Elementary constructive theory of ordered fields

HENRI LOMBARDI MARIE-FRANÇOISE ROY

1. Introduction

The classical theory of ordered fields (Artin-Schreier theory) makes intensive use of non-constructive methods, in particular of the axiom of choice. However since Tarski (and even since Sturm and Sylvester) one knows how to compute in the real closure of an ordered field **K** solely by computations in **K**. This apparent contradiction is solved in this paper.

We give here a constructive proof of the first results of the theory of ordered fields, including the existence of the real closure.

The proofs can be interpreted in the particular philosophy of each reader. In a classical point of view for example, the effective procedures in the definitions may be interpreted as given by oracles. Hence one gets the existence of the real closure of an arbitrary ordered field without the axiom of choice. In a constructive framework "à la Bishop" one gets the existence of the real closure of a discrete ordered field. The reference for discrete fields is [**MRR**]. From the point of view of classical recursive theory the proofs give uniformly primitive recursive algorithms for Turing machines with oracles (cf [**Kl**]).

The essential tools needed are the following: a constructive version of the mean value theorem in an ordered field, the notions of prime cone (see [**BCR**]) and of ordered d-closed field.

The use of algorithm IF from [**CR**] gives a concrete representation for elements of the real closure, with no need of primitive elements.

Through the paper "A real root calculus" of Zassenhauss ([**Za**]), we discovered recently Holkott 's thesis [**Ho**]. Holkott's method and ideas are, sometimes surprisingly, very similar to ours. Our paper can be considered as a modern and, we hope, clearer presentation of Holkott's results. Thanks to L. Gonzalez for communicating the reference [**Za**] and to T. Sander for translating to us decisive parts of [**Ho**].

Tomas Sander also studied recently and independently the existence of the real closure without the axiom of choice ([**Sa**]).

2. Preliminaries

Ordered fields.

Definition 1: A set is *discrete* when the equality of two elements is decidable. A *discrete field* is a field $\mathbf{K}$, discrete as a set and in which the laws of addition, multiplication, opposite and inverse are computable. A discrete ordered field $\mathbf{K}$ is a discrete field where the sign of an element is decidable. From now on, all fields and ordered fields considered are assumed to be discrete.

Remark 1: An ordered field with an oracle giving results of arithmetic operations and sign of elements is a discrete ordered field. A codable ordered field where elements are represented by a finite data structure and where arithmetic operations and sign determinations are given by algorithms is a discrete ordered field.

Let $\mathbf{K}$ be an ordered field. An open interval is by definition a set

$$]a, b[= \{x \in \mathbf{K} \mid a < x < b\}$$

where a and b are in $\mathbf{K}$ or equal to $+\infty$ or $-\infty$.

Theorem 1 (constructive mean value theorem). *Let $\mathbf{K}$ be an ordered field, a and b two elements of $\mathbf{K}$ with $a < b$.*

There exist two families $(\lambda_{n,i})_{n\in\mathbf{N},i=1,2,\dots,n}$ and $(r_{n,i})_{n\in\mathbf{N},i=1,2,\dots,n}$ of rational numbers in $]0,1[$ such that, for every polynomial P of $\mathbf{K}[X]$ of degree $\leq n$, the following equality holds:

$$P(a) - P(b) = (a-b) \sum_{i=1,\dots,n} r_{n,i}.P'(a + \lambda_{n,i}(b-a)).$$

In particular

1) if P' is positive on an interval, P is increasing on this interval,

2) on every bounded interval the function defined by P is Lipschitz.

Proof: The theorem is an immediate consequence of the following lemma:

Lemma. *There exist two families $(\lambda_{n,i})_{i=1,2,\dots,n}$ and $(r_{n,i})_{i=1,2,\dots,n}$ of rational numbers in $]0,1[$ such that, for every polynomial P in $[X]$ of degree $\leq n$, the following equality holds:*

$$P(a) - P(b) = (a-b) \sum_{i=1,\dots,n} r_{n,i}.P'(a + \lambda_{n,i}(b-a)).$$

The lemma gives algebraic identities about variables a, b, and the coefficients of the polynomial which are valid in any commutative ring which is a -algebra, and in particular in fields of characteristic zero.

Let us prove the lemma. Using an affine change of coordinates one may suppose $a = -1$ and $b = 1$. Let the degree n be fixed. The function sending P to $P(1) - P(-1)$ is a linear form where the constant coefficient plays no role. Such linear forms constitue a vector space of dimension n. For every choice of n different rational numbers $(\lambda_{n,i})_{i=1,\dots,n}$, the linear forms sending P to $P'(\lambda_{n,i})$ are independent in this space. So to this choice corresponds rational numbers $r_{n,i}$ making the formula true. The only difficult point is to choose $\lambda_{n,i}$ in $]0,1[$ such that the corresponding $r_{n,i}$ are still in $]0,1[$. Gauss formulas (where one has to consider zeroes of Legendre polynomials, cf. [**L**]) correspond to such a choice, but with real numbers and not rational numbers. A choice of $\lambda_{n,i}$ rational numbers close enough to the $\lambda_{n,i}$ of Gauss ensures that the corresponding $r_{n,i}$ are still positive.

Remark 2: Explicit upper and lower bounds for P' are easy to compute on a bounded interval, hence a Lipschitz modulus for P.

Definition 2: A *sign condition* is a member of $\{> 0, = 0, < 0\}$. A *generalized sign condition* is a member of $\{< 0, \leq 0, = 0, > 0, \geq 0\}$. When a sign condition < 0 or > 0 is replaced by the corresponding generalized sign condition ≤ 0 or ≥ 0, the sign condition is said to have been *relaxed*.

A subset of an ordered field is *open* if it is a union of open intervals. A function from **K** to **K** is *continuous* if the inverse image of an open set is open.

Lemma. *A polynomial function from an ordered field into itself is continuous.*

2. Prime cones

Definitions 3 (see [**BCR**]:

a) A *prime cone* of a ring **A** is a subset α such that

1) $\forall x \in A, x^2 \in \alpha$,
2) $\alpha + \alpha \subset \alpha$,
3) $\alpha.\alpha \subset \alpha$,
4) $\forall x \in \mathbf{A}, \forall y \in \mathbf{A}, xy \in \alpha \Rightarrow x \in \alpha$ or $-y \in \alpha$.

b) The *support* of α, $\mathrm{Supp}(\alpha) = \alpha \cap -\alpha$, is a prime ideal whose residue field $k(\mathrm{Supp}(\alpha))$ is ordered: positive or zero elements of $k(\mathrm{Supp}(\alpha))$ are images of elements of α.

c) Let **K** be an ordered field and **A** a **K**-algebra. The prime cone α is *compatible with the order of* **K** if moreover

5) $\alpha \cap \mathbf{K} = \{x \in \mathbf{K} \mid x \geq 0\}$.

The field $k(\mathrm{Supp}(\alpha))$ is then an ordered extension of **K**. Let **L** be an ordered extension of **K** and f a ring homomorphism of **A** in **L**. **L** is an ordered extension of $k(\mathrm{Supp}(\alpha))$ if and only if $\{x \in \mathbf{A} \mid f(x) \geq 0 \text{ in } \mathbf{L}\} = \alpha$.

d) When $k(\mathrm{Supp}(\alpha))$ is an algebraic extension of $\mathbf{K}$, α is *algebraic over* $\mathbf{K}$.

e) Let us denote by α_0, α_+ and α_- the subsets of $\mathbf{A}$ of elements whose images in $k(\mathrm{Supp}(\alpha)$ are 0, $+1$ and -1. Then $\alpha_0 = \mathrm{Supp}(\alpha)$ and $\alpha = \alpha_0 \cup \alpha_+$.

Axioms 1), 2), 3) and 4) can be rewritten as

1') $\mathbf{A}$ is the disjoint union of α_0, α_+ and α_-, and $\alpha_- = -\alpha_+$,

2'a) $\alpha_0 + \alpha \subset \alpha$,

2'b) $\alpha_+ + \alpha_+ \subset \alpha_+$,

3'a) $\alpha_0.\alpha \subset \alpha_0$,

3'b) $\alpha_+.\alpha_+ \subset \alpha_+$.

f) When $\mathbf{A} = \mathbf{K}[X]$ one writes X_α for the image of X in $k(\mathrm{Supp}(\alpha))$. When moreover α is algebraic over $\mathbf{K}$ one writes $\mathbf{K}[X_\alpha]$ for the ordered field $k(\mathrm{Supp}(\alpha))$.

3. d-closed ordered fields

3.1. Definitions.

Definition 4: A field is *real* if -1 is not a sum of squares.

An ordered field is *d-closed* (where $d \geq 1$) if every polynomial P of degree $\leq d$ such that $P(a)P(b) < 0$ has a root on the interval $]a, b[$.

In the classical situation, this definition is equivalent to the definition of d-real closed field in [**B**].

Remark 3: Every ordered field is real and 1-closed. Every real field is of characteristic zero.

Comment: In the classical theory, using Zorn's lemma it is possible to prove that any real field can be ordered. This is no longer true from a constructive point of view. More concretely it is impossible to prove constructively that in a real field it is possible to add a real square root to a or to $-a$ and get a real extension: it would be necessary to assert that a or $-a$ is not a sum of squares. This would clearly imply the "lesser limited principle of omniscience" (LLPO) which is not constructively valid (cf [**MRR**], Chapter 1). An example of recursive real field not recursively orderable appears in [**MN**].

3.2. Construction of the 2-closure of an ordered field.

Definition 5: An ordered extension $\mathbf{R}$ of an ordered field $\mathbf{K}$ is an *ordered 2-closure* of $\mathbf{K}$ if it is a 2-closed ordered field and if every element of $\mathbf{R}$ is obtained starting from elements of $\mathbf{K}$ by repetition of arithmetic operations and extraction of the real square root of a positive element.

The next proposition is training for the proof of the existence of the real closure that will be proved later along the same lines.

Proposition 1. *Every ordered field* $\mathbf{K}$ *has an ordered 2-closure, unique up to (unique)* $\mathbf{K}$*-isomorphism of ordered fields.*

Proof: If a is a positive element of $\mathbf{K}$, it is easy to see that there exists an ordered extension $\mathbf{K}$ obtained by adding a positive real square root of a: without taking into consideration the fact that $\mathbf{K}$ might or might not have had such a positive real root, one may give without ambiguity a sign to each expression $x+y\sqrt{a}$, where x and y are in $\mathbf{K}$, hence also to every expression $Q(\sqrt{a})$ where $Q \in \mathbf{K}[X]$, by considering the remainder of the division of $Q(X)$ by X^2-a; this defines a prime cone of $\mathbf{K}[X]$, the corresponding residue field is denoted by $\mathbf{K}[\sqrt{a}]$.

If $\mathbf{L}$ is an ordered extension of $\mathbf{K}$ in which a has a positive square root a', there exists a unique $\mathbf{K}$-isomorphism of ordered fields from $\mathbf{K}[\sqrt{a}]$ to $\mathbf{K}[a']$ (the subfield of $\mathbf{L}$ generated by $\mathbf{K}$ and a').

This implies the following lemma:

Lemma. *Let a and b be two positive elements of an ordered field* $\mathbf{K}$*. The ordered fields* $\mathbf{K}[\sqrt{a}][\sqrt{b}]$ *and* $\mathbf{K}[\sqrt{b}][\sqrt{a}]$ *are isomorphic as ordered extensions of* $\mathbf{K}$*.*

Let us consider now the union of all $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]\cdots[\sqrt{a_i}]$ with a_j, $(j=1,\dots,i)$ positive in $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]\cdots[\sqrt{a_{j-1}}]$. The ordered 2-closure we look for, will be the quotient of this union by an equivalence relation.

Let us define this equivalence relation. Let

$$\mathbf{K}_1 = \mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]\cdots[\sqrt{a_i}]$$

with $a_j (j=1,\dots,i)$ positive in $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]\cdots[\sqrt{a_{j-1}}]$ and

$$\mathbf{K}_2 = \mathbf{K}[\sqrt{b_1}][\sqrt{b_2}]\cdots[\sqrt{b_{i'}}]$$

with $b_j (j=1,\dots,i')$ positive in $\mathbf{K}[\sqrt{b_1}][\sqrt{b_2}]\cdots[\sqrt{b_{j-1}}]$. Let us define

$$\mathbf{K}' = \mathbf{K}_1[\sqrt{b_1}][\sqrt{b_2}]\cdots[\sqrt{b_{i'}}].$$

Using several times the lemma one has a unique $\mathbf{K}$-isomorphism from $\mathbf{K}'$ to

$$\mathbf{K}'' = \mathbf{K}_2[\sqrt{a_1}][\sqrt{a_2}]\cdots[\sqrt{a_i}].$$

By definition, elements of $\mathbf{K}_1$ and $\mathbf{K}_2$ are equivalent if their images in $\mathbf{K}'$ and $\mathbf{K}''$ coincide up to the isomorphism. This defines an equivalence relation compatible with the ordered field structure: reflexivity and symmetry are immediate. Transitivity involves three extensions. The ordered 2-closure is then the quotient of the union of $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]\cdots[\sqrt{a_i}]$ (with a_j, $(j=1,\dots,i)$ positive in $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]\cdots[\sqrt{a_{j-1}}]$) by this equivalence relation.

3.3. Sign conditions.

Definition 6: Let $L = [P_1, P_2, \ldots, P_k]$ be a list of polynomials of $\mathbf{K}[X]$ of degrees less than or equal to d, where $\mathbf{K}$ is a subfield of a d-closed field $\mathbf{R}$. The complete list of signs of the list L is known when the roots of P_i in $\mathbf{R}$ have been computed, they are in increasing order, and the sign of each of the polynomials in each of these roots and on each interval between these roots is computed.

Theorem 2. *Let* $\mathbf{K}$ *be an ordered field, subfield of a* d*-closed ordered field* $\mathbf{R}$*. Let*

$$L = [P_1, P_2, \ldots, P_k]$$

be a list of polynomials of $\mathbf{K}[X]$ *of degrees less than or equal to* d*. It is possible to compute the complete list of signs of* L*.*

Proof: Because of theorem 1 and of the intermediate value theorem for polynomials of degree less than or equal to d, we have all the tools needed to apply Hörmander's method to L (cf. [**BCR**] Chapter 1).

Comment: For a constructivist this theorem has the following provoking corollary: *in a* d*-closed ordered field, the roots of a polynomial of degree* $\leq d$ *form a finite set.*

Theorem 3 (Thom's lemma). *Let* $\mathbf{K}$ *be an ordered field contained in a* d*-closed ordered field* $\mathbf{R}$*,* P *be a polynomial of* $\mathbf{K}[X]$*, of degree* $n \leq d$*, and* $[\sigma_0, \sigma_1, \ldots, \sigma_n]$ *be a list of sign conditions other than* $= 0$*. The set*

$$A_\sigma = \{x \in \mathbf{R} \mid P(x)\sigma_0, P'(x)\sigma_1, \ldots, P^{(i)}(x)\sigma_i, \ldots, P^{(n-1)}(x)\sigma_{n-1}\}$$

is either empty, or an open interval with endpoints $+\infty$*,* $-\infty$*, or a root of one of the polynomials* $P, P', P'', \ldots$*. If the sign conditions are relaxed, and if the open* A_σ *were a non empty interval, one gets the corresponding closed interval. If now the first condition is* $= 0$*, the set has zero or one point.*

Proof: One can perform the usual proof by induction on the degree of P (cf. [**BCR**]).

3.4. Sturm's algorithm.

Definition 6: Let $\mathbf{K}$ be an ordered field. Let P and Q be two polynomials with coefficients in $\mathbf{K}$ and R be the remainder of the euclidean division of $P'Q$ by P. Let a and b be two elements of $\mathbf{K}$ with $a < b$ (or possibly $a = -\infty$, $b = +\infty$), a and b not being roots of P.

The Sturm sequence of P and Q is defined by

$\mathrm{Stu}_0(P, Q) = P$
$\mathrm{Stu}_1(P, Q) = R$
$\mathrm{Stu}_{i+1}(P, Q) = -$ Remainder$(\mathrm{Stu}_i(P, Q), \mathrm{Stu}_{i-1}(P, Q))$
The Sturm sequence of P is obtained when $Q = 1$.

One denotes by $v_{\mathrm{St}}(P, Q, a, b)$ the difference between the number of sign variations in the Sturm sequence at a and at b.

Theorem 4 (Sturm-Sylvester in degree $\leq d$ in a d-closed ordered field). *Let* $\mathbf{K}$ *be an ordered field, subfield of a d-closed ordered field* $\mathbf{R}$. *Let P and Q be two polynomials with coefficients in* $\mathbf{K}$ *with P of degree less than or equal to d. Using the preceding notations, the number $v_{\mathrm{St}}(P, Q, a, b)$ is equal to the difference between the number of roots of P between a and b with $Q > 0$ and the number of roots of P between a and b with $Q < 0$.*

Proof: The classical proof (see for example [**GLRR**]) works because of theorem 2.

Remark 4: There are examples of ordered fields with polynomials P of constant sign on an interval, but with the number of roots predicted by Sturm non zero: add to an infinitely small positive element ϵ, and consider the polynomial $P = (X^2 - \epsilon^3).(X^3 - \epsilon^4)$ and the interval $[\epsilon^2, \epsilon]$.

Proposition 2 (polynomial of degree $d+1$ in an ordered d-closed field). *Let P be a polynomial of degree $d + 1$ in an ordered d-closed field* $\mathbf{K}$ *and let $]a, b[$ $(a < b)$ be an interval of the field* $\mathbf{K}$ *such that P is not* 0 *at a and at b. If P is square free $v_{\mathrm{St}}(P, 1, a, b)$ gives the number of sign changes of P on $]a, b[$. In particular $v_{\mathrm{St}}(P, 1, a, b)$ is always positive or zero and the number of roots of P in* $\mathbf{K}$ *over $]a, b[$ is less than or equal to $v_{\mathrm{St}}(P, 1, a, b)$. If P is reducible in* $\mathbf{K}[X]$ *(in particular if it is not square-free) $v_{\mathrm{St}}(P, 1, a, b)$ is equal to the number of roots of P in* $\mathbf{K}$ *over $]a, b[$.*

Proof: When P is square-free, consider the roots of all polynomials in the Sturm-sequence except P in $\mathbf{K}$ and repeat the usual proof. When P is reducible in $\mathbf{K}[X]$ repeat the usual proof (see for example [**GLRR**]).

3.5. Algorithm IF.

Algorithm IF ("inégalités formelles") proposed in [**CR**] (on the basis of [**BKR**]) in order to determine, by computations in $\mathbf{K}$ (only arithmetic operations and sign determinations) the signs of a list of polynomials at the roots of a polynomial of degree less than or equal to d may be applied in any ordered field $\mathbf{K}$ with d-closed ordered extension $\mathbf{R}$ because of preceding theorems.

Algorithm IF, applied to P (of degree less than or equal to d) and its derivatives, is called RAN (Real Algebraic Number) and works in any ordered field $\mathbf{K}$ with d-closed ordered extension $\mathbf{R}$: that is to say that, to every sign condition on the derivatives predicted by RAN, there corresponds effectively a root of P in $\mathbf{R}$ satisfying these sign conditions.

One may also use systems of equations.

A triangular system of equations (of degrees less than or equal to d) over the field $\mathbf{K}$ is given by a list of polynomials

$$P = [P_1, P_2, \dots, P_k]$$

with

$$P_1 \in \mathbf{K}[X_1], P_2 \in \mathbf{K}[X_1, X_2], \dots, P_k \in \mathbf{K}[X_1, X_2, \dots, X_k]$$

each P_j being monic of degree d_j as polynomial in X_j with $d_j \geq 2$ for every j and $d_{X_h}(P_j) < d_h$ for every $h < j$. A real solution of the system defined by the list P is a k-tuple $x = [x_1, x_2, \dots, x_k]$ in an ordered extension of $\mathbf{K}$, with:

$$P_1(x_1) = 0, P_2(x_1, x_2) = 0, \dots, P_k(x_1, x_2, \dots, x_k) = 0.$$

If $\mathbf{K}$ has a d-closed ordered extension $\mathbf{R}$, and if all the d_i are less than or equal to d, a root in $\mathbf{R}$ of the triangular system may be characterized à la Thom, by the list of signs of the derivatives of the $P_i(x_1, x_2, \dots, x_{i-1}, X)$ at $X = x_i$, by computations only in $\mathbf{K}$.

The computation goes as follows: the case of one variable corresponds to algorithm RAN above. In the case of a triangular system one applies the preceeding algorithm IF in an iterative way (with respect to the number of variables) and determines, by computations in $\mathbf{K}$, all the codings à la Thom of the solutions $(x_1, x_2, \dots, x_k)$ in $\mathbf{R}^k$ of the system.

Theorem 6. *Let* $\mathbf{K}$ *be an ordered field contained in a d-closed ordered extension* $\mathbf{R}$*. It is possible, by computations in* $\mathbf{K}$*, to characterize à la Thom the roots in* $\mathbf{R}$ *of a triangular system of equations with coefficients in* $\mathbf{K}$ *(of degrees less than or equal to d) and to decide the sign of every polynomial* $\mathbf{K}[X_1, \dots, X_k]$ *at these roots.*

4. Real closure

4.1. Real closed field.

Definition 7: A field $\mathbf{K}$ is *real closed* if it is ordered, if every positive element is a square, and if every polynomial of odd degree has a root.

Theorem 7. *Let* $\mathbf{K}$ *be a field. The following properties are equivalent*

a) $\mathbf{K}$ *is real closed,*

b) $\mathbf{K}$ *is ordered, and d-closed for every integer d,*

c) $\mathbf{K}$ *is real and* $\mathbf{K}[\sqrt{-1}]$ *is algebraically closed,* *d)* **K** *is real and every polynomial is decomposable in factors of degree one or two,*

e) **K** *is ordered and the number of roots on an interval* $]a, b[$ *(*$a < b$*) coincides with the number given by applying the Sturm's Theorem.*

Proof:

a) ⇒ b) is clear (cf. [**BCR**] page 9).

b) ⇒ a) is immediate.

a) ⇒ c) as in [**BCR**] page 9.

c) ⇒ d) group the conjugate roots.

d) ⇒ a) one starts by proving that for every a, a or $-a$ is a square: it is sufficient to decompose the polynomial $T^4 - a$ as a product of two monic polynomials of degree 2 and to equate coefficients; hence **K** is ordered and 2-closed; one constructs easily the sign table of any polynomial, and it is then clear that it has a root on every interval where its sign changes (irreducible factors of degree 2 have no influence on the sign table).

a) ⇒ e) after theorem 4

e) ⇒ b) Sturm's algorithm prescribes two roots to a polynomial $X^2 - c$ with $c > 0$ hence **K** is 2-closed. Then one proves by induction on d that **K** is d-closed using Proposition 2.

4.2. How to add one root.

Proposition 3. *Let* **K** *be a d-closed ordered field,* P *be a polynomial of degree* $d + 1$*,* a *and* b*,* $a < b$*, be two elements of* **K***. Let us suppose that* $P(a).P(b) < 0$ *and that* P' *is of constant sign over* $]a, b[$*. There exists a unique prime cone* α *of* **K**$[X]$ *algebraic over* **K** *such that* X_α *satisfies* $P(X_\alpha) = 0$ *and* $a < X_\alpha < b$*. Moreover in any ordered extension* **L** *of* **K***, with a root* c *of* P *in* $]a, b[$*, there exists a unique* **K***-isomorphism of ordered fields from* **K**$[X_\alpha]$ *to the subfield* **K**$[c]$ *of* **L***.*

Proof: Let suppose for example that P' is positive over the interval. Let Q be a polynomial of **K**$[X]$ and let us decide whether it belongs to α. Let Q_1 be the remainder of the division of Q by P. If Q_1 is zero (case 1) one has $Q \in \alpha$. Else, let us compute the subdivision defined by the roots of Q_1 over the interval $]a, b[$, and so the ordered list $[a = u_0, u_1, \ldots, u_n = b]$. The successive values of P are in strictly increasing order (by theorem 1). If $P(u_i) = 0$ for some i, (case 2), one has to take $Q \in \alpha$. Else P passes from sign $-$ to sign $+$ over one of the subintervals $[u_i, u_{i+1}]$, and Q_1 is of known constant sign σ over the interval $]u_i, u_{i+1}[$ (case 3). One has to take then $Q \in \alpha$ if σ is > 0.

Let us verify that we have defined a prime cone. Let us make two preliminary remarks. First, in the case when P has a root c in **K** on $]a, b[$, Q belongs to α_0 (resp. α_+, α_-) if and only if $Q(c)$ is 0 (resp. > 0, < 0) and it is clear that we have a prime cone. So we never have to consider case 2.

For the same reason we never have to consider in the proof cases where P is 0 at the root of a polynomial of degree $\leq d$. Second, if there exists an ordered extension $\mathbf{L}$ of $\mathbf{K}$ in which P has a root c on $]a,b,[$, P belongs to α_0 (resp. α_+,α_-) if and only if $P(c)$ is 0 (resp. >0, <0). This implies that α is a prime cone, as well as the existence of a unique $\mathbf{K}$-isomorphism from $\mathbf{K}[X_\alpha]$ to the subfield $\mathbf{K}[c]$ of $\mathbf{L}$.

Conditions 1') and 5) of definition 3 are trivially verified. Let us look at conditions 2'a) 2'b), 3'a), 3'b).

2'a) and 3'a): Let us suppose that Q is in α_0 (case 1). Then $Q+S$ and S have the same remainder modulo P, this implies $\alpha_0+\alpha\subset\alpha$. Also QS is 0 modulo P hence $\alpha_0.\alpha\subset\alpha_0$.

2'b) $\alpha_+{+}\alpha_+\subset\alpha_+$: Let Q and S be in α_+ (case 3), Q_1 and S_1 be the remainders of their euclidean division by P. Let us denote by $[u_0,u_1,\ldots,u_n]$ and $[v_0,v_1,\ldots,v_m]$ the subdivisions introduced by the roots of Q_1 and S_1 respectively. Let us join them in one subdivision, $[w_0,w_1,\ldots,w_l]$. The two polynomials Q_1 and S_1 are positive over the open interval of this subdivision where P changes sign. Hence Q_1+S_1 is also positive on this interval and the interval is a subinterval of those considered for the assignment of a sign to $Q+S$ via Q_1+S_1.

3'b) $\alpha_+.\alpha_+\subset\alpha_+$: The case of the product is slightly more complicated. It is necessary to introduce R, the remainder of the division of QS by P, which is also the remainder of the division of Q_1S_1 by P. One can consider the subdivision $[t_0,t_1,\ldots,t_s]$ associated to R and join the subdivisions u, v and t in one subdivision l. Let us define A as the quotient of Q_1S_1 by P, that is by the equality $Q_1S_1=AP+R$. One has $\deg(A)<d$. Over the minimal open interval of the subdivision l where P changes sign, one knows that Q_1 and S_1 are >0, hence if A is zero R is >0 which means that QS is in α_+. Else it is necessary to consider also the subdivision associated to A and join it with l in a subdivision m. Over the interval of the subdivision $]c,d[$ where P changes sign A has a sign σ and we chose the endpoint of the interval where P has sign $-\sigma$. Since P is continuous, there exists a point c' of the interval where P has again sign $-\sigma$. The sign of R over the interval, which is constant, is then the same as the sign of $R(c')=(Q_1S_1-AP)(c')$, hence >0.

Comment: We have not supposed P irreducible and we do not use factorization. It is well known that the existence of a factorization is not in general guaranteed from the constructive or computational point of view [**Se**].

4.3. Construction of the real closure.

Definition 8: A *real closure of an ordered field* $\mathbf{K}$ is an algebraic ordered extension of $\mathbf{K}$ which is a real closed field. An extension $\mathbf{R}$ of an ordered field $\mathbf{K}$ is an *ordered d-closure* of $\mathbf{K}$ if it is a d-closed ordered field and if every element of $\mathbf{R}$ can be obtained from elements of $\mathbf{K}$ by repetition of arithmetic operations and addition of a root of a polynomial of degree $\leq d$.

Theorem 7. *It is possible to construct a real closure for every ordered field* $\mathbf{K}$. *The real closure is unique up to unique* $\mathbf{K}$-*isomorphism of ordered fields.*

Proof: The proof is by induction on d, in order to show that:

(H_d) for every ordered field $\mathbf{L}$ we can construct a d-closure $\mathbf{L}^{(d)}$, unique up to unique $\mathbf{L}$-isomorphism of ordered fields. Moreover if $\mathbf{M}$ is a d-closed ordered extension of $\mathbf{L}$ there exists a unique increasing $\mathbf{L}$-morphism from $\mathbf{L}^{(d)}$ to $\mathbf{M}$.

For d =1, there is nothing to prove.

Let us suppose the hypothesis (H_d) true for d. If $\mathbf{K}$ is an ordered field, if P is a monic polynomial of degree $d+1$ in $\mathbf{K}^{(d)}[X]$, and if a and b are two consecutive roots of P' (or at infinity) satisfying $P(a).P(b) < 0$, we shall denote by $\mathbf{K}^{(d)}[X_\alpha]^{(d)}$ the d-closure of the field $\mathbf{K}^{(d)}[X_\alpha]$ with X_α root of P in $]a,b[$.

This ordered extension of $\mathbf{K}$ is unique up to (unique) $\mathbf{K}$-isomorphism of ordered fields as d-closed ordered extension of $\mathbf{K}^{(d)}$ containing a root of P over $]a,b[$. More precisely hypothesis (H_d) and proposition 3 show the following lemma.

Lemma. *If* $\mathbf{M}$ *is a d-closed extension of* $\mathbf{K}$ *there exists an algebraic ordered extension* $\mathbf{M}[X_\alpha]$ *of* $\mathbf{M}$ *such that there exists a (unique) increasing* $\mathbf{K}$-*morphism from* $\mathbf{K}^{(d)}[X_\alpha]$ *into* $\mathbf{M}[X_\alpha]$.

Let us use the following obvious notation when iterating the construction:

$$\mathbf{K}^{(d)}[X_{\alpha_1}]^{(d)}[X_{\alpha_2}]^{(d)}\cdots[X_{\alpha_i}]^{(d)}.$$

To obtain $\mathbf{K}^{(d+1)}$ one has to glue together all these extensions: which means introducing a good equivalence relation over their disjoint union. If

$$\mathbf{K}_1 = \mathbf{K}^{(d)}[X_{\alpha_1}]^{(d)}[X_{\alpha_2}]^{(d)}\cdots[X_{\alpha_i}]^{(d)}$$

and

$$\mathbf{K}_2 = \mathbf{K}^{(d)}[X_{\beta_1}]^{(d)}[X_{\beta_2}]^{(d)}\cdots[X_{\beta_j}]^{(d)}$$

are two extensions as before, there exists a unique $\mathbf{K}$-isomorphism of ordered fields of the composite extension

$$\mathbf{K}' = \mathbf{K}_1[X_{\beta_1}]^{(d)}[X_{\beta_2}]^{(d)}\cdots[X_{\beta_j}]^{(d)}$$

to

$$\mathbf{K}'' = \mathbf{K}_2[X_{\alpha_1}]^{(d)}[X_{\alpha_2}]^{(d)}\cdots[X_{\alpha_i}]^{(d)}.$$

An element of $\mathbf{K}_1$ will be considered as equal (in $\mathbf{K}^{(d+1)}$) to an element of $\mathbf{K}_2$, if and only if their images in $\mathbf{K}'$ and $\mathbf{K}''$ coincide up to the isomorphism. This defines an equivalence relation compatible with the ordered field structure: reflexivity and symmetry are immediate. Transitivity involves three extensions. It is clear that one gets in this way a $(d+1)$-closed extension and that it is unique up to unique $\mathbf{K}$-isomorphism of ordered fields.

It would be interesting to have a more direct proof of the following corollary.

Corollary. *In every ordered field, the Sturm algorithm prescribes a number of roots positive or zero.*

4.4. Data structure for the real closure.

The preceding theorem does not give immediately a finite data structure for the elements of the real closure since it is necessary to construct a lot of d-closures. Thinking a little about the proof one sees that the whole d-closure is not needed and that it would suffice to add a finite number of roots of polynomials of degree $\leq d$ (essentially the polynomials needed in Hörmander's method (cf [**BCR**], Chapter 1)). This point of view would lead to a much more technical proof of the existence of the real closure.

Since we proved that every ordered field may be embedded in a real closed field, it will be possible now to give a more concrete description of the real closure.

We have the following result:

Proposition 4. *The subfield of the real closure* $\mathbf{R}$ *of* $\mathbf{K}$ *consisting of the roots in* $\mathbf{R}$ *of triangular systems with coefficients in* $\mathbf{K}$ *is a real closed field equal to* $\mathbf{R}$*.*

Proof: The ring structure is clear. The existence of an inverse is shown by induction on the number k of equations of a triangular system. Finally it is clear that by adding one variable one can represent the square root of a positive number and the roots of polynomials of odd degree with coefficients in $\mathbf{K}$.

If one deals with a codable field it is thus possible to represent an element of the real closure as a polynomial expression of a real root coded à la Thom of a triangular system. One has to note that a given element of the real closure admits several representations and that it is possible to test by algorithm IF (with computations only in $\mathbf{K}$) whether two representations correspond or not to the same element. The computer algebra system SCRATCHPAD where one may use ordered fields as parameters will be necessary to implement our point of view.

5. Constructive theory of real closed fields

Theorem 10 (Tarski-Seidenberg principle). *Let* $\mathbf{K}$ *be an ordered field, subfield of a real closed field* $\mathbf{R}$ *and* Φ *be a formula of the language of ordered fields in* $n+1$ *variables with coefficients in* $\mathbf{K}$*, and without quantifiers. There exists a formula* Ψ *of the language of ordered fields with coefficients in* $\mathbf{K}$ *in* n *variables without quantifiers such that*

$$\{\mathbf{y} \in \mathbf{R}^n \mid \exists x \in \mathbf{R}\ \Phi(x, \mathbf{y})\} = \{\mathbf{y} \in \mathbf{R}^n \mid \Psi(\mathbf{y})\}$$

Proof: As in [**BCR**] by using Hörmander's method since all the tools needed are available.

It is not difficult to mimic the previous proofs in the framework of the formal intuitionistic theory of discrete real closed fields with parameters in $\mathbf{K}$. The general excluded-middle principle is not used, but one has a restricted excluded-middle of the form:

$$\forall x\ x > 0 \text{ or } x = 0 \text{ or } x < 0$$

which is a formal translation of the discrete character of the order considered. It is not possible to put immediately every formula under prenex form. Nevertheless the Tarski-Seidenberg principle above implies the possibility of eliminating one quantifier $\exists$ (before a quantifier free formula), hence to eliminate quantifiers even in formulas not in prenex form. So that the theory is also complete. The existence of a model (the real closure of $\mathbf{K}$) gives a constructive proof of the consistency of this formal theory. In short, as far as first order statements are concerned, one can use either classical logic or intuitionistic logic in a real closed field. Let us note also that a direct proof of the consistency and of the completeness of the formal intuitionistic theory considered would not give a method for constructing the real closure of $\mathbf{K}$, as we can see in the example of the theory of discrete algebraically closed fields (the "completeness theorem" is not valid constructively; on the contrary the consistency of the theory is assured as soon as any denumerable field has an algebraic closure).

Theorem 11. *Let* $\mathbf{K}$ *be an ordered field and* $T_1(\mathbf{K})$ *be the formal intuitionistic theory of real closed discrete fields with parameters in* $\mathbf{K}$*. Then* $T_1(\mathbf{K})$ *is decidable, complete and non contradictory. In particular, for every formula* F*, "*F *or not* F*" is a theorem.*

REFERENCES

[BCR] J. Bochnak, M. Coste, M.-F. Roy, "Géométrie algébrique réelle," Springer Verlag, 1987.

[BKR] M. Ben-Or, D. Kozen, J. Reif, *The complexity of elementary algebra and geometry*, J. of Computation and Systems Sciences **32** (1986), 251–264.

[B] S. Boughattas, "L'arithmétique ouverte et ses modèles non-standards," Thèse, Université Paris VI, 1987.

[CR] M. Coste, M.-F. Roy, *Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets*, J. Symbolic Computation **5** (1988), 121–129.

[GLRR] L. Gonzalez, H. Lombardi, T. Recio, M.-F. Roy, *Spécialisation de la suite de Sturm et sous-résultants*, To appear in RAIRO Informatique théorique. Detailed version, in CALSYF Journées du GRECO de Calcul Formel 1989.

[Ho] A. Hollkott, "Finite Konstruktion geordneter algebraischer Erweiterungen von geordneten Grundkörpen," Dissertation. Hamburg, 1941.

[Kl] S. C. Kleene, "Introduction to Metamathematics.," Van Nostrand, 1952.

[L] J. Legras, "Méthodes numériques," Dunod, 1963.

[MN] G. Metakides, A. Nerode, *Effective content of field theory*, Annals of Math. Logic **17** (1979), 289–320.

[MRR] R. Mines, F. Richman, W. Ruitenburg, "A Course in Constructive Algebra," Universitext, Springer-Verlag, 1988.

[Sa] T. Sander, *Existence and uniqueness of the real closure of an ordered field*, Journal of Pure and Applied Algebra (to appear).

[Se] A. Seidenberg, *Constructions in algebra*, Transactions of AMS **197** (1974), 273–313.

[Za] H. Zassenhauss, *A real root calculus*, in "Computational aspects in abstract algebra," Proceedings of a Conference held at Oxford, Pergamon Press, 1967, pp. 383–392.

Henri Lombardi
Mathématiques UFR des Sciences et Techniques
Université de Franche-Comté
25 030 Besançon cédex
France

Marie-Françoise Roy
I R M A R Université de Rennes 1
Campus de Beaulieu
35 042 Rennes cedex
France