_v}$. Thus $X_{T_i} \cap Z(f) \subseteq Z(g)$ so, applying the Nullstellensatz (Corollary 1.11) to the preordering $\bar{T}_i = T_i/(f)$ in $A/(f)$ induced by T_i , we have $-\bar{g}^{2m_i} \in \bar{T}_i$ so $-g^{2m_i} = s_i - a_i f$ for some $m_i \geq 0, s_i \in T_i, a_i \in A$. Multiplying by a suitable even power of g , we can assume $m_1 = \dots = m_v = m$. Thus, on X_{T_i} ,

$$g^{2m} = -s_i + a_i f \leq a_i f = |a_i| |f| \text{ so } |g|^{2m+1} \leq |ga_i| |f| \leq p|f|$$

where $p = 1 + g^2(a_1^2 + \dots + a_v^2)$. Since $S = \cup_{i=1}^v X_{T_i}$, this implies $|g|^{2m+1} \leq p|f|$ on S . \square

Note. It is easy to arrange things so that $|g|^{2m+1} < p|f|$ on $S \setminus Z(f)$. (e.g., just replace p by $p + f^2$). Once this is done, $f_1 := pf + g^{2m+1}$ and f have the same sign on S .

We use Theorem 1.19 several times, but always in the following special form:

Theorem 1.20. *Suppose $S \subseteq X_T$ is a closed constructible set and $f \geq 0$ on $S \cap Z(g) \cap U(h^2)$ for some $g, h \in A$. Then $\exists f_1 \in A$ such that $f_1 \geq 0$ on S and f_1, f have the same sign on $Z(g) \cap U(h^2)$.*

Proof. Let $S' = S \cap W(-f)$. Then $fh^2 = 0$ on $S' \cap Z(g)$. Of course, $Z(g^2) = Z(g)$. Thus, by Theorem 1.19 and the Note following, $\exists p > 0$ on X_T and

$m \geq 0$ such that $f_1 := pg^2 + (fh^2)^{2m+1}$ has the same sign as g^2 on S' . Now $f_1 \geq 0$ on S is clear. Also, f_1 and f have the same sign on $Z(g) \cap U(h^2)$ so the proof is complete. \square

Notation. For $S \subseteq X_T$ and $p \subseteq A$ a prime, let $S(p) := \{P \in S : \text{Supp}(P) = p\} = S \cap X_{T(p)}$. Thus S decomposes as $S = \dot{\cup}_p S(p)$ (disjoint union).

Corollary 1.21. *Suppose $S \subseteq X_T$ is a closed constructible, $p \subseteq A$ is a prime, and $f \in A$ satisfies $f \geq 0$ on $S(p)$. Then $\exists g \in A$ such that $g \geq 0$ on S and f, g have the same sign on $X_{T(p)}$.*

Proof. $X_{T(p)}$ is the intersection of the sets $Z(g) \cap U(h^2), g \in p, h \in A \setminus p$. Thus $S(p)$ is the intersection of the sets $S \cap Z(g) \cap U(h^2), g \in p, h \in A \setminus p$, and these form a nested family. Also, $f \geq 0$ on $S(p)$ so, by compactness, $\exists g \in p, h \in A \setminus p$ such that $f \geq 0$ on $S \cap Z(g) \cap U(h^2)$. Thus the result follows from Theorem 1.20. \square

8. Basic constructible sets

The material in this section is taken from [21]. It generalizes results in real algebraic geometry due to Bröcker. Recall that constructible sets $S \subseteq X_T$ of the form

$$(*) \quad S = U(a_1, \dots, a_m) \cap Z(b), a_1, \dots, a_m, b \in A,$$

form a basis for the Tychonoff topology; see section 5. More generally, we say that a constructible set $S \subseteq X_T$ is *basic* if

$$(**) \quad S = U(a_1, \dots, a_m) \cap W(b_1, \dots, b_n), a_1, \dots, a_m, b_1, \dots, b_n \in A.$$

As in section 5, we say S is *basic open* (resp; *basic closed*) if S is expressible as in $(**)$ but with $n = 0$ (resp., with $m = 0$). (Of course, in the field case, basic = basic open = basic closed).

Note:

- (1) $Z(b) = W(b, -b)$ so sets of the form $(*)$ are basic (but not conversely).
- (2) $a_i > 0, i = 1, \dots, m \Leftrightarrow a_i \geq 0, i = 1, \dots, m$ and $\prod_{i=1}^m a_i \neq 0$ so any basic set $S \subseteq X_T$ has the form $S = U(a^2) \cap W(c_1, \dots, c_k)$ for some $a, c_1, \dots, c_k \in A$.

Corollary 1.22. *For any constructible $S \subseteq X_T$, the following are equivalent:*

- (1) S is basic closed in X_T .
- (2) S is basic and closed in X_T .
- (3) S is closed in X_T and $S(p)$ is basic in $X_{T(p)}$ for each prime p .

Proof. (1) \Rightarrow (2) and (2) \Rightarrow (3) are trivial. To prove (3) \Rightarrow (1), apply Corollary 1.21 to obtain, for each p and for each $P \in X_{T(p)} \setminus S(p)$, an element $f \in A$ such that $f \geq 0$ on S and $f <_P 0$. Thus $S = \cap \{W(f) : f \in A, f \geq 0 \text{ on } S\}$ so, by compactness of $X_T \setminus S$, $S = W(f_1, \dots, f_s)$ for some finite set $\{f_1, \dots, f_s\} \subseteq A$. \square

Corollary 1.23. *For any constructible $S \subseteq X_T$, the following are equivalent:*

- (1) S is basic in X_T .
- (2) $S \cap \text{cl}(\overline{S} \setminus S) = \emptyset$ and $S(p)$ is basic in $X_{T(p)}$ for each prime p .

Note:

- (1) If S is closed in X_T , then $\overline{S} = S$ so the condition $S \cap \text{cl}(\overline{S} \setminus S) = \emptyset$ is vacuous, so condition (2) of Corollary 1.23 is just condition (3) of Corollary 1.22.
- (2) If S is open in X_T , then $\overline{S} \setminus S = \partial S$ (the boundary of S in X_T).

Proof. (1) \Rightarrow (2). Suppose $S = U(a^2) \cap W(b_1, \dots, b_n)$. Thus, if $P \in \overline{S} \setminus S$, then $a =_P 0$. Thus $\overline{S} \setminus S \subseteq Z(a)$ and clearly $S \cap Z(a) = \emptyset$.

(2) \Rightarrow (1). By compactness of S , $\exists a \in A$ such that $\overline{S} \setminus S \subseteq Z(a)$ and $S \cap Z(a) = \emptyset$. Look at the localization $A[\frac{1}{a}]$ and the preordering $T[\frac{1}{a^2}] \subseteq A[\frac{1}{a}]$. $X_{T[\frac{1}{a^2}]}$ is identified with $U(a^2) \subseteq X_T$. Thus $S \subseteq X_{T[\frac{1}{a^2}]} \subseteq X_T$ and S is closed in $X_{T[\frac{1}{a^2}]}$ by choice of a . Thus, by Corollary 1.22,

$$S = W_{T[\frac{1}{a^2}]}(b_1, \dots, b_n) = U_T(a^2) \cap W_T(b_1, \dots, b_n)$$

for some b_1, \dots, b_n which (after clearing denominators) are elements of A . \square

Theorem 1.24. *For any constructible $S \subseteq X_T$, the following are equivalent:*

- (1) S is basic open in X_T .
- (2) S is basic and open in X_T .
- (3) S is open in X_T and $S \cap \text{z-cl}(\partial S) = \emptyset$ and $S(p)$ is basic in $X_{T(p)}$ for each prime p .

Proof. (1) \Rightarrow (2) is clear and (2) \Leftrightarrow (3) is immediate from Corollary 1.23. Thus it only remains to establish (2) \Rightarrow (1). By (2) $S = U(b^2) \cap W(c_1, \dots, c_n)$ for some $b, c_1, \dots, c_n \in A$. Look at the localization $A[\frac{1}{b}]$ and the preordering $T[\frac{1}{b^2}] \subseteq A[\frac{1}{b}]$. Then $S \subseteq X_{T[\frac{1}{b^2}]} = U_T(b^2) \subseteq X_T$ and S is clopen in $X_{T[\frac{1}{b^2}]}$. To prove (1) it suffices (by compactness of $X_T \setminus S$) to show that, for each $P \in X_T \setminus S$, $\exists a \in A, a > 0$ on $S, a \leq_P 0$. This is clear if $P \notin X_{T[\frac{1}{b^2}]}$ (take $a = b^2$), so we can assume $P \in X_{T[\frac{1}{b^2}]}$. Thus, replacing A by $A[\frac{1}{b^2}]$ and T by $T[\frac{1}{b^2}]$, we are reduced to the case where S is clopen in X_T and $S = W(c_1, \dots, c_n)$. Let $Q \in X_T$ be the ordering maximal such that $Q \succ P$ (See Theorem 1.18). Since $X_T \setminus S$ is closed and $P \notin S$, it follows from Corollary 1.16 that $Q \notin S$. Since $S = W(c_1, \dots, c_n)$, $\exists c_i$ such that $c_i <_Q 0$. Applying the Positivstellensatz to $T' = \{a \in A : a \geq_Q 0\}$, we have $c_i < 0$ on $X_{T'} = \{Q\}$, so $-c_i(1+s) = 1+t$ for some $s, t \in T'$. But then

$$a := 1 + 2c_i(1+s)^2 = -(1 + 2(s+t+st))$$

satisfies $a > 0$ on S and $a <_Q 0$ (so $a <_P 0$). This completes the proof. \square

II CONSTRUCTIBLE SETS AND SEMI-ALGEBRAIC SETS

In this part, it is assumed the reader is familiar with basic results from the theory of real closed fields, in particular, with quantifier elimination and the transfer principle [5].

1. The basic correspondence

In the definition of constructible sets, A is any ring (commutative with 1) and T is any preordering of A . To get the connection between constructible sets and semi-algebraic sets, we have to specialize to the set-up considered in the introduction:

Fix an ordered field (F, P) and a real closed field extension R of (F, P) (so $P = F \cap R^2$). We consider algebraic sets and semi-algebraic sets in R^N which are defined over F . Denote the polynomial ring $F[X_1, \dots, X_N]$ by $F[X]$ for short. Fix $h_1, \dots, h_k \in F[X]$ and consider the algebraic set

$$V := \{x \in R^N : h_i(x) = 0 \text{ for } i = 1, \dots, k\}$$

and the finitely generated F -algebra

$$A := F[X]/(h_1, \dots, h_k).$$

(For example, we could take $k = 0$, so $V = R^N$, $A = F[X]$.) Let $T := \sum A^2 P$ (all finite sums $\sum a_i^2 t_i$, $a_i \in A$, $t_i \in P$). If $p \subseteq A$ is a prime, then $F(p)$ is a finitely generated field extension of F and $T(p) = \sum F(p)^2 P$. Thus $X_{T(p)}$ consists of all orderings on $F(p)$ extending the ordering P on F .

Note. We could take R to be the real closure of (F, P) but this is a bit restrictive (since we might want to take $F = \mathbb{Q}$, $R = \mathbb{R}$, for example). To obtain the classical case, take (F, P) real closed and $R = F$. In this case, $T = \sum A^2$, so $X_T = \text{Sper } A$.

Each $x = (x_1, \dots, x_N) \in V$ induces a homomorphism $A \rightarrow R$ defined by evaluation, i.e., $f \mapsto f(x)$. This has kernel $p_x := \{f \in A : f(x) = 0\}$ and image $F[x]$, so $F(p_x) \cong F(x) \subseteq R$. Thus we have an ordering P_x on A with support p_x obtained by pulling back the ordering $F(x) \cap R^2$ on $F(x)$. Thus we have a mapping

$$\Phi : V \rightarrow X_T, x \mapsto P_x.$$

Observe that $f =_{P_x} 0 \Leftrightarrow f(x) = 0$, $f >_{P_x} 0 \Leftrightarrow f(x) > 0$, and $f \geq_{P_x} 0 \Leftrightarrow f(x) \geq 0$. Consequently, for any $f \in A$,

$$\begin{aligned}\Phi^{-1}(Z(f)) &= \{x \in V : f(x) = 0\} \\ \Phi^{-1}(U(f)) &= \{x \in V : f(x) > 0\} \\ \Phi^{-1}(W(f)) &= \{x \in V : f(x) \geq 0\}.\end{aligned}$$

Sets of the form $\Phi^{-1}(S) \subseteq V$ where $S \subseteq X_T$ is constructible will be called *semi-algebraic sets* (more precisely, *semi-algebraic sets defined over F*). Since $S \mapsto \Phi^{-1}(S)$ preserves complements, finite unions, and finite intersections, the set of all semi-algebraic sets in V is a Boolean algebra. According to Corollary 1.14 (3), any semi-algebraic set in V is expressible as

$$\bigcup_{i=1}^m \{x \in V : f_{ij}(x) > 0, j = 1, \dots, n_i, g_i(x) = 0\}$$

for some integers $m, n_i \geq 0$ and some $f_{ij}, g_i \in A$ ($i = 1, \dots, m, j = 1, \dots, n_i$).

Semi-algebraic sets in V can also be described more directly as follows: they are just the subsets of V which are describable in the elementary language of real closed fields. That is, they are the sets of the form $\{x \in V : \Psi(a, x) \text{ holds in } R\}$ where $\Psi = \Psi(a, x)$ is an elementary statement in the language of real closed fields. Here, $x = (x_1, \dots, x_N)$ and $a = (a_1, \dots, a_M)$ is any array of elements of F . This follows from quantifier elimination.

Remark. A semi-algebraic set is defined over the real closure of (F, P) in R iff it is defined over F . This follows from quantifier elimination, since each $a \in R$ which is algebraic over F is described by some elementary statement Ψ_a with coefficients in F (the coefficients of the minimal polynomial of a).

The basic connection between semi-algebraic sets and constructible sets is given by the following:

Theorem 2.1. *The image of $\Phi : V \rightarrow X_T$ is dense in the Tychonoff topology (and hence also in the Harrison and Zariski topology). Consequently, the mapping $S \mapsto \Phi^{-1}(S)$ is injective on constructible sets. i.e., if $S_1, S_2 \subseteq X_T$ are constructible then $\Phi^{-1}(S_1) = \Phi^{-1}(S_2) \Rightarrow S_1 = S_2$.*

Proof. Let $S = (S_1 \setminus S_2) \cup (S_2 \setminus S_1)$. Then showing

$$\Phi^{-1}(S_1) = \Phi^{-1}(S_2) \Rightarrow S_1 = S_2$$

is equivalent to showing

$$\Phi^{-1}(S) = \emptyset \Rightarrow S = \emptyset.$$

Thus we are reduced to proving the first assertion. Sets of the form $U(f_1, \dots, f_m) \cap Z(g)$ are a basis for the Tychonoff topology so we are reduced further to showing that if the system

$$(*) \quad f_1(x) > 0, \dots, f_m(x) > 0, \quad g(x) = 0$$

has no solution $x \in V$, then $U(f_1, \dots, f_m) \cap Z(g) = \emptyset$. This follows from Tarski's transfer principle: Suppose $Q \in U(f_1, \dots, f_m) \cap Z(g)$ and let R_1 denote the real closure of $(F(q), Q)$ where $q = \text{Supp}(Q)$. Thus the system

$$(**) \quad f_1(x) > 0, \dots, f_m(x) > 0, \quad g(x) = 0, \quad h_1(x) = 0, \dots, h_k(x) = 0$$

has a solution $x \in R_1^N$. (Just take x_i to be the image of X_i via the composite map $F[X] \rightarrow A \rightarrow A/q \subseteq F(q) \subseteq R_1$, $i = 1, \dots, N$). Since R and R_1 both contain (F, P) , this implies $(**)$ has a solution in R^N and consequently that $(*)$ has a solution in V . \square

As an example of how Theorem 2.1 can be applied we now rewrite the Nullstellensatz (Corollary 1.11) in a more concrete form:

Corollary 2.2. *If $f \in A$ satisfies $f(x) = 0 \forall x \in V$, then $-f^{2k} \in T (= \sum A^2 P)$ for some integer $k \geq 0$ (and conversely).*

Proof. According to Corollary 1.11, it suffices to show that $f =_P 0 \forall P \in X_T$.

But this follows from Theorem 2.1 by considering the constructible sets

$$S_1 = \{P \in X_T : f =_P 0\}, S_2 = X_T.$$

□

Similarly, we have the following concrete version of the Positivstellensatz (Corollary 1.12):

Corollary 2.3. *For $f \in A$*

(1) $f(x) > 0 \forall x \in V \Rightarrow (1+s)f = 1+t$ for some $s, t \in T$ (and conversely).

(2) $f(x) \geq 0 \forall x \in V \Rightarrow (f^{2k}+s)f = f^{2k}+t$ for some $s, t \in T$ and some $k \geq 0$ (and conversely).

2. Finiteness theorem

By the *Euclidean* topology on V , we mean the topology induced by the product topology on R^N , where R is given the order topology.

It is clear that $\Phi : V \rightarrow X_T$ is continuous, giving V the Euclidean topology and X_T the Harrison topology (since polynomial functions are continuous in the Euclidean topology). But, to be able to interpret our results properly, we need a deeper result:

Theorem 2.4. (Finiteness Theorem) *If $S \subseteq X_T$ is constructible and $\Phi^{-1}(S)$ is open (resp., closed) in V in the Euclidean topology, then S is open (resp., closed) in X_T .*

This has been proved by several people. The proof given here is due to van den Dries; see [3].

Proof. Taking complements, it suffices to consider the case where $\Phi^{-1}(S)$ is closed in V . According to Corollary 1.16, we have to show

$$Q, Q' \in X_T, Q \prec Q', Q \in S \Rightarrow Q' \in S.$$

Let $q = \text{Supp}(Q)$ and let $x = (x_1, \dots, x_N)$ where $x_i \in A/q$ is the image of X_i , $i = 1, \dots, N$. Thus $A/q = F[x]$, $F(q) = F(x)$. Let $F[x] \subseteq B \subseteq F(x)$ be a Q -compatible valuation ring in $F(x)$ defining Q' . (See the Remark after Theorem 1.18). Let R_1 be the real closure of $(F(x), Q)$ and let C be the convex hull of B in R_1 . This is a valuation ring in R_1 compatible with the ordering on R_1 (Remark after Theorem 1.7) and $R_2 := C/M_C$ is real closed (Lemma 1.9), let $- : C \rightarrow R_2$ be the natural homomorphism. Let R_3 be any maximal subfield of C containing F . Then $R_3 \cap M_C = 0$ so $- : R_3 \rightarrow R_2$ is an embedding.

We claim R_3 is real closed and $- : R_3 \rightarrow R_2$ is an isomorphism. Since R_3 has a real closure in R_1 and C is integrally closed, it is clear that R_3 is real closed. Thus R_2 cannot be algebraic over the image of R_3 . On the other hand, if $\bar{t} \in R_2$ is transcendental over the image of R_3 , then $R_3 \subseteq R_3(t) \subseteq C$, contradicting the maximality of R_3 . This proves the claim.

Of course, since B is a valuation ring in $F(x)$ compatible with Q , B is its own convex hull in $F(x)$. Thus $C \cap F(x) = B$ so $B/M_B \subseteq C/M_C = R_2$ and Q' is the ordering on A induced by the homomorphism $A \rightarrow F[\bar{x}] \subseteq F(\bar{x}) \subseteq R_2$ where $\bar{x} := (\bar{x}_1, \dots, \bar{x}_N)$.

Now, for $i \in \{1, 2, 3\}$, $F \subseteq R_i$ so we can form the algebraic set $V_i \subseteq R_i^N$ and the mapping $\Phi_i : V_i \rightarrow X_T$ as in section 1. Moreover, by the transfer principle, $\Phi_i^{-1}(S)$ is closed in V_i (since $\Phi^{-1}(S)$ is closed in V). Assume now that $Q \in S$ but $Q' \notin S$. Then $x \in \Phi_1^{-1}(S)$ but $\bar{x} \notin \Phi_2^{-1}(S)$. Consequently, $y \notin \Phi_3^{-1}(S)$ where $y \in V_3$ is defined by $\bar{y}_i = \bar{x}_i$, $i = 1, \dots, N$. Thus we have $\varepsilon \in R_3$, $\varepsilon > 0$ such that

$$z \in V_3, |y_i - z_i| < \varepsilon, \quad i = 1, \dots, N \Rightarrow z \notin \Phi_3^{-1}(S).$$

But $R_3 \subseteq R_1$ so, by the transfer principle,

$$z \in V_1, |y_i - z_i| < \varepsilon, \quad i = 1, \dots, N \Rightarrow z \notin \Phi_1^{-1}(S).$$

On the other hand, $y_i - x_i \in M_C$ by definition of y_i , so we can apply this with $z = x$ to conclude $x \notin \Phi_1^{-1}(S)$. This contradicts our assumption. \square

Corollary 2.5 *Any semi-algebraic set in V which is open in V is expressible as a union of basic open sets*

$$\cup_{i=1}^m \{x \in V : f_{ij}(x) > 0, \quad j = 1, \dots, n_i\}$$

for some integers $m, n_i \geq 0$ and some $f_{ij} \in A, \quad i = 1, \dots, m, \quad j = 1, \dots, n_i$ (and similarly for closed).

Proof. Combine the finiteness theorem with Corollary 1.14 (1) (2). □

Theorems 2.1 and 2.4, when combined, allow us to transfer results back and forth between semi-algebraic sets in V and constructible sets in X_T in a most satisfactory manner. The reader can check this, by stating and proving the semi-algebraic analogues of Theorem 1.19 and Corollaries 1.22 and 1.23, for example. In this regard, the following result is also useful:

Theorem 2.6. *The closure (resp., interior) of a semi-algebraic set in V is semi-algebraic. Consequently (using Theorems 2.1 and 2.4) the closure (resp. interior) of a constructible set in X_T is constructible.*

Proof. Again, we only need deal with the assertion concerning closure. Let $S \subseteq X_T$ be constructible. By definition of closure, the closure of $\Phi^{-1}(S)$ is described by an elementary formula $\Psi = \Psi(a, x)$ in the language of real closed fields: here, $x = (x_1, \dots, x_N)$ and $a = (a_1, \dots, a_M)$ is an array of constants from F (= the coefficients of the various polynomials in the description of S). Thus, by elimination of quantifiers, the set

$$\overline{\Phi^{-1}(S)} = \{x \in V : \Psi(a, x) \text{ holds in } R\}$$

is semi-algebraic. □

Remark. $\Phi : V \rightarrow X_T$ is not injective in general. On the other hand, if the real closure of (F, P) is dense in R , one can show that Φ is injective and, moreover, that the topology on V obtained by pulling back the Harrison topology is just the Euclidean topology on V .

3. Dimension

To complete our study of the relationship between constructible sets and semi-algebraic sets, we need to know the meaning of the dimension of a constructible set, as defined in Part I, section 6. We begin by recalling a standard result from algebraic geometry:

Theorem 2.7 *Suppose D is a finitely generated F -algebra which is a domain and K is the quotient field of D . Then $\dim D = \text{trdeg}(K : F)$.*

Proof. The inequality $\dim D \leq \text{trdeg}(K : F)$ is an immediate consequence of the following:

Claim: Suppose $q_0 \subsetneq q_1 \subsetneq \cdots \subsetneq q_m$ is a chain of primes in D and $x_i \in q_i \setminus q_{i-1}$, $i = 1, \dots, m$. Then x_1, \dots, x_m are algebraically independent over F . The proof is by induction on m . Suppose $f(x_1, \dots, x_m) = 0$ for some non-zero polynomial f with coefficients in F . Dividing by a suitable power of x_1 , we can assume x_1 does not appear in some term. Applying the homomorphism $- : D \rightarrow D/q_1$ yields $f(0, \bar{x}_2, \dots, \bar{x}_m) = 0$. But this is a contradiction since, by induction on m , $\bar{x}_2, \dots, \bar{x}_m$ are algebraically independent over F .

The other inequality, $\dim D \geq \text{trdeg}(K : F)$, is less trivial. (For example, if $\dim D = 0$, this is Hilbert's Nullstellensatz). It can be proved as follows: By Noether normalization [2], $\exists x_1, \dots, x_n \in D$ algebraically independent over F with D integral over $F[x_1, \dots, x_n]$. Then K is algebraic over $F(x_1, \dots, x_n)$ so $\text{trdeg}(K : F) = n$. Clearly \exists a chain of primes of length n in $F[x_1, \dots, x_n]$. (e.g., take $q_i = (x_1, \dots, x_i)$, $i = 0, \dots, n$). By "going up" [2], this extends to a chain of primes of length n in D . \square

Thus, $\dim A/p = \text{trdeg}(F(p) : F)$ for any prime $p \subseteq A$ so, if $S \subseteq X_T$ is a constructible set, then, using the result in Part I, section 6,

$$\begin{aligned} \dim S &= \max\{\dim A/p : S \cap X_{T(p)} \neq \emptyset\} \\ &= \max\{\text{trdeg}(F(p) : F) : S \cap X_{T(p)} \neq \emptyset\}. \end{aligned}$$

But we would also like to know that the dimension of S coincides with the geometric dimension of $\Phi^{-1}(S)$, as defined in [5], for example (so, in particular,

$\dim X_T = \dim V$). For completeness, we outline the proof of this: Let $S_i \subseteq R^{N_i}$ be semi-algebraic sets, $i = 1, 2$. A function $f : S_1 \rightarrow S_2$ is called *semi-algebraic* if the graph

$$\text{Gr}(f) := \{(x, y) \in R^{N_1+N_2} : x \in S_1, y \in S_2, f(x) = y\}$$

is a semi-algebraic set. As usual, the semi-algebraic sets we consider are required to be defined over F . f is said to be a *semi-algebraic homeomorphism* if f is semi-algebraic, bijective, and bicontinuous in the Euclidean topology.

Theorem 2.8. *Suppose $\tilde{S} \subseteq V$ is semi-algebraic. Then*

- (1) *There exist semi-algebraic sets $\tilde{S}_1, \dots, \tilde{S}_p$ in V such that $\tilde{S} = \tilde{S}_1 \dot{\cup} \dots \dot{\cup} \tilde{S}_p$ (disjoint union) and \tilde{S}_i is semi-algebraically homeomorphic to the open d_i -cube*

$$]0, 1[^{d_i} := \{x \in R^{d_i} : 0 < x_i < 1, i = 1, \dots, d_i\}, \quad i = 1, \dots, p.$$

- (2) *In this situation, if $S \subseteq X_T$ is the unique constructible such that $\Phi^{-1}(S) = \tilde{S}$, then $\dim S = \max\{d_1, \dots, d_p\}$.*

Proof. If $F = R$ this follows from results on cylindrical decomposition in [5, Chapter 2]; specifically, [5, Corollaries 2.3.6 and 2.8.9]. The general case can be derived from this in a standard way [22, Lemma 1.5]: By the transfer principle, we can reduce to the case where R is the real closure of (F, P) . In this situation, a semi-algebraic set in R^N is defined over F iff it is defined over R , so this completes (1). For (2), use the fact that dimension doesn't change under integral extension (by "going up") plus the fact that orderings in X_T extend uniquely to orderings on the ring $R[X]/(h_1, \dots, h_k)$. \square

III ORDERINGS, VALUATIONS, AND QUADRATIC FORMS

[17] and [23] are excellent references for the material covered in Part III.

1. Quadratic forms

Let F be a field of characteristic 0. By a (non-degenerate diagonal quadratic) form of dimension m over F is meant an m -tuple $\rho = \langle a_1, \dots, a_m \rangle$, $a_1, \dots, a_m \in F^*$. Operations on forms are defined in the usual way [17]. Namely, if $\rho = \langle a_1, \dots, a_m \rangle$, $\psi = \langle b_1, \dots, b_n \rangle$, $c \in F^*$, $k \in \mathbb{N}$, we define

$$\begin{aligned}\rho \oplus \psi &:= \langle a_1, \dots, a_m, b_1, \dots, b_n \rangle \\ c\rho &:= \langle ca_1, \dots, ca_m \rangle \\ \rho \otimes \psi &:= a_1\psi \oplus \dots \oplus a_m\psi \\ k \times \rho &:= \rho \oplus \dots \oplus \rho \text{ (} k \text{ times)}.\end{aligned}$$

For a proper preordering $T \subseteq F$, the T -value set of ρ is $D_T(\rho) := a_1T + \dots + a_mT$. ρ is T -isotropic if $\exists t_1, \dots, t_m \in T$ not all zero such that $\sum_{i=1}^m a_i t_i = 0$. A form ρ which is not T -isotropic is said to be T -anisotropic.

Theorem 3.1

- (1) $D_T(\rho) = F \Leftrightarrow D_T(\rho) \cap -D_T(\rho) \neq \{0\} \Leftrightarrow \rho$ is T -isotropic.
- (2) $D_T(\rho) = D_T(k \times \rho)$. In particular, ρ is T -isotropic iff $k \times \rho$ is T -isotropic.
- (3) For $b \in F^*$, $b \in D_T(\rho) \Leftrightarrow \langle -b \rangle \oplus \rho$ is T -isotropic.
- (4) $a \in D_T(\rho \oplus \psi)$, $a \neq 0$, $\Rightarrow \exists b \in D_T(\rho), c \in D_T(\psi)$, $b, c \neq 0$ such that $a \in D_T(b, c)$.

(Actually, it is possible to choose b, c so that $a = b + c$, but this is another story.)

Proof. (1) Let $\rho = \langle a_1, \dots, a_m \rangle$. Replacing ρ by $a_1^{-1}\rho$, we can assume $a_1 = 1$. Thus $S := D_T(\rho)$ is a T -semi-preordering so $S \cap -S$ is an ideal in the field F (see proof of Theorem 1.1). This proves $D_T(\rho) = F \Leftrightarrow D_T(\rho) \cap -D_T(\rho) \neq \{0\}$. Now suppose $b \in D_T(\rho) \cap -D_T(\rho)$, $b \neq 0$. Then $b = \sum a_i s_i$, $-b = \sum a_i t_i$, $s_i, t_i \in T$ and s_i, t_i are not all zero (since $b \neq 0$). Then $0 = \sum a_i (s_i + t_i)$ and the $s_i + t_i \in T$ are not all zero (since $T \cap -T = \{0\}$). Thus ρ is T -isotropic. Conversely,

if $0 = \sum a_i t_i$ with $t_1, \dots, t_m \in T$ and $t_1 \neq 0$ say, then $-a_1 = \sum_{i=2}^m a_i t_i t_1^{-1}$ so $a_1 \in D_T(\rho) \cap -D_T(\rho)$.

(2) is clear.

(3) If $b = \sum a_i t_i$, $t_1, \dots, t_m \in T$, then $-b + \sum a_i t_i = 0$ so $\langle -b \rangle \oplus \rho$ is T -isotropic. Conversely, suppose $-bt_0 + a_1 t_1 + \dots + a_m t_m = 0$ for some $t_0, \dots, t_m \in T$ not all zero. If $t_0 \neq 0$, this yields $b = \sum a_i t_i t_0^{-1}$ so $b \in D_T(\rho)$. If $t_0 = 0$, then ρ is T -isotropic so $D_T(\rho) = F$ by (1) so $b \in D_T(\rho)$ holds in this case too.

(4) Suppose $\rho = \langle b_1, \dots, b_m \rangle$, $\psi = \langle c_1, \dots, c_n \rangle$, $a = \sum b_i s_i + \sum c_j t_j$ with $s_i, t_j \in T$. Since $a \neq 0$, one of the $\sum b_i s_i$, $\sum c_j t_j$ is $\neq 0$. If they are both not zero, take $b = \sum b_i s_i$, $c = \sum c_j t_j$. If one of them is zero, say $\sum c_j t_j = 0$, take $b = \sum b_i s_i$ and take $c \in D_T(\psi)$ arbitrary $\neq 0$. \square

For an ordering $P \in \text{Sper } F$, we define $\sigma_P : F^* \rightarrow \{\pm 1\}$ by

$$\sigma_P(a) = \begin{cases} 1 & \text{if } a \in P \\ -1 & \text{if } a \notin P \end{cases}.$$

The (Sylvester) *signature* of $\rho = \langle a_1, \dots, a_m \rangle$ at $P \in \text{Sper } F$ is defined by $\sigma_P(\rho) := \sum_{i=1}^m \sigma_P(a_i) \in \mathbb{Z}$. (Hopefully, this multiple use of the σ_P notation will cause no confusion). T -equivalence and T -isometry of forms ρ, ψ over F are defined as follows:

$$\begin{aligned} \rho \sim_T \psi & \text{ means } \sigma_P(\rho) = \sigma_P(\psi) \quad \forall P \in X_T, \\ \rho \cong_T \psi & \text{ means } \rho \sim_T \psi \text{ and } \dim(\rho) = \dim(\psi). \end{aligned}$$

Examples:

- (1) $\langle a \rangle \cong_T \langle at \rangle$ if $t \in T^*$.
- (2) $\langle a, b \rangle \cong_T \langle a + b, (a + b)ab \rangle$ if $a + b \neq 0$.
- (3) $\langle a, -a \rangle \sim_T 0$. (Here, $0 := \langle \rangle$, the zero dimensional form.)

Note:

- (1) $\sigma_P(\rho) \equiv \dim(\rho) \pmod{2}$. Thus $\rho \sim_T \psi \Rightarrow \dim(\rho) \equiv \dim(\psi) \pmod{2}$ (since $X_T \neq \emptyset$).

- (2) In particular, if $\rho \sim_T \psi$ and $\dim(\rho) \geq \dim(\psi)$, then $\rho \cong_T k \times \langle 1, -1 \rangle \oplus \psi$ where $k := \frac{\dim(\rho) - \dim(\psi)}{2}$.

Theorem 3.2

- (1) ρ is T -isotropic iff \exists a form ψ with $\dim(\psi) < \dim(\rho)$ and $\psi \sim_T \rho$.
- (2) Suppose $b \in F^*$. Then $b \in D_T(\rho)$ iff \exists a form ψ with $\rho \cong_T \langle b \rangle \oplus \psi$.

Proof. It is easy to prove (2) from (1) (or the other way around). Also, the implication (\Rightarrow) is easy. The implication (\Leftarrow) is not so easy.

We begin by proving the implication (\Rightarrow) of (2) by induction on $\dim(\rho) = m$. It is clear if $m = 1$, so we assume $m > 1$. Say $\rho = \langle a_1, \dots, a_m \rangle$. By Theorem 3.1(4), $\exists x \in D_T\langle a_2, \dots, a_m \rangle$, $x \neq 0$, such that $b \in D_T\langle a_1, x \rangle$ and, by induction on m , $\langle a_2, \dots, a_m \rangle \cong_T \langle x \rangle \oplus \psi_1$ for some form ψ_1 of dimension $m - 2$. But then $\rho \cong_T \langle a_1, \dots, a_m \rangle \cong_T \langle a_1, x \rangle \oplus \psi_1 \cong_T \langle b, a_1bx \rangle \oplus \psi_1$, so we can take $\psi = \langle a_1bx \rangle \oplus \psi_1$.

We use this to prove the implication (\Rightarrow) of (1). Suppose $\rho = \langle a_1, \dots, a_m \rangle$ is T -isotropic. By Theorem 3.1 (3), $-a_1 \in D_T\langle a_2, \dots, a_m \rangle$, so $\langle a_2, \dots, a_m \rangle \cong_T \langle -a_1 \rangle \oplus \psi$ for some form ψ of dimension $m - 2$. But then $\rho \cong_T \langle a_1, -a_1 \rangle \oplus \psi \sim_T \psi$.

We now prove the implication (\Leftarrow) of (2), assuming the implication (\Leftarrow) of (1). Suppose $\rho \cong_T \langle b \rangle \oplus \psi$. Then $\langle -b \rangle \oplus \rho \cong_T \langle -b, b \rangle \oplus \psi \sim_T \psi$ so $\langle -b \rangle \oplus \rho$ is T -isotropic and consequently, by Theorem 3.1 (3), $b \in D_T(\rho)$.

The implication (\Leftarrow) of (1) can be proved using Pfister's local-global principle [17]. Since we do not want to assume this here, we defer the proof until the end of §3 at which time we will have the Isotropy Theorem and the Baer-Krull-Springer theorem at our disposal. \square

Corollary 3.3 *If $\rho \cong_T \psi$ then $D_T(\rho) = D_T(\psi)$ and ρ is T -isotropic iff ψ is T -isotropic.*

Proof. This is immediate from the characterization of isotropy and value sets given in Theorem 3.2. \square

The Witt ring $W_T(F)$ is defined to be the set of T -equivalence classes of forms $\langle a_1, \dots, a_n \rangle$, $a_1, \dots, a_n \in F^*$, $n \geq 0$ with operations induced by \oplus and \otimes .

Remark. The reader familiar with quadratic form theory will know that $W_T(F)$ is a quotient of the usual Witt ring $W(F)$ [4], [17]. The kernel of the natural surjection $W(F) \rightarrow W_T(F)$ is generated as an ideal by the binary forms $\langle 1, -t \rangle$, $t \in T^*$. If $T = \sum F^2$, the kernel of $W(F) \rightarrow W_T(F)$ is just the torsion part of $W(F)$.

2. Baer-Krull-Springer theorem

If v is a valuation on F , denote by B_v , M_v , F_v the valuation ring, maximal ideal, and residue field respectively and by $\bar{} : B_v \rightarrow B_v/M_v = F_v$ the natural homomorphism. B_v^* denotes the unit group, i.e., $B_v^* := B_v \setminus M_v$. Let $T \subseteq F$ be a proper preordering. T_v denotes the pushdown of T to F_v , i.e., $T_v := \overline{T \cap B_v}$. This is a preordering in F_v . T^v denotes the smallest preordering in F containing T and $1 + M_v$.

Lemma 3.4. *The following are equivalent:*

- (1) T^v is proper.
- (2) T_v is proper.
- (3) $v(t_1 + \dots + t_n) = \min\{v(t_i) : i = 1, \dots, n\}$ for all $t_1, \dots, t_n \in T^*$.

Moreover, in this case, $T^v = T(1 + M_v)$.

Proof. (1) \Rightarrow (2): If T^v is proper then $\exists P \in X_{T^v}$ (Theorem 1.2) so $1 + M_v \subseteq P$ and consequently, the pushdown P_v is proper (Lemma 1.6). Since $T_v \subseteq P_v$, this implies T_v is proper.

(2) \Rightarrow (3) : If $v(\sum_{i=1}^n t_i) > \min\{v(t_i) : i = 1, \dots, n\}$ then, dividing by a term of lowest value and applying $- : B_v \rightarrow F_v$, we obtain $-1 \in T_v$, contradicting (2).

(3) \Rightarrow (1) : Suppose $y = \sum t_i(1 + x_i)$, $t_i \in T^*$, $x_i \in M_v$. Then $y = t(1 + x)$ where $t = \sum t_i$ and $x = (\sum t_i x_i)(\sum t_i)^{-1}$ and, by (3), $x \in M_v$. Thus $T^*(1 + M_v)$ is closed under addition so $T(1 + M_v)$ is a preordering. This proves $T^v = T(1 + M_v)$. If $-1 \in T^v$ then $-1 = t(1 + x)$ for some $t \in T^*$, $x \in M_v$. This forces $v(t) = 0$ and $v(1 + t) = v(-xt) > \min\{v(1), v(t)\} = 0$. This contradicts (3). \square

We say T, v are *compatible* if T^v is proper (equivalently, if T_v is proper). In terms of orderings, this just means that there exists an ordering $P \in X_T$ compatible with v (Theorem 1.2).

Suppose now that v is T -compatible (so $T^v = T(1 + M_v)$). We have a natural short exact sequence.

$$(*) \quad 0 \rightarrow F_v^*/T_v^* \xrightarrow{p} F^*/T^{v*} \xrightarrow{q} v(F^*)/v(T^*) \rightarrow 0.$$

(This is easy to check. p is given by $\bar{a}T_v^* \mapsto aT^{v*}$, and q is induced by v).

Note. If $T = \sum F^2$, Lemma 3.4 (3) gives $T_v = \sum F_v^2$ and $v(T^*) = 2v(F^*)$.

For a group G of exponent 2 (i.e., $a^2 = 1$ for all $a \in G$), a *character* on G is a group homomorphism $\sigma : G \rightarrow \{\pm 1\}$. The *character group* $\chi(G)$ of G is the set of all characters $\sigma : G \rightarrow \{\pm 1\}$ with multiplication defined by $(\sigma\tau)(a) = \sigma(a)\tau(a)$. $\chi(G)$ is a topological group, giving it the coarsest topology such that the mappings $\sigma \mapsto \sigma(a)$ ($\sigma \in \chi(G)$) are continuous for all $a \in G$. This topology is compact, Hausdorff, and totally disconnected. Also, $G \mapsto \chi(G)$ is a contravariant functor: If $f : G \rightarrow H$ is a group homomorphism of groups of exponent 2, then $\chi(f) : \chi(H) \rightarrow \chi(G)$ is given by $(\chi(f)(\sigma))(a) = \sigma(f(a))$ for all $\sigma \in \chi(H)$ and all $a \in G$.

We identify $X_T \hookrightarrow \chi(F^*/T^*)$ by identifying each $P \in X_T$ with the character on F^*/T^* induced by σ_P . The Harrison (=Tychonoff) topology on X_T is induced by the topology on $\chi(F^*/T^*)$. By Artin's Theorem (Theorem 1.2) X_T generates

$\chi(F^*/T^*)$ as a topological group.

Applying the functor $G \mapsto \chi(G)$ to $(*)$ yields the exact sequence of character groups:

$$(**) \quad 0 \rightarrow \chi(v(F^*)/v(T^*)) \xrightarrow{\chi(q)} \chi(F^*/T^{v*}) \xrightarrow{\chi(p)} \chi(F_v^*/T_v^*) \rightarrow 0.$$

We refer to $\chi(p)$ as *restriction* and denote $\chi(p)(\sigma)$ by $\bar{\sigma}$ for short. Thus $\bar{\sigma}(\bar{a}T_v^*) = \sigma(aT^{v*})$ for $a \in B_v^*$. After identifying $X_{T^*} \subseteq \chi(F^*/T^{v*})$, $X_{T_v^*} \subseteq \chi(F_v^*/T_v^*)$, one checks easily that the pushdown $P \mapsto P_v$ from X_{T^*} to $X_{T_v^*}$ is identified with the restriction map $\chi(p)$.

Also, using $(*)$, for each form ρ over F , \exists a form $\bar{\rho}$ obtained from ρ by permuting the entries and scaling the entries by suitable elements of T^* of the shape

$$\bar{\rho} = \langle x_1 a_{11}, \dots, x_1 a_{1n_1}, \dots, x_s a_{s1}, \dots, x_s a_{sn_s} \rangle = x_1 \rho_1 \oplus \dots \oplus x_s \rho_s$$

with $x_1, \dots, x_s \in F^*$, $v(x_1), \dots, v(x_s)$ distinct modulo $v(T^*)$ and with the

$$\rho_i := \langle a_{i1}, \dots, a_{in_i} \rangle, \quad i = 1, \dots, s$$

forms with entries in B_v^* . The induced forms $\bar{\rho}_i := \langle \bar{a}_{i1}, \dots, \bar{a}_{in_i} \rangle$, $i = 1, \dots, s$ over F_v are called the *residue forms* of ρ with respect to T, v .

Theorem 3.5. (Baer-Krull-Springer) *If v is T -compatible, then*

- (1) $X_{T^*} \rightarrow X_{T_v^*}$ is surjective. X_{T^*} consists of all characters on F^*/T^{v*} whose restriction to F_v^*/T_v^* lies in $X_{T_v^*}$.
- (2) $\rho \sim_{T^*} 0 \Leftrightarrow \bar{\rho}_i \sim_{T_v^*} 0$ for $i = 1, \dots, s$.
- (3) ρ is T^v -isotropic $\Leftrightarrow \bar{\rho}_i$ is T_v -isotropic for some $i \in \{1, \dots, s\}$.

In the literature, Part (1) of Theorem 3.5 is usually referred to as the Baer-Krull Theorem. Parts (2) and (3) generalize a result for discrete valuations due to Springer.

Proof. (See [4]). (1) is immediate from Lemma 1.8. (2): for $\sigma \in X_{T^*}$,

$$\begin{aligned}\sigma(\rho) &= \sigma(\bar{\rho}) = \Sigma_i \Sigma_j \sigma(x_i a_{ij}) = \Sigma_i \sigma(x_i) \Sigma_j \sigma(a_{ij}) \\ &= \Sigma_i \sigma(x_i) \Sigma_j \bar{\sigma}(\bar{a}_{ij}) = \Sigma_i \sigma(x_i) \bar{\sigma}(\bar{\rho}_i)\end{aligned}$$

where $\bar{\sigma} \in X_{T^*}$ denotes the restriction of σ to F_v^*/T_v^* . Thus, if $\bar{\sigma}(\bar{\rho}_i) = 0$, $i = 1, \dots, s$, then $\sigma(\rho) = 0$ so the implication (\Leftarrow) is clear using (1). To prove the other implication, suppose $\rho \sim_{T^*} 0$. Fix $\sigma \in X_{T^*}$ and suppose $\gamma \in \chi(F^*/T^{v*})$ satisfies $\bar{\gamma} = \bar{1}$. Then $\bar{\sigma}\bar{\gamma} = \bar{\sigma}\bar{\gamma} = \bar{\sigma}$ so we also have $\sigma\gamma \in X_{T^*}$ by (1). Thus, as before,

$$0 = (\sigma\gamma)(\rho) = \dots = \Sigma_i \sigma(x_i) \gamma(x_i) \bar{\sigma}(\bar{\rho}_i).$$

This holds for all $\gamma \in \text{Ker } \chi(p)$. By linear independence of characters [19] (x_1, \dots, x_s act as distinct characters on $\text{Ker } \chi(p)$), this means $\bar{\sigma}(\bar{\rho}_i) = 0$, $i = 1, \dots, s$. But $X_{T^*} \rightarrow X_{T_v}$ is surjective, so this holds for any $\bar{\sigma} \in X_{T_v}$ and consequently $\bar{\rho}_i \sim_{T_v} 0$, $i = 1, \dots, s$.

(3) (\Rightarrow) : If ρ is T^v -isotropic then we have $t_{ij} \in T$ not all zero and $y_{ij} \in M_v$ with

$$(*) \quad \Sigma_i \Sigma_j x_i a_{ij} t_{ij} (1 + y_{ij}) = 0.$$

Say $x_1 a_{11} t_{11} (1 + y_{11})$ is a non-zero term with minimum value. Since $v(x_1), \dots, v(x_s)$ are distinct modulo $v(T^*)$, the other terms of minimum value (if any) are of the form $x_1 a_{1j} t_{1j} (1 + y_{1j})$, $j \in \{2, \dots, n_1\}$. Thus, dividing $(*)$ by $x_1 t_{11}$ and applying $- : B_v \rightarrow F_v$ we see that $\bar{\rho}_1$ is T_v -isotropic. (\Leftarrow) : Conversely, suppose $\bar{\rho}_1$ (say) is T_v -isotropic. Then we have $t_{1j} \in T$, $j = 1, \dots, n_1$ with \bar{t}_{1j} not all zero and $\Sigma_j \bar{a}_{1j} \bar{t}_{1j} = 0$. Say $\bar{t}_{11} \neq 0$. Thus $x = \Sigma_j a_{1j} t_{1j} \in M_v$ so $\Sigma_j a_{1j} s_{1j} = 0$ where $s_{11} = t_{11} (1 - x(t_{11} a_{11})^{-1})$ and $s_{1j} = t_{1j}$ if $j \geq 2$. Thus $\Sigma_i \Sigma_j x_i a_{ij} s_{ij} = 0$ with $s_{ij} = 0$, $i \geq 2$. This completes the proof. \square

Remark. If one chooses a splitting for the exact sequence $(*)$, then the Witt ring $W_{T^*}(F)$ is identified with the group ring $W_{T_v}(F_v)[v(F^*)/v(T^*)]$. This is an immediate consequence of Theorem 3.5 (2).

3. Criterion for T -isotropy

This criterion was proved, originally, by Bröcker and Prestel (independently). The special version given here is taken from [4], [17].

Theorem 3.6 (Isotropy Theorem) *Suppose $T \subseteq F$ is a proper preordering and $\rho = \langle a_1, \dots, a_n \rangle$ is a form over F which is T -anisotropic. Then either*

- (1) ρ is P -definite, i.e. , $|\sigma_P(\rho)| = \dim(\rho)$, for some $P \in X_T$ or
- (2) \exists a valuation v on F such that T^v is proper, ρ is T^v -anisotropic, and not all of the $v(a_1), \dots, v(a_n)$ are in the same coset modulo $v(T^*)$ (so ρ has at least 2 residue forms with respect to T, v).

Proof. Replacing ρ by $a_1^{-1}\rho$, we can assume $a_1 = 1$. Thus $D_T(\rho)$ is a proper T -semi-preordering so, by Theorem 1.3, \exists a T -semi-ordering $S \subseteq F$ with $D_T(\rho) \subseteq S$. Let $<$ denote the associated linear ordering on $(F, +)$. Let v be the finest valuation on F compatible with S . By Theorem 1.7,

$$B_v = \{x \in F : -r \leq x \leq r \text{ for some } r \in \mathcal{Q}^+\},$$

$$M_v = \{x \in F : -r < x < r \text{ for all } r \in \mathcal{Q}^+\}.$$

Of course, $1 + M_v \subseteq S$ so, by Lemma 1.6, S induces a T_v -semi-ordering $S_v = \overline{B_v \cap S}$ on the residue field $F_v = B_v/M_v$. But S_v is Archimedean so, by Lemma 1.5, S_v is an ordering. Thus, by Theorem 3.5(1), $\exists P \in X_{T^*}$, $P_v = S_v$. If $v(a_i) \in v(T^*)$ for all $i = 1, \dots, n$ then $a_1, \dots, a_n \in (B_v \cap S^*)T^* \subseteq P^*$ (since $a_1, \dots, a_n \in S$ and $TS \subseteq S$) so $\sigma_P(\rho) = \dim(\rho)$ and we are done.

This leaves the case where $v(a_i) \not\equiv v(a_1) = v(1) \pmod{v(T^*)}$ for some $i \geq 2$. The problem is that ρ may not be T^v -anisotropic. To rectify this we go to a coarser valuation w . Take w to be the coarsest valuation coarser than v such that $w(a_i) \notin w(T^*)$ for some $i \in \{2, \dots, n\}$.

Claim 1. If $w(x) > 0$ then for each $i = 1, \dots, n$ $\exists t \in T^*$ such that $0 \leq w(a_i t) \leq w(x)$. For let $B_u = B_w[1/x]$. u is strictly coarser than w so

there exists $s \in T^*$ with $a_i s \in B_u^*$. $(a_i s)^{-1} = a_i s'$ where $s' = (a_i^2 s)^{-1} \in T^*$ so, replacing s by s' if necessary, we can assume $a_i s \in B_w$. Also, $(a_i s)^{-1} \in B_u$ so $(a_i s)^{-1} = b x^{-k}$ for some $b \in B_w$, $k \geq 1$. Thus $0 \leq w(a_i s) \leq w(x^k)$. Choose $k \geq 1$ minimal so that this is so. Then $0 \leq w(x^{k-1}) \leq w(a_i s) \leq w(x^k)$. If $k = 2m + 1$, take $t = s x^{-2m}$. If $k = 2m$ take $t = x^{2m} (a_i^2 s)^{-1}$.

Of course, w is coarser than v so $B_w \supseteq B_v$, $M_w \subseteq M_v$ so $T^w \subseteq T^v$. Also, by construction, $\exists i \geq 2$ with $w(a_i) \not\equiv w(a_1) = w(1) \pmod{w(T^*)}$. Also, $1 + M_w \subseteq 1 + M_v \subseteq S$ so, by Lemma 1.6, $(B_w^* \cap S)(1 + M_w) \subseteq S$. We show ρ is T^w -anisotropic by means of the following:

Claim 2. $(1 + M_w)a_i \subseteq S$ for $i = 1, \dots, n$.

Once this is established then $\sum T^w a_i = \sum T(1 + M_w)a_i \subseteq \sum TS \subseteq S$ so ρ is T^w -anisotropic and we are done.

Suppose, to the contrary, that $x \in M_w$, $(1 - x)a_i < 0$ so $0 < a_i < x a_i$. By claim 1, $\exists t \in T^*$ such that $0 \leq w(a_i t) \leq w(x)$. Dividing by $a_i^2 t \in T^*$ we obtain

$$(*) \quad 0 < (a_i t)^{-1} < x(a_i t)^{-1}.$$

If $w(x(a_i t)^{-1}) > 0$ then $v(x(a_i t)^{-1}) > 0$ so $x(a_i t)^{-1} \in M_v$ so $(a_i t)^{-1} \in M_v \subseteq B_v \subseteq B_w$ (by (*), looking at the definition of M_v). This forces $w(a_i t) = 0$ so $(1 - x)a_i t \in (1 + M_w)(B_w^* \cap S^*) \subseteq S^*$, a contradiction. This leaves the case $w(x(a_i t)^{-1}) = 0$. But then $a_i t x^{-1}(1 - x) \in (B_w^* \cap S^*)(1 + M_w) \subseteq S^*$ so $a_i t x^{-1} > a_i t > 0$ contradicting (*) (using Lemma 1.4(3)). \square

The Baer-Krull-Springer Theorem and the Isotropy Theorem can be combined nicely to prove facts about quadratic forms by induction on the dimension. As an example, we now give the long promised proof of Theorem 3.2:

Proof of Theorem 3.2. It remains to show that if ρ, ψ are forms over F with ρ T -anisotropic, $\psi \sim_T \rho$, then $\dim(\psi) \geq \dim(\rho)$. The proof is by induction on $n = \dim(\rho)$. By Theorem 3.6, there are two possibilities:

(1) $|\sigma_P(\rho)| = \dim(\rho)$ for some $P \in X_T$. In this case

$$\dim(\psi) \geq |\sigma_P(\psi)| = |\sigma_P(\rho)| = \dim(\rho).$$

(2) \exists a T -compatible valuation v with ρ T^v -anisotropic, and ρ has a least two residue forms with respect to T, v . Let

$$\rho \cong_T x_1 \rho_1 \oplus \cdots \oplus x_s \rho_s, \quad \psi \cong_T x_1 \psi_1 \oplus \cdots \oplus x_s \psi_s$$

be the residue form decompositions of ρ, ψ with respect to v, T . By Theorem 3.5 (2) (applied to $\psi \oplus -\rho$), $\bar{\psi}_i \sim_{T_v} \bar{\rho}_i$ and, by Theorem 3.5 (3) each $\bar{\rho}_i$ is T_v -anisotropic (or 0-dimensional). Thus, by induction on n , $\dim(\bar{\psi}_i) \geq \dim(\bar{\rho}_i)$, $i = 1, \dots, s$, so $\dim(\psi) \geq \dim(\rho)$. \square

The next result, although not used in what follows, is another application of the method:

Theorem 3.7. *If ρ is T -anisotropic, then \exists a preordering $T \subseteq \tilde{T} \subseteq F$ with ρ \tilde{T} -anisotropic and $|F^*/\tilde{T}^*| < \infty$.*

Proof. (See [4]). By induction on $n = \dim(\rho)$. If $|\sigma_P(\rho)| = \dim(\rho)$ for some $P \in X_T$, take $\tilde{T} = P$. Otherwise \exists a T -compatible valuation v such that ρ is T^v -anisotropic and has at least two residue forms. Say $\rho \cong_T x_1 \rho_1 \oplus \cdots \oplus x_s \rho_s$, $s \geq 2$, is the decomposition into residue forms. By Theorem 3.5, the residue forms $\bar{\rho}_1, \dots, \bar{\rho}_s$ are T_v -anisotropic. By induction on n \exists preorderings S_i , $i = 1, \dots, s$ $T_v \subseteq S_i \subseteq F_v$, $|F_v^*/S_i^*| < \infty$ with $\bar{\rho}_i$ S_i -anisotropic. Thus $\bar{\rho}_1, \dots, \bar{\rho}_s$ are all $\cap_{i=1}^s S_i$ -anisotropic and $|F_v^*/(\cap_i S_i^*)| \leq \prod_i |F_v^*/S_i^*| < \infty$. Pick $\tilde{T} \supseteq T^v$ maximal such that (1) $\tilde{T}_v = \cap_i S_i$ and (2) $v(x_1), \dots, v(x_s)$ are still distinct modulo $v(\tilde{T}^*)$. It is pretty clear that such a preordering \tilde{T} exists and that it has all the required properties. ($\tilde{T} = \tilde{T}^v$ and ρ is \tilde{T}^v -anisotropic by Theorem 3.5: the residue forms of ρ with respect to \tilde{T}, v are the same as the residue forms of ρ with respect to T, v .) \square

Remark. Looking ahead a bit, in Part IV we will be using this same combination of the Baer-Krull-Springer Theorem and the Isotropy Theorem:

- (1) to get a valuation-theoretic description of the stability index s_T ; see Theorems 4.4, 4.5 and Corollaries 4.6, 4.7
- (2) to get a bound for the t -invariant in terms of the stability index; see Theorem 4.15 and Corollary 4.16.

At the same time, it is worth mentioning that there are other important applications which will not be discussed here, e.g.,

- (3) to the description of the Witt ring $W_T(F)$ as a subring of the ring of all continuous functions from X_T to \mathbb{Z} ; see [4].

IV MINIMAL GENERATION OF CONSTRUCTIBLE SETS

1. Pfister forms

Let T be a (proper) preordering in a field F . X_T with the Harrison (=Tychonoff) topology is compact Hausdorff and totally disconnected. Basic clopen sets in X_T have the form

$$U(a_1, \dots, a_n) = U_T(a_1, \dots, a_n) = \{P \in X_T : a_i >_P 0, i = 1, \dots, n\},$$

$n \geq 1$, $a_1, \dots, a_n \in F^*$. These are closely related to n -fold Pfister forms which are defined as follows:

Definition. An n -fold Pfister form over F is a form of the type

$$\langle\langle a_1, \dots, a_n \rangle\rangle := \langle 1, a_1 \rangle \otimes \dots \otimes \langle 1, a_n \rangle, \quad n \geq 1, \quad a_1, \dots, a_n \in F^*.$$

The *derived form* $\langle\langle a_1, \dots, a_n \rangle\rangle'$ of the Pfister form $\langle\langle a_1, \dots, a_n \rangle\rangle$ is defined by $\langle\langle a_1, \dots, a_n \rangle\rangle = \langle 1 \rangle \oplus \langle\langle a_1, \dots, a_n \rangle\rangle'$.

(Thus $\langle\langle a \rangle\rangle = \langle 1, a \rangle$, $\langle\langle a, b \rangle\rangle = \langle 1, a, b, ab \rangle$, $\langle\langle a \rangle\rangle' = \langle a \rangle$, $\langle\langle a, b \rangle\rangle' = \langle a, b, ab \rangle$, etc.). Convention: $\langle 1 \rangle$ is the unique 0-fold Pfister form. The derived form in this case is the empty (0-dimensional) form.

Theorem 4.1 If $P \in X_T$, $\rho = \langle\langle a_1, \dots, a_n \rangle\rangle$, then

$$(1) \sigma_P(\rho) = \prod_{i=1}^n (1 + \sigma_P(a_i)) = \begin{cases} 2^n & \text{if } P \in U(a_1, \dots, a_n) \\ 0 & \text{otherwise.} \end{cases}$$

$$(2) \rho \cong_T \langle \langle b_1, \dots, b_n \rangle \rangle \text{ iff } U(a_1, \dots, a_n) = U(b_1, \dots, b_n).$$

$$(3) \rho \text{ is } T\text{-isotropic iff } \rho \sim_T 0 \text{ iff } U(a_1, \dots, a_n) = \emptyset.$$

Proof. (1) is clear and (2) is immediate from (1). (3): It is clear from (1) that $\rho \sim_T 0$ iff $U(a_1, \dots, a_n) = \emptyset$. If $U(a_1, \dots, a_n) \neq \emptyset$ then $\exists P \in X_T$ with $\sigma_P(\rho) = 2^n = \dim(\rho)$ (so ρ is P -definite). Consequently, ρ is T -anisotropic in this case. On the other hand, if $U(a_1, \dots, a_n) = \emptyset$ then $\rho \sim_T 0$, so ρ is T -isotropic (by Theorem 3.2). \square

Theorem 4.2 *If $b \in D_T(\langle \langle a_1, \dots, a_n \rangle \rangle')$, $b \neq 0$, then $\exists b_2, \dots, b_n \in F^*$ such that $U(a_1, \dots, a_n) = U(b, b_2, \dots, b_n)$.*

Proof. By induction on n . If $n = 1$, $\langle \langle a_1 \rangle \rangle' = \langle a_1 \rangle$ so $b = ta_1$, $t \in T$, $t \neq 0$. The result is clear in this case. Suppose $n \geq 2$. Decompose $\rho = \langle \langle a_1, \dots, a_n \rangle \rangle$ as $\rho = \langle 1, a_1 \rangle \otimes \psi = \psi \oplus a_1\psi$ where $\psi = \langle \langle a_2, \dots, a_n \rangle \rangle$. Thus $\rho' = \psi' \oplus a_1\psi$ so, by Theorem 3.1(4), $b \in D_T(\langle c, a_1d \rangle)$ for some non-zero $c \in D_T(\psi')$, $d \in D_T(\psi)$. By induction $\exists b_3, \dots, b_n \in F^*$ with

$$(*) \quad U(a_2, \dots, a_n) = U(c, b_3, \dots, b_n).$$

We claim this implies $U(a_1, \dots, a_n) = U(b, a_1cd, b_3, \dots, b_n)$ (so we are done, taking $b_2 = a_1cd$). Let $P \in X_T$. Suppose first that $a_i >_P 0$, $i = 1, \dots, n$. Then $b, c, d >_P 0$ (since $b, c, d \in D_T(\rho)$) and $b_3, \dots, b_n >_P 0$ by (*), so $P \in U(b, a_1cd, b_3, \dots, b_n)$. Conversely, suppose $b, a_1cd, b_3, \dots, b_n >_P 0$. Then, since $b \in D_T(\langle c, a_1d \rangle)$, $bc \in D_T(\langle c^2, a_1cd \rangle)$ so $bc >_P 0$ and hence $c >_P 0$. Thus $a_2, \dots, a_n >_P 0$ using (*) so $d >_P 0$ (since $d \in D_T(\psi)$). Finally, from $a_1cd >_P 0$ it follows that $a_1 >_P 0$ too. \square

Corollary 4.3. *For $a_1, \dots, a_n \in F^*$, $n \geq 1$, the following are equivalent:*

$$(1) \exists b_2, \dots, b_n \in F^* \text{ such that } U(a_1, \dots, a_n) = U(b_2, \dots, b_n).$$

(2) $1 \in D_T \langle \langle a_1, \dots, a_n \rangle \rangle'$, i.e., $\langle -1 \rangle \oplus \langle \langle a_1, \dots, a_n \rangle \rangle'$ is T -isotropic.

Proof. If (1) holds, then $\langle \langle a_1, \dots, a_n \rangle \rangle \cong_T 2 \times \langle \langle b_2, \dots, b_n \rangle \rangle$ (by Theorem 4.1) so $\langle \langle a_1, \dots, a_n \rangle \rangle' \cong_T \langle 1 \rangle \oplus 2 \times \langle \langle b_2, \dots, b_n \rangle \rangle'$. Thus (2) holds (using Theorem 3.2). Conversely, if (2) holds, then $U(a_1, \dots, a_n) = U(1, b_2, \dots, b_n) = U(b_2, \dots, b_n)$ by Theorem 4.2. \square

2. The stability index

We continue with the assumptions of §1, i.e., F is a field and $T \subseteq F$ is a proper preordering. $S = U(a_1, \dots, a_n)$, $a_1, \dots, a_n \in F^*$, is a fixed basic clopen set in X_T and $\rho = \langle \langle a_1, \dots, a_n \rangle \rangle$.

We say the presentation $S = U(a_1, \dots, a_n)$ is *minimal* if $\nexists b_2, \dots, b_n \in F^*$ such that $S = U(b_2, \dots, b_n)$. According to Corollary 4.3, this occurs iff $\langle -1 \rangle \oplus \rho'$ is T -anisotropic.

Theorem 4.4

- (1) Suppose the presentation $S = U_T(a_1, \dots, a_n)$ is minimal. Then either $n \leq 1$ or \exists a T -compatible valuation v on F such that the presentation $S^v = U_{T^*}(a_1, \dots, a_n)$ is minimal and at least one of $v(a_1), \dots, v(a_n)$ is not in $v(T^*)$.
- (2) Suppose v is any T -compatible valuation and a_1, \dots, a_n are such that $v(a_1), \dots, v(a_k)$ are \mathbb{Z}_2 -independent modulo $v(T^*)$ and $a_{k+1}, \dots, a_n \in B_v^*$. Then the presentation $S^v = U_{T^*}(a_1, \dots, a_n)$ is minimal iff the presentation $S_v = U_{T_v}(\bar{a}_{k+1}, \dots, \bar{a}_n)$ is minimal (assuming $S_v \neq \emptyset$).

Proof. (1) We can suppose $n \geq 2$. By Corollary 4.3, $\langle -1 \rangle \oplus \rho'$ is T -anisotropic. For any $P \in X_T$, at least one of $a_1, a_2, a_1 a_2$ is positive at P , so $\langle -1 \rangle \oplus \rho'$ is P -indefinite. Thus, by Theorem 3.6, \exists a T -compatible valuation v such that $\langle -1 \rangle \oplus \rho'$ is T^v -anisotropic and the $v(a_i)$ are not all in $v(T^*)$.

(2) Let $\bar{\rho} = \langle \langle \bar{a}_{k+1}, \dots, \bar{a}_n \rangle \rangle$. Since

$$\rho = \langle \langle a_1, \dots, a_k \rangle \rangle \otimes \langle \langle a_{k+1}, \dots, a_n \rangle \rangle = \sum a_1^{t_1} \cdots a_k^{t_k} \langle \langle a_{k+1}, \dots, a_n \rangle \rangle,$$

(t_1, \dots, t_k) running through $\{0, 1\}^k$, the residue forms of $\langle -1 \rangle \oplus \rho'$ are

$$\begin{cases} \langle -1 \rangle \oplus \bar{\rho}' & (\text{occurring once}) \\ \bar{\rho} & (\text{occurring } 2^k - 1 \text{ times}). \end{cases}$$

Thus, if $\langle -1 \rangle \oplus \rho'$ is T^v -anisotropic, then these forms are T_v -anisotropic (Theorem 3.5). In particular, $\langle -1 \rangle \oplus \bar{\rho}'$ is T_v -anisotropic. Conversely, if $\langle -1 \rangle \oplus \bar{\rho}'$ is T_v -anisotropic, then so is $\bar{\rho}$. (Use Theorem 4.1(3) if $n \geq k+2$. If $n = k+1$, use $S_v \neq \emptyset$). But then, by Theorem 3.5, $\langle -1 \rangle \oplus \rho'$ is T^v -anisotropic. \square

Remark. The special hypothesis on a_1, \dots, a_n in Theorem 4.4 (2) is not restrictive. We can always rearrange a_1, \dots, a_n so that $v(a_1), \dots, v(a_k)$ are \mathbb{Z}_2 -independent modulo $v(T^*)$ and, for $j = k+1, \dots, n$,

$$a_j \equiv b_j \prod_{i=1}^k a_i^{s_{ij}} \pmod{T^*}, \quad s_{ij} \in \{0, 1\}, \quad b_j \in B_v^*.$$

Then, modulo T^* , $a_1, \dots, a_k, b_{k+1}, \dots, b_n$ generate the same group as a_1, \dots, a_n so $S = U_T(a_1, \dots, a_n) = U_T(a_1, \dots, a_k, b_{k+1}, \dots, b_n)$.

Theorem 4.5. Suppose the presentation $S = U_T(a_1, \dots, a_n)$ is minimal. Then \exists a T -compatible valuation v on F such that the presentation remains minimal over T^v and such that at least $n-1$ of the $v(a_i)$ are \mathbb{Z}_2 -independent modulo $v(T^*)$.

Proof. If $n \leq 1$, take v to be the trivial valuation. Assume $n \geq 2$. By Theorem 4.4 (1), \exists a T -compatible valuation v such that the presentation remains minimal over T^v and at least one of the $v(a_i)$ is not in $v(T^*)$. By the Remark, we can assume $v(a_1), \dots, v(a_k)$ are \mathbb{Z}_2 -independent modulo $v(T^*)$ and $a_{k+1}, \dots, a_n \in B_v^*$. Thus, by Theorem 4.4(2), the presentation $S_v = U_{T_v}(\bar{a}_{k+1}, \dots, \bar{a}_n)$ is minimal. By induction on n , we have a T_v -compatible valuation w on F_v and $s \in \{n-1, n\}$ such that this presentation of S_v remains minimal over $(T_v)^w$ and, after reindexing, $w(\bar{a}_i)$, $i = k+1, \dots, s$ are

\mathbb{Z}_2 -independent modulo $w(T_v^*)$. Looking at the valuation u on F associated to w , we have $F_u = (F_v)_w$, $T_u = (T_v)_w$ and we have the natural exact sequence

$$(*) \quad 0 \rightarrow w(F_v^*)/w(T_v^*) \rightarrow u(F^*)/u(T^*) \rightarrow v(F^*)/v(T^*) \rightarrow 0.$$

Now one checks immediately that the presentation $S^u = U_{T^*}(a_1, \dots, a_n)$ is minimal and the $u(a_i)$, $i = 1, \dots, s$ are \mathbb{Z}_2 -independent modulo $u(T^*)$. \square

The *stability index* s_T is defined as follows: If $|X_T| = 1$, then $s_T := 0$. If $|X_T| \geq 2$, then s_T is the least integer $s \geq 1$ such that each basic clopen set $S \subseteq X_T$ is expressible as $S = U(a_1, \dots, a_s)$ for some $a_1, \dots, a_s \in F^*$ (or $s_T = \infty$ if no such finite s exists).

Corollary 4.6. (Bröcker)

(1) If $|X_T| > 1$, then

$$s_T = \sup\{1, s_{T^*} : v \text{ is a } T\text{-compatible valuation on } F, v(T^*) \neq v(F^*)\}.$$

(2) $s_{T^*} = \dim_2 v(F^*)/v(T^*) + s_{T^*}$. (Here, \dim_2 denotes dimension as a \mathbb{Z}_2 -vector space).

Proof. This is immediate from Theorem 4.4. \square

Also, we define

$$\bar{s}_T := \sup\{\dim_2 v(F^*)/v(T^*) : v \text{ is a } T\text{-compatible valuation on } F\}.$$

Corollary 4.7. s_T is finite iff \bar{s}_T is finite. Moreover, in this case $s_T = \bar{s}_T + \varepsilon_T$ where $\varepsilon_T \in \{0, 1\}$ is defined as follows: $\varepsilon_T = 0$ iff $|X_{T^*}| = 1$ holds for all T -compatible valuations v with $\dim_2 v(F^*)/v(T^*) = \bar{s}_T$. Otherwise, $\varepsilon_T = 1$.

Proof. Immediate from Theorem 4.5. \square

Remark. There are various other characterizations of s_T [4], [17]. For example, 2^{s_T} is the exponent of the cokernel of the natural embedding $W_T(F) \hookrightarrow \text{Cont}(X_T, \mathbb{Z})$. This will not be proved here (even though the ingredients are all close at hand; see Theorem 4.2 and Lemma 4.14 below).

3. Complexity of basic open sets

In Part V we will come back to Corollary 4.7, using it to study the behaviour of the stability index under field extension (see Theorem 5.1).

But, for now, we return to the general situation considered in Part I. i.e., A is a ring (commutative with 1), $T \subseteq A$ is a proper preordering, and $X_T := \dot{\cup}_p X_{T(p)}$, p running through the primes of A with $T(p) \subseteq F(p)$ proper. For $S \subseteq X_T$, $S(p) := S \cap X_{T(p)}$.

The following result was proved first by Bröcker and Scheiderer in the case of the coordinate ring of a real variety. The general version presented here is taken from [21].

Theorem 4.8. *Suppose $S \subseteq X_T$ is basic open. Suppose $\exists k \geq 0$ such that, for each prime $p \subseteq A$ with $T(p)$ proper, $\exists b_1, \dots, b_k \in F(p)^*$ such that $S(p) = U_{T(p)}(b_1, \dots, b_k)$. Then $\exists a_1, \dots, a_k \in A$ such that $S = U_T(a_1, \dots, a_k)$.*

The proof is similar to the proof in [20]. We use a little notation from the theory of quadratic forms: $A^* :=$ the unit group of A . If $\rho = \langle a_1, \dots, a_n \rangle$, $a_1, \dots, a_n \in A^*$ (or A), the T -value set of ρ is $D_T(\rho) := \sum_i a_i T$. The operations \oplus, \otimes , etc; on forms are defined as in the field case. As usual, $\langle \langle a_1, \dots, a_n \rangle \rangle$ denotes the n -fold Pfister form $\langle 1, a_1 \rangle \otimes \dots \otimes \langle 1, a_n \rangle$.

Proof of Theorem 4.8 The case $k = 0$ is trivial. (If $S(p) = X_{T(p)}$ for all p , then $S = X_T$). Assume $k \geq 1$. By hypothesis, $\exists a_1, \dots, a_n \in A$ such that $S = U_T(a_1, \dots, a_n)$. If $n \leq k$ we are done. Thus we assume $n > k$ and try to reduce from n to $n - 1$.

Claim : We can assume each $a \in A$ satisfying $a \neq 0$ on S is in A^* . For, consider the localization $B = \Sigma^{-1}A$ where

$$\Sigma = \{a \in A : a \neq 0 \text{ on } S\} = A \setminus \bigcup \{\text{Supp}(P) : P \in S\}.$$

Let $\Sigma^{-2}T$ denote the extension of T to B , i.e., $\Sigma^{-2}T = \{t/a^2 : t \in T, a \in \Sigma\}$. After identifying $X_{\Sigma^{-2}T} \subseteq X_T$, $X_{\Sigma^{-2}T}$ is identified with $U_T(\Sigma^2) \subseteq X_T$

and $S \subseteq U_T(\Sigma^2)$ by definition of Σ . Thus it suffices to prove the result for $S \subseteq X_{\Sigma^{-2}T}$. For suppose we have proved $S = U_{\Sigma^{-2}T}(b_2, \dots, b_n)$ for some $b_2, \dots, b_n \in B$. Clearing fractions, we can suppose $b_2, \dots, b_n \in A$ so then $S = U_T(b_2, \dots, b_n) \cap U_T(\Sigma^2)$. Thus, by compactness of $X_T \setminus S$ in the Tychonoff topology, $S = U_T(b_2, \dots, b_n, a^2) = U_T(a^2 b_2, b_3, \dots, b_n)$ for some $a \in \Sigma$. Thus, replacing A by $B = \Sigma^{-1}A$ and T by $\Sigma^{-2}T$, we can assume $\Sigma \subseteq A^*$. This proves the claim.

Thus, for example, since $2 > 0$ and $a_i > 0$ on S , we have $2, a_1, \dots, a_n \in A^*$. Now set $\rho = \langle \langle a_1, \dots, a_n \rangle \rangle$ and consider the semi-preordering $M := D_T(\langle 1 \rangle \oplus -\rho')$ where ρ' is the derived form, i.e., $\rho = \langle 1 \rangle \oplus \rho'$. If $-1 \notin M$, then M is proper so, by Theorem 1.1, $-1 \notin M(p) = D_{T(p)}(\langle 1 \rangle \oplus -\rho')$ for some prime $p \subseteq A$. This contradicts our hypothesis. After all, $S(p) = U_{T(p)}(a_1, \dots, a_n) = U_{T(p)}(b_1, \dots, b_k)$ for some $b_1, \dots, b_k \in F(p)^*$, $k < n$, so, by Corollary 4.3, $\langle 1 \rangle \oplus -\rho'$ is $T(p)$ -isotropic. Thus $-1 \in M$ so $-1 = t - b$, i.e., $b = 1 + t$ for some $b \in D_T(\rho')$, $t \in T$. We now prove the following generalization of Theorem 4.2 by induction on n :

Theorem 4.9. *Suppose $S = U_T(a_1, \dots, a_n)$, $\rho = \langle \langle a_1, \dots, a_n \rangle \rangle$, for some $a_1, \dots, a_n \in A$ and suppose $b \in D_T(\rho')$ satisfies $b \neq 0$ on S . Then $\exists b_2, \dots, b_n \in A$ such that $S = U_T(b, b_2, \dots, b_n)$.*

Applying this with $b = 1+t$ gives the desired reduction: $S = U_T(a_1, \dots, a_n) = U_T(b_2, \dots, b_n)$ (since $b > 0$ on X_T). Thus it only remains to prove Theorem 4.9.

Proof of Theorem 4.9. This is clear if $n = 1$, so we assume $n \geq 2$. If $\Sigma = \{a \in A : a \neq 0 \text{ on } S\}$ and $S = U_{\Sigma^{-2}T}(b, b_2, \dots, b_n)$ then, by compactness, $S = U_T(b, b_2, \dots, b_n, a^2) = U_T(b, a^2 b_2, b_3, \dots, b_n)$ for some $a \in \Sigma$. Thus, replacing A by $B = \Sigma^{-1}A$ and T by $\Sigma^{-2}T$, we may as well assume to begin with that $\Sigma \subseteq A^*$. Write $\rho = \psi \oplus a_1 \psi$ where $\psi = \langle \langle a_2, \dots, a_n \rangle \rangle$, so $\rho' = \psi' \oplus a_1 \psi$. Thus $b = c + da_1$ with $c \in D_T(\psi')$, $d \in D_T(\psi)$. We can assume $c, d \in A^*$. To prove this use the identity $x = (\frac{x+1}{2})^2 - (\frac{x-1}{2})^2$ to write $\frac{a_1+d}{b} = r^2 - s^2$, $r, s \in A$. Thus

$r^2b = s^2b + a_1 + a_2$ so

$$\begin{aligned}(1 + r^2)b &= (1 + s^2)b + a_1 + a_2 = (1 + s^2)(c + da_1) + a_1 + a_2 \\ &= (1 + s^2)c + a_2 + ((1 + s^2)d + 1)a_1.\end{aligned}$$

Thus $b = c' + d'a_1$ where

$$c' = \frac{(1 + s^2)c + a_2}{1 + r^2}, \quad d' = \frac{(1 + s^2)d + 1}{1 + r^2}.$$

Thus $c' \in D_T(\psi'), d' \in D_T(\psi)$. The point is, c', d' are strictly positive on S so $c', d' \in A^*$. Thus, replacing c, d by c', d' we can assume $c, d \in A^*$. Thus, by induction on n , $\exists b_3, \dots, b_n \in A$ such that

$$U_T(a_2, \dots, a_n) = U_T(c, b_3, \dots, b_n).$$

But now we see, exactly as in the proof of Theorem 4.2, that $S = U_T(b, a_1cd, b_3, \dots, b_n)$ so we are done, taking $b_2 = a_1cd$. \square

Corollary 4.10 *For any proper preordering T in any ring A , each basic open set $S \subseteq X_T$ is expressible as $S = U_T(a_1, \dots, a_m)$ for some $a_1, \dots, a_m \in A$,*

$$m \leq \sup\{1, s_{T(p)} : p \text{ a prime of } A \text{ with } X_{T(p)} \neq \emptyset\}.$$

4. Complexity of basic closed sets

The result presented here is a general version of a result for real varieties proved first by Bröcker. Again, the proof is taken from [21].

We continue to assume that A is an arbitrary ring and $T \subseteq A$ is a proper preordering. Assume though that

$$d = \dim X_T := \sup\{\dim A/p : X_{T(p)} \neq \emptyset\} < \infty$$

and for $i = 0, \dots, d$ define

$$s_i := \sup\{1, s_{T(p)} : X_{T(p)} \neq \emptyset, \dim A/p \leq i\}.$$

Then we have the following:

Theorem 4.11. *If $\dim X_T = d < \infty$ and s_0, \dots, s_d are defined as above, then each basic closed set $S \subseteq X_T$ is expressible as $S = W_T(a_1, \dots, a_n), a_1, \dots, a_n \in A, n \leq s_0 + \dots + s_d$.*

For the proof we use the following:

Lemma 4.12. *Suppose $S \subseteq X_T$ is basic and clopen and suppose $\exists a_1, \dots, a_s \in A$ such that $S = U_T(a_1, \dots, a_s)$. Then $\exists b_1, \dots, b_s \in A$ (same s) such that $S = U_T(b_1, \dots, b_s) = W_T(b_1, \dots, b_s)$.*

Proof. By hypothesis and Corollary 1.22, $S = W_T(c_1, \dots, c_t)$ for some $c_1, \dots, c_t \in A$. Thus $S = X_{T_1}$ where $T_1 \supseteq T$ is the preordering generated by T and c_1, \dots, c_t . But $a_i > 0$ on S so, by the Positivstellensatz (Corollary 1.12), $a_i(1 + s_i) = 1 + t_i$ for some $s_i, t_i \in T_1$. Thus

$$b_i := -1 + 2a_i(1 + s_i)^2 = 1 + 2(s_i + t_i + s_i t_i)$$

satisfies $b_i > 0$ on S and $b_i < 0$ on $W(-a_i)$, $i = 1, \dots, s$. This means

$$S \subseteq U_T(b_1, \dots, b_s) \subseteq W_T(b_1, \dots, b_s) \subseteq U_T(a_1, \dots, a_s) = S,$$

so the proof is complete. \square

Proof of Theorem of 4.11 By induction on d . The boundary of S is $\partial S := S \cap \overline{X_T \setminus S}$. Let $I := \{a \in A : a = 0 \text{ on } \partial S\}$ so $\text{z-cl}(\partial S) = Z_T(I)$. By Corollary 1.17, $\dim Z_T(I) = \dim \partial S < \dim X_T = d$. On the other hand, $Z_T(I) = X_{\bar{T}}$ where $\bar{T} = T/I$ is the preordering in A/I generated by T . Thus, by induction on d ,

$$S \cap Z_T(I) = W_T(b_1, \dots, b_n) \cap Z_T(I)$$

for some $b_1, \dots, b_n \in A$, $n \leq s_0 + \dots + s_{d-1}$. By compactness, $\exists b \in I$ such that

$$S \cap Z_T(b) = W_T(b_1, \dots, b_n) \cap Z_T(b).$$

The point is, b vanishes on ∂S so $S \cap U_T(b^2)$ is clopen in $U_T(b^2)$. Thus, applying Lemma 4.12 to the ring $B = A[1/b]$ and the preordering $T[1/b^2] \subseteq B$ and using the Corollary 4.10, $\exists a_1, \dots, a_m \in A$, $m \leq s_d$ such that

$$S \cap U_T(b^2) = W_T(a_1, \dots, a_m) \cap U_T(b^2).$$

Now, $b_i \geq 0$ on $S \cap Z_T(b)$, so we can apply the Hörmander-Lojasiewicz inequality (specifically, Theorem 1.20) to obtain $c_i \in A$, $c_i \geq 0$ on S such that b_i, c_i have the same sign on $Z_T(b)$. Thus

$$S \doteq W_T(b^2 a_1, \dots, b^2 a_m, c_1, \dots, c_n).$$

Since $m + n \leq s_0 + \dots + s_d$, this completes the proof. \square

5. Bröcker's t -invariant

Let T be a proper preordering in a field F . X_T is compact so each constructible (=clopen) set $S \subseteq X_T$ is expressible as a finite union of basic clopen sets (Corollary 1.14(1)). It is easy to arrange things so the basic clopen sets appearing are pairwise disjoint: If $S = S_1 \cup \dots \cup S_m$ where $S_i = U(a_{i1}, \dots, a_{in})$, $a_{ij} \in F^*$, then X_T is the disjoint union of the basic clopen sets $\cap_{i,j} U(\varepsilon_{ij} a_{ij})$, $\varepsilon = (\varepsilon_{ij})$ running through all possible choices of ± 1 , and each S_i is a union of sets of this type.

Lemma 4.13. *If $s_T \leq 1$ then each clopen $S \subseteq X_T$ is basic.*

Proof. Write $S = S_1 \dot{\cup} \dots \dot{\cup} S_m$ (disjoint union) where each S_i is basic clopen, say $S_i = U(a_i)$. Then use $U(a) \dot{\cup} U(b) = U(-ab)$ to reduce the number of terms. \square

Lemma 4.14. *Suppose $S \subseteq X_T$ is clopen and $s = s_T \geq 1$. Then there exists a T -anisotropic form $\psi = \psi_s$ satisfying:*

$$\sigma(\psi) = \begin{cases} 2^s & \text{for } \sigma \in S \\ 0 & \text{for } \sigma \in X_T \setminus S. \end{cases}$$

Proof. Decompose S as $S = S_1 \dot{\cup} \dots \dot{\cup} S_m$ where S_i is basic, say $S_i = U(a_{i1}, \dots, a_{is})$, and take

$$\psi \sim_T \sum_{i=1}^m \langle \langle a_{i1}, \dots, a_{is} \rangle \rangle.$$

Taking $\dim(\psi)$ as small as possible, we can assume ψ is T -anisotropic (Theorem 3.2). \square

Remark.

- (1) If $S \neq \emptyset$, then $\dim(\psi) \geq 2^s$.
- (2) Actually, it is possible to show that $\dim(\psi) = 2^s$ iff S is basic.
- (3) Using this along with Theorem 3.7, one sees that S is basic in X_T iff $S \cap X_{\tilde{T}}$ is basic in $X_{\tilde{T}}$ for all preorderings $T \subseteq \tilde{T} \subseteq F$ with $(F^*/\tilde{T}^*) < \infty$. See [12] for more details and for other characterizations of basic sets in the field case.

Theorem 4.15. (Bröcker) Suppose $s = s_T \geq 1$ and $S \subseteq X_T$ is clopen. Then \exists a form ρ over F such that

$$(a) \quad \dim(\rho) \leq 4^{s-1} \quad (b) \quad \sigma(\rho) = \begin{cases} 2^{s-1} & \text{for } \sigma \in S \\ -2^{s-1} & \text{for } \sigma \in X_T \setminus S \end{cases}.$$

Proof. Take $\rho \sim_T \psi \oplus 2^{s-1} \times \langle -1 \rangle$, ψ as in Lemma 4.14. This satisfies (b). Taking $\dim(\rho)$ as small as possible, we can assume ρ is T -anisotropic (Theorem 3.2). It remains to show $\dim(\rho) \leq 4^{s-1}$. This is clear if $|\sigma(\rho)| = \dim(\rho)$ for some $\sigma \in X_T$. Thus, by Theorem 3.6, we can assume ρ is T^v -anisotropic for some T -compatible valuation v on F with $v(T^*) \neq v(F^*)$. Let $t = \dim_2 v(F^*)/v(T^*)$, so $t \geq 1$. Then $s_{T^*} + t \leq s_{T^*} \leq s_T = s$ (Corollary 4.6(2)), so $s_{T^*} \leq s - t < s$. Let $S^v = S \cap X_{T^*}$. The idea is to build a form ψ over F satisfying

$$(a) \quad \dim(\psi) \leq 4^{s-1} \quad (b) \quad \sigma(\psi) = \begin{cases} 2^{s-1} & \text{for } \sigma \in S^v \\ -2^{s-1} & \text{for } \sigma \in X_{T^*} \setminus S^v \end{cases}.$$

Then $\psi \sim_{T^*} \rho$ and, since ρ is T^v -anisotropic, $\dim(\rho) \leq \dim(\psi)$ by Theorem 3.2, and we are done.

Choose $z_1, \dots, z_t \in F^*/T^{v*}$ independent modulo F_v^*/T_v^* . Then

$$\begin{aligned} F^*/T^{v*} &= F_v^*/T_v^* \times \{1, z_1\} \times \dots \times \{1, z_t\} \quad \text{and} \\ X_{T^*} &= X_{T_v^*} \times \{1, \gamma_1\} \times \dots \times \{1, \gamma_t\} \end{aligned}$$

where $\gamma_1, \dots, \gamma_t$ is the dual basis to z_1, \dots, z_t . Let $\pi : X_{T^*} \rightarrow X_{T_v^*}$ denote the pushdown (restriction), $\pi(\sigma) = \bar{\sigma}$. For each choice of $\varepsilon = (\varepsilon_1, \dots, \varepsilon_t) \in \{\pm 1\}^t$, let

$$S_\varepsilon := \pi(S^v \cap U(\varepsilon_1 z_1, \dots, \varepsilon_t z_t))$$

so $S_\varepsilon \subseteq X_{T_v^*}$ is clopen. By induction on s we have a form $\bar{\rho}_\varepsilon$ over F_v such that

$$\dim(\bar{\rho}_\varepsilon) = 4^{s-t-1}, \quad \bar{\sigma}(\bar{\rho}_\varepsilon) = \begin{cases} 2^{s-t-1} & \text{for } \bar{\sigma} \in S_\varepsilon \\ -2^{s-t-1} & \text{for } \bar{\sigma} \in X_{T_v^*} \setminus S_\varepsilon \end{cases}.$$

Then $\psi := \sum_\varepsilon \bar{\rho}_\varepsilon \otimes \langle \varepsilon_1 z_1, \dots, \varepsilon_t z_t \rangle$ satisfies (a) and (b). This breaks down if $s = t$. In this case $s_{T^*} \leq s - t = 0$ so $|X_{T_v^*}| = 1$, $|X_{T^*}| = 2^t$. In this case, take

$$X' = X_{T_v^*} \times \{1, \gamma_1\}, \quad G' = \{1, -1\} \times \{1, z_1\}, \quad \pi' : X_{T^*} \rightarrow X' \text{ the projection,}$$

and take $\psi = \sum_\delta a_\delta \langle \delta_2 z_2, \dots, \delta_t z_t \rangle$ where $a_\delta \in G'$ is defined by

$$\pi'(S^v \cap U(\delta_2 z_2, \dots, \delta_t z_t)) = \{\sigma \in X' : \sigma(a_\delta) = 1\}.$$

□

Now define $\tau(s)$, $s \geq 1$ as follows: If $s \in \{1, 2\}$, define $\tau(s) = s$. If $s \geq 3$, define $\tau(s)$ to be the number of ways of choosing $(p(s) + 1)/2$ things from a set of $p(s)$ things, where $p(s) := 4^{s-1} - 2^{s-1} + 1$.

Corollary 4.16. *If $s = s_T \geq 1$, then each clopen set $S \subseteq X_T$ is expressible as a union of $\leq \tau(s)$ basic clopen sets.*

Proof. This is true by Lemma 4.13 if $s = 1$. If $s \geq 2$ then, by Theorem 4.15, we have a form $\rho = \langle a_1, \dots, a_m \rangle$, $m = 4^{s-1}$ with

$$\sigma(\rho) = \begin{cases} 2^{s-1} & \text{for } \sigma \in S \\ -2^{s-1} & \text{for } \sigma \in X_T \setminus S \end{cases}.$$

This means $\sigma \in S$ iff exactly $(p-1)/2$ of the a_i are negative at σ , and $\sigma \notin S$ iff exactly $(p-1)/2$ of the a_i are positive at σ , where $p = p(s)$. Thus we need only look at the first p entries of ρ : $\sigma \in S$ iff at least $(p+1)/2$ of the entries a_1, \dots, a_p are positive at σ . This proves the result if $s \geq 3$. If $s = 2$, then $\rho = \langle a_1, a_2, a_3, a_4 \rangle$, $\sigma(\rho) = 2$ if $\sigma \in S$, $\sigma(\rho) = -2$ if $\sigma \notin S$. In this case it is easy to check that $S = U(a_1, a_2) \dot{\cup} U(a_3, a_4)$. \square

The t -invariant is defined to be the least positive integer t such that each clopen set in X_T is expressible as a union of $\leq t$ basic clopen sets. Corollary 4.16 proves that $t \leq \tau(s)$ but this bound is probably not best possible for $s \geq 3$.

s	1	2	3	4
t	1	2	≤ 1716	$\leq 1.50336 \times 10^{16}$

Remark. Actually there is a much better bound for t if $|X_T| < \infty$ (namely $t \leq 2^{s-1}$) but the Isotropy Theorem is not strong enough to pull this back to the case of arbitrary X_T .

6. Complexity of arbitrary constructible sets

We return to the case where A is a ring and $T \subseteq A$ is a proper preordering.

Theorem 4.17. Assume that A is Noetherian and that $d := \dim X_T < \infty$. Then any constructible set in $S \subseteq X_T$ is expressible as a union of m basic sets $S = S_1 \cup \dots \cup S_m$, $m \leq \tau(s_0) + \dots + \tau(s_d)$ where s_0, \dots, s_d are defined as in Theorem 4.11.

Remark. Actually, we only need A/I Noetherian where $I = \cap \{\text{Supp}(P) : P \in X_T\}$. Also (as one sees from the proof) we can always choose the basic sets S_i of the special form $S_i = U(a_{i1}, \dots, a_{in_i}) \cap Z(b_i)$. Recall: basic sets of this type are a basis for the Tychonoff topology.

Proof. Let p_1, \dots, p_v be the primes in A lying over $I = \cap \{\text{Supp}(P) : P \in X_T\}$

with $\dim A/p_i = d$. By Corollary 4.16, we have $m \leq \tau(s_d)$ and elements $a_{ijk} \in A$, $i = 1, \dots, v$, $j = 1, \dots, s = s_d$, $k = 1, \dots, m$ such that

$$S(p_i) = \cup_{k=1}^m U_{T(p_i)}(a_{i1k}, \dots, a_{isk}), \quad i = 1, \dots, v.$$

Pick $x_i \in (\cap_{h \neq i} p_h) \setminus p_i$, $i = 1, \dots, v$, and define $a_{jk} = \sum_i x_i^2 a_{ijk}$ and let $S' = \cup_{k=1}^m U_T(a_{1k}, \dots, a_{sk})$. Thus

$$(*) \quad S(p_i) = S'(p_i), \quad i = 1, \dots, v.$$

Consider $S \triangle S' := (S \setminus S') \cup (S' \setminus S)$ and let $J := \cap \{\text{Supp}(P) : P \in S \triangle S'\}$. Thus $Z_T(J) = \text{z-cl}(S \triangle S')$. According to Corollary 1.15, the minimal primes lying over J have the form $p = \text{Supp}(P)$, $P \in S \triangle S'$ so by $(*)$, $\dim A/p < d$ for all such p . Thus $\dim A/J < d$ so by induction, we have $n \leq \tau(s_0) + \dots + \tau(s_{d-1})$ basic sets $S_1, \dots, S_n \subseteq X_T$ such that

$$S \cap Z(J) = \cup_{i=1}^n S_i \cap Z(J).$$

Choose $b \in A$ such that $Z(J) = Z(b)$. (J is finitely generated, so we can take $b = b_1^2 + \dots + b_w^2$ where b_1, \dots, b_w generate J). Thus

$$S \cap Z(b) = \cup_{i=1}^n S_i \cap Z(b).$$

Also, by definition of J and b ,

$$S \cap U(b^2) = S' \cap U(b^2) = \cup_{k=1}^m U(a_{1k}, \dots, a_{sk}) \cap U(b^2).$$

Since $S = (S \cap Z(b)) \cup (S \cap U(b^2))$, this completes the proof. \square

Modifying the construction just a bit, using the Hörmander-Lojasiewicz inequality, we obtain the following refinement:

Theorem 4.18. (Bröcker) *Set-up as in Theorem 4.17. Then each open constructible set in X_T is expressible as a union of m basic open sets, $m \leq \tau(s_0) + \dots + \tau(s_d)$.*

Proof. Begin exactly as in the proof of Theorem 4.17. Say $S_i = U(b_{1i}, \dots, b_{si})$. We modify b_{1i} so that $S_i \subseteq S$. Consider the closed constructible set

$W(b_{2i}, \dots, b_{si}) \setminus S$. Then $b_{1i} \leq 0$ on $(W(b_{2i}, \dots, b_{si}) \setminus S) \cap U(b_i^2) \cap Z(b)$ where $b_i := \prod_{j=2}^s b_{ji}$. Thus, by Theorem 1.20, $\exists c_i \leq 0$ on $W(b_{2i}, \dots, b_{si}) \setminus S$ such that b_{1i}, c_i have the same sign on $U(b_i^2) \cap Z(b)$. Then

$$S_i \cap Z(b) \subseteq U(c_i, b_{2i}, \dots, b_{si}) \subseteq S.$$

Thus, replacing S_i by $U(c_i, b_{2i}, \dots, b_{si})$, we have

$$S = \bigcup_{i=1}^n S_i \cup \bigcup_{k=1}^m U(a_{1k}, \dots, a_{sk}, b^2),$$

a union of $m + n \leq \tau(s_0) + \dots + \tau(s_d)$ basic open sets. \square

Remark.

- (1) Using Theorem 4.18 and taking complements, one also gets a bound for the number of basic closed sets required to describe a closed constructible, but this bound is *very* large.
- (2) It is not known if Theorems 4.17, 4.18 hold if the assumption that A is Noetherian is dropped. The method of Theorem 4.11 is not quite strong enough to handle this.

V APPLICATION TO REAL ALGEBRAIC GEOMETRY

1. Behaviour of stability under field extension

To get the desired application to semi-algebraic sets we need to consider the following set-up: let $P \subseteq F$ be a preordering (F a field). We are interested in the case where P is an *ordering*, but there is no need to assume this to begin with. Let $K \supseteq F$ be an extension field, and consider the preordering $T := \sum K^2 P \subseteq K$. Assume T is proper. Define

$$\bar{s}_P := \sup\{\dim_2 v(F^*)/2v(F^*) : v \text{ is a } P\text{-compatible valuation on } F\}.$$

Example. If P is an ordering, then $\bar{s}_P = \dim_2 v_P(F^*)/2v_P(F^*)$ where v_P is the unique finest valuation on F compatible with P ; see Theorem 1.7.

We use Corollary 4.7 to prove the following estimate for s_T :

Theorem 5.1. *Set-up as above. Then*

$$s_T \leq \text{trdeg}(K : F) + \bar{s}_P + \delta_P$$

where $\delta_P \in \{0, 1\}$ is defined as follows: $\delta_P = 0$ iff for all P -compatible valuations v on F with $\dim_2 v(F^*)/2v(F^*) = \bar{s}_P$, $|X_{P_v}| = 1$ and moreover, if the unique ordering in X_{P_v} extends to some algebraic extension of F_v , then it extends uniquely. Otherwise $\delta_P = 1$.

We use two Lemmas in the proof:

Lemma 5.2 *Suppose v is a valuation on K and w is the restriction of v to F . Suppose $a_1, \dots, a_m \in K^*$ are such that $v(a_1), \dots, v(a_m)$ are \mathbb{Z} -independent modulo $w(F^*)$ and $b_1, \dots, b_n \in B_v^*$ are such that $\bar{b}_1, \dots, \bar{b}_n \in K_v^*$ are algebraically independent over F_w . Then $a_1, \dots, a_m, b_1, \dots, b_n$ are algebraically independent over F .*

Proof. This is a standard exercise in valuation theory. \square

Lemma 5.3 *Suppose $U \subseteq W$ are torsion free abelian groups and W/U is 2-primary torsion and $\dim_2 U/2U < \infty$. Then $\dim_2 W/2W \leq \dim_2 U/2U$ (with equality if $|W/U| < \infty$).*

Proof. If $\alpha_1, \dots, \alpha_n \in W$ are \mathbb{Z}_2 -independent modulo $2W$, then $\alpha_1, \dots, \alpha_n$ are also \mathbb{Z}_2 -independent modulo $2W'$ where $W' \subseteq W$ is the subgroup generated by $\alpha_1, \dots, \alpha_n$ and U . Thus, replacing W by W' , we are reduced to the case where W/U is finite. By induction, we can even assume $|W/U| = 2$. But in this case $W \supseteq U \supseteq 2W \supseteq 2U$ and $W/U \cong 2W/2U$ (via $\alpha + U \mapsto 2\alpha + 2U$) so the result is clear. \square

Proof of Theorem 5.1 (See [6, 22].) We can assume $\text{trdeg}(K : F) + \bar{s}_P + \delta_P <$

∞ . Let v be any T -compatible valuation on K and let w denote the restriction of v to F . Since v is T -compatible, Lemma 3.4 implies

$$v\left(\sum_{i=1}^n b_i^2 t_i\right) = \min \{v(b_i^2 t_i) : i = 1, \dots, n\}, \quad \text{for } b_i \in K^*, t_i \in P^*.$$

Thus $v(T^*) = v(K^{*2}P^*) = 2v(K^*) + w(P^*)$. Define

$$W = \{\alpha \in v(K^*) : 2^r \alpha \in w(F^*) \text{ for some integer } r \geq 0\}.$$

Thus

$$\begin{aligned} \dim_2 v(K^*)/v(T^*) &= \dim_2 v(K^*)/(2v(K^*) + w(P^*)) \\ &= \dim_2 v(K^*)/(2v(K^*) + W) + \dim_2 (2v(K^*) + W)/(2v(K^*) + w(P^*)). \end{aligned} \quad (1)$$

If $a_i \in K^*$, $n_i \in \mathbb{Z}$ not all zero are such that $\sum n_i v(a_i) \in w(F^*)$ then, dividing by the highest power of 2 common to the n_i we have $\sum m_i v(a_i) \in W$ where $m_i \in \mathbb{Z}$ and at least one of the m_i is odd. This shows that $\dim_{\mathbb{Z}} v(K^*)/w(F^*) \geq \dim_2 v(K^*)/(2v(K^*) + W)$ and hence, using Lemma 5.2, that

$$\begin{aligned} \text{trdeg}(K : F) &\geq \dim_{\mathbb{Z}} v(K^*)/w(F^*) + \text{trdeg}(K_v : F_w) \\ &\geq \dim_2 v(K^*)/(2v(K^*) + W) + \text{trdeg}(K_v : F_w). \end{aligned} \quad (2)$$

Also, $(2v(K^*) + W)/(2v(K^*) + w(P^*)) \cong W/(2W + w(P^*))$ so, using Lemma 5.3,

$$\begin{aligned} \dim_2 (2v(K^*) + W)/(2v(K^*) + w(P^*)) &= \dim_2 W/(2W + w(P^*)) \\ &\leq \dim_2 W/2W \leq \dim_2 w(F^*)/2w(F^*). \end{aligned} \quad (3)$$

Putting (1), (2), (3) together, we obtain

$$\dim_2 v(K^*)/v(T^*) \leq \text{trdeg}(K : F) + \dim_2 w(F^*)/2w(F^*). \quad (4)$$

Thus we see that s_T is finite (using (4) and Corollary 4.7). Now, using Corollary 4.7, choose v so that $\dim_2 v(K^*)/v(T^*) = \bar{s}_T$, $|X_{T_v}| > 1$ if $\varepsilon_T = 1$. Thus $s_T = \dim_2 \frac{v(K^*)}{v(T^*)} + \varepsilon_T$ so we are done by (4) except possibly if $\varepsilon_T = 1$ and we have equality in (4) and $\dim w(F^*)/2w(F^*) = \bar{s}_P$. It remains to show that $\delta_P = 1$ in this case. But this is pretty clear. Since we have equality in (4) we

must also have $\text{trdeg}(K_v : F_w) = 0$ in (2) so K_v is an algebraic extension of F_w with at least two orderings extending orderings in X_{P_w} (namely, the orderings in X_{T_v}), so $\delta_P = 1$. \square

2. Application to finitely generated algebras

Suppose now that A is any finitely generated F -algebra. Thus

$$A \cong F[X_1, \dots, X_N]/I \text{ for some } N \geq 0 \text{ and some ideal } I \subseteq F[X_1, \dots, X_N]$$

and, by the Hilbert basis theorem, $I = (h_1, \dots, h_k)$ for some finite set of polynomials h_1, \dots, h_k . Let $P \subseteq F$ be a preordering and let $T := \sum A^2 P \subseteq A$. If $p \subseteq A$ is a prime, then $F(p)$ is a finitely generated field extension of F and $\text{trdeg}(F(p) : F) = \dim A/p$ by Theorem 2.7. Also, $T(p) = \sum F(p)^2 P$ so we have the estimate for $s_{T(p)}$ given in Theorem 5.1.

Theorem 5.4. *Set-up as above, if $d := \dim X_T$, then*

- (1) *Each basic open set $S \subseteq X_T$ is expressible as $S = U(a_1, \dots, a_m)$, $a_1, \dots, a_m \in A$, $m \leq \max\{1, d + \bar{s}_P + \delta_P\}$.*
- (2) *Each basic closed set $S \subseteq X_T$ is expressible as $S = W(a_1, \dots, a_n)$, $a_1, \dots, a_n \in A$, $n \leq \max\{1, d(d+1)/2 + (d+1)(\bar{s}_P + \delta_P)\}$.*
- (3) *Each constructible set in X_T is expressible as a union of p basic sets, $p \leq \sum_{i=0}^d \tau(i + \bar{s}_P + \delta_P)$.*
- (4) *Each open constructible set in X_T is expressible as a union of p basic open sets, $p \leq \max\{1, \sum_{i=0}^d \tau(i + \bar{s}_P + \delta_P)\}$.*

(Here, τ is the function defined in part IV. $\tau(0) := 1$ in (3), $\tau(0) := 0$ in (4).)

Proof. (See [22].) If $p \subseteq A$, $X_{T(p)} \neq \emptyset$, $\dim A/p \leq i$, then, by Theorem 5.1,

$$s_{T(p)} \leq \text{trdeg}(F(p) : F) + \bar{s}_P + \delta_P = \dim A/p + \bar{s}_P + \delta_P \leq i + \bar{s}_P + \delta_P.$$

Thus (almost) everything follows from Corollary 4.10 and Theorems 4.11, 4.17, 4.18. Note, in regard to (2), that $\sum_{i=0}^d (i + \bar{s}_P + \delta_P) = d(d+1)/2 + (d+1)(\bar{s}_P + \delta_P)$. Unfortunately, $s_0 \geq 1$ by definition, so there is a problem with (2) and (4) when $\bar{s}_P + \delta_P = 0$. To fix this, since Theorems 4.11 and 4.18 are proved by induction on d , it suffices to handle the case $d \leq 1$. In this case, we have the following result.

Lemma 5.5. *Set-up as in 5.4 but suppose $d \leq 1$ and $\bar{s}_P + \delta_P = 0$. Then each open constructible $S \subseteq X_T$ has the form $S = U(a)$. (Equivalently, each closed constructible $S \subseteq X_T$ has the form $S = W(a)$.)*

Proof. Suppose $S \subseteq X_T$ is open and constructible. For any prime $p \subseteq A$ with $X_{T(p)} \neq \emptyset$, $s_{T(p)} \leq \dim A/p \in \{0, 1\}$, so $S(p) = U_{T(p)}(b)$ by Lemma 4.13. Thus, we can conclude $S = U(a)$ by Theorem 4.8 as soon as we establish that S is basic open. According to Theorem 1.24, to do this, we need only establish that $S \cap \text{z-cl}(\partial S) = \emptyset$. But $\dim \partial S < \dim X_T \leq 1$ by Corollary 1.17 and consequently $\text{z-cl}(\partial S) = \partial S$ so this is clear. (Use the fact that $|X_{T(p)}| = 1$ if $\dim A/p = 0$.) \square

Finally, we apply Theorem 5.4 to the geometric set-up considered in Part II. i.e., we take $P \subseteq F$ to be an ordering, R a real closed extension of (F, P) , and

$$V = \{x \in R^N : h_i(x) = 0, i = 1, \dots, k\}.$$

Then, combining various results proved so far, we have proved the following:

Theorem 5.6. *Suppose $d = \dim V$. Then*

- (1) *Each basic open set in V is describable by m inequalities $f_i(x) > 0$, $f_1, \dots, f_m \in A$, $m \leq \max\{1, d + \bar{s}_P + \delta_P\}$.*
- (2) *Each basic closed set in V is describable by n inequalities $f_i(x) \geq 0$, $f_1, \dots, f_n \in A$, $n \leq \max\{1, d(d+1)/2 + (d+1)(\bar{s}_P + \delta_P)\}$.*
- (3) *Each semi-algebraic set in V is expressible as the union of p basic sets,*

$$p \leq \sum_{i=0}^d \tau(i + \bar{s}_P + \delta_P).$$

- (4) Each open semi-algebraic set in V is expressible as a union of p basic open sets, $p \leq \max\{1, \sum_{i=0}^d \tau(i + \bar{s}_P + \delta_P)\}$.

(Here, τ is the function defined in Part IV. $\tau(0) := 1$ in (3), $\tau(0) := 0$ in (4)).

Proof. This is immediate from Theorem 5.4, using Theorems 2.1, 2.4, and 2.8. \square

If (F, P) is real closed, we obtain from Theorem 5.6 the classical bounds obtained by Bröcker and Scheiderer [12, 20, 24] as a consequence of:

Lemma 5.7 Suppose (F, P) is real closed. Then $\bar{s}_P = 0 = \delta_P$.

Proof. See Lemma 1.9. \square

For another case where the bounds in Theorem 5.6 are small, note the following:

Lemma 5.8 If (F, P) is Archimedean, then the only P -compatible valuation on F is the trivial valuation (so $\bar{s}_P = 0$).

Proof. The unique finest valuation on F compatible with P is trivial. \square

Remark:

- (1) If (F, P) is real closed (so $\bar{s}_P + \delta_P = 0$), then the bounds in Theorem 5.6 (1), (2) are best possible: i.e., there do exist basic open sets (resp; basic closed sets) in V requiring d (resp; $d(d+1)/2$) inequalities [12, 24].
- (2) If (F, P) is not real closed, the bounds in Theorem 5.6 (1), (2) are still best possible if $V = R^N$, i.e., if A is the polynomial algebra $F[X_1, \dots, X_N]$ [22] (and $d = N$ in this case).

References

- [1] Andradas, C. ; Bröcker, L.; Ruiz, J. , *Minimal generation of basic open semi-analytic sets*, Invent. Math. 92, (1988), 409–430.
- [2] Atiyah, M.; MacDonald, I., *Introduction to commutative algebra*, Addison-Wesley, (1969).
- [3] Becker, E., *On the real spectrum of a ring and its applications to semi-algebraic geometry*, Bull. Amer. Math. Soc. 15, (1986), 19–60.
- [4] Becker, E.; Bröcker, L., *On the description of the reduced Witt ring*, J. Algebra 52, (1978), 328–346.
- [5] Bochnak, J.; Coste, M.; Roy, M.- F. *Géométrie Algébrique Réelle*, Ergeb Math., Springer, Berlin, Heidelberg, New York, (1987).
- [6] Bröcker, L., *Zur Theorie der quadratischen Formen über formal reellen Körpern*, Math. Ann. 210, (1974), 233–256.
- [7] Bröcker, L., *Positivbereiche in kommutativen Ringen*, Abh. Math. Sem. Univ. Hamb. 52, (1982), 170–178.
- [8] Bröcker, L., *Minimale Erzeugung von Positivbereichen*, Geom. Dedicata 16, (1984), 335–350.
- [9] Bröcker, L., *Spaces of orderings and semi-algebraic sets*, in Quadratic and Hermitian Forms, Can. Math. Soc. Conf. Proc. Vol 4, (1984). 231–248.
- [10] Bröcker, L., *Description of semi-algebraic sets by few polynomials*, Lecture at CIMPA Nice, (1985).
- [11] Bröcker, L., *On separation of basic semi-algebraic sets by polynomials*, Manuscripta Math. 60, (1988), 497–508.
- [12] Bröcker, L., *On basic semi-algebraic sets*, Expositiones Math. Vol. 9 (1991), 289–334.

- [13] Bröcker, L., *On the stability index of Noetherian rings*, in Real analytic and algebraic geometry, Springer Verlag, Lecture Notes 1420, (1990), 72–80.
- [14] Brumfiel, G., *Partial ordered rings and semi-algebraic geometry*, Cambridge University Press (1979).
- [15] Kelly, J., *General Topology*, Van Nostrand, (1955).
- [16] Knebusch, M.; Scheiderer, C., *Einführung in die reelle Algebra*, Braunschweig/Wiesbaden, Vieweg, (1989).
- [17] Lam, T.Y., *Orderings, valuations, and quadratic forms*, Regional Conf. Series in Math. 52, AMS, (1983).
- [18] Lam, T. M., *An introduction to real algebra*, Rocky Mtn. J. Math. 14, (1984), 767–814.
- [19] Lang, S., *Algebra*, Addison-Wesley, (1965).
- [20] Mahé, L., *Une démonstration élémentaire du théorème de Bröcker-Scheiderer*, C. R. Acad. Sci. Paris 309 Serie I, (1989), 613–616.
- [21] Marshall, M., *Minimal generation of basic sets in the real spectrum of a commutative ring*, in Contemporary Math., to appear.
- [22] Marshall, M.; Walter, L., *Minimal generation of basic semi-algebraic sets over an arbitrary ordered field*, in Real algebraic geometry proceedings, Rennes, Springer-Verlag, Lecture Notes 1524, (1991), 346–353.
- [23] Prestel, A., *Lectures on formally real fields*, Springer Lecture Notes 1093, (1984).
- [24] Scheiderer, C., *Stability index of real varieties*, Invent. Math. 97, (1989), 467–483.

Department of Mathematics & Statistics
University of Saskatchewan
Saskatoon, SK, Canada, S7N 0W0