Chapter IV

Quantifier elimination

1 - Definition and examples

One of the goals of model theory in general is to study definable sets (which may have geometric meaning, for instance), hoping that they have some nice structure. The first important model-theoretic idea to achieve this goal is quantifier elimination. This is a property of (certain!) models or of theories which state, informally, that every formula is equivalent to one that is built without quantifiers. When this holds, we can expect that the definable sets will be much simpler to describe than in general.

Definition - $\mathcal{L}$ language, T an $\mathcal{L}$-theory.

One says that T has <u>quantifier elimination</u> if for every <u>formula</u> $\phi(v_1, \dots, v_k)$, there exists a <u>quantifier-free</u> formula $\psi(v_1, \dots, v_k)$ such that

$$T \models (\phi \leftrightarrow \psi).$$

(We might also state this for a single model M of T.)

<u>Example.</u> Consider $\mathcal{L} = (+, -, \cdot, 0, 1)$ and the $\mathcal{L}$-theory T of algebraically closed fields. Then the formula

$$\phi(a,b,c) : \quad \exists x, \; ax^2 + bx + c = 0$$

is equivalent (using T) to

$$\psi(a,b,c) : \quad (a \neq 0) \vee (b \neq 0) \vee (c = 0).$$

On the other hand, the same formula is not equivalent to a quantifier-free formula in the $\mathcal{L}$-theory of commutative rings with unit, say.

<u>Remark.</u> Existence or not of quantifier elimination <u>depends</u> on the language! Indeed, we can

extend a language by adding definable relations which can then represent satisfiability of certain formulas, and this way achieve quantifier elimination artificially [say we had to $\mathcal{L}_{ring}$ a relation $(\underline{q}, 3)$ and enlarge the theory of commutative rings by the sentence

$$\forall a \forall b \forall c, \ q(a,b,c) \longleftrightarrow \exists x, \ ax^2+bx+c=0$$

Then the formula $\phi(a,b,c)$ is equivalent to the quantifier-free formula

$$\tilde{\psi}(a,b,c) : \quad q(a,b,c) \quad .]$$

Theorem -

(1) The theory of algebraically closed fields in $\mathcal{L}_{ring}$ has quantifier elimination.

(2) The theory RCF of real closed fields in $\mathcal{L}_{\substack{ordered\\rings}} = (+, -, \cdot, 0, 1, \leq)$ has quantifier elimination

Remark – For (2), note that the theory of real-closed fields (e.g. $\mathbb{R}$) can be axiomatized in $\mathcal{L}_{ring}$ because the order is definable (in such a field) by the formula

$$\leq (x,y) : \quad \exists z, \ x + z^2 = y \qquad (*)$$

This however involves a quantifier! So for instance, we can express

$\phi(a,b) : \ \exists x, \ x^2 + ax + b = 0$

by $\quad \psi(a,b) : \ a^2 - 4b \geq 0$ in a real-closed field, but translating to

$$\psi'(a,b) : \ \exists z, \ a^2 - 4b = z^2$$

amounts to going in circles...

(Note, however, that the definable sets in $\mathcal{L}_{ring}$ or $\mathcal{L}_{ordered\ rings}$ are the same, because of $(*)$, so the quantifier elimination in the second language <u>does</u> help understanding models of T).

We will sketch the proof of (2) to illustrate the type of methods available.

[Reference: S. Lang, "Algebra", 2nd Ed, chapter XI]

Definition. (Real-closed field)

(1) A field F is formally real if and only if -1 is not a sum of squares in F: for any $n \geq 1$, $a_1, \dots, a_n$ in F, $\sum a_i^2 \neq -1$.

(2) A field F is real closed if it is formally real and has no proper algebraic extension $K \supsetneq F$ such that K is formally real.

The basic examples of formally real fields are subfields of $\mathbb{R}$, and $\mathbb{R}$ itself is real closed.

Proposition. The real closed fields can be axiomatized in $\mathcal{L}_{ring}$ (i.e., there is a theory T such that $F \models T \iff F$ is real-closed).

Proof. The key algebraic fact that implies this is the following characterization of real-closed fields among formally real fields (which are clearly axiomatized by the sentences ϕ_n, $n \geq 1$,

$$\forall a_1 \dots \forall a_n,\ a_1^2 + \dots + a_n^2 + 1 \neq 0 \Big):$$

$$F \text{ is real closed}$$
$$\Updownarrow$$
$$F(\sqrt{-1}) \text{ is algebraically closed}$$
$$\Updownarrow$$
if $a \in F$ is not a square, then $-a$ is
and
any $f \in F[X]$ of odd degree has a root in F

The last statements are definable by :

$$\sigma : \quad \forall a,\ \exists z,\ (z^2 = a \vee z^2 = -a)$$

$$\psi_n : \quad \forall a_0 \dots \forall a_{2n},\ \exists y,\ y^{2n+1} + a_{2n} y^n + \dots + a_0 = 0$$

$\square$

It is moreover easy to check additionnally that if F is real closed then it has a unique order compatible with the field structure, defined by

$$x \leq y \iff \exists z,\ x + z^2 = y.$$

(Formally real fields can always be ordered, but the order may not be unique, e.g. in $\mathbb{Q}(\sqrt{2})$ we can define $a+b\sqrt{2}$ "$\leq$" $c+d\sqrt{2}$ either by the usual real ordering, or by the relation $a-b\sqrt{2} \leq c-d\sqrt{2}$; this is a compatible order because $a+b\sqrt{2} \longmapsto a-b\sqrt{2}$ is a field automorphism.)

2 - A model-theoretic criterion

We begin with a criterion that simplifies a potential proof of quantifier illumination (abbreviated q.e.).

For simplicity, we will assume that $\mathcal{L}$ has always at least one constant symbol. (In particular, $\mathcal{L}$-structures are not empty.)

Proposition - $\mathcal{L}$ language [with some constant]

T an $\mathcal{L}$-theory.

(1) T as q.e. if and only if for every q.f.

(quantifier-free) formula $\theta(v, v_1, \ldots, v_k)$, there exists a q.f. formula $\psi(v_1, \ldots, v_k)$ such that

$$T \models (\exists v,\ \theta(v, v_1, \ldots, v_k) \longleftrightarrow \psi(v_1, \ldots, v_k))$$

[In other words: it suffices to eliminate one existential quantifier at a time]

(2) Let $\phi(v_1, \ldots, v_m)$ be an $\mathcal{L}$-formula. Then ϕ is T-equivalent to a q.f. formula if and only if: for any models M, N of T, and any substructure $A \subset M \cap N$, [recall this implies that relations hold in A iff they hold in M and in N] we have

$$\forall\, a = (a_1, \ldots, a_m) \in A^m, \qquad M \models \phi(a) \iff N \models \phi(a).$$

It is the combination of these two facts that makes q.e. manageable in many circumstances.

Proof. (1) This is an elementary argument based on induction on the complexity of the formula combined with the fact that the $\forall$ quantifier can be represented by negation and $\exists$ [$\forall x\ \phi(x)$ being the same as $\neg \exists x, \neg \phi(x)$].

So for instance suppose ϕ is a formula of the form $\neg \psi$, and we already know (by induction) that ψ is equivalent to a q.f. formula ψ_0; then

$$T \models (\neg \psi \leftrightarrow \underbrace{\neg \psi_0}_{q.f})$$

and similarly for $\wedge, \vee$.

Suppose now $\phi(v_1, \dots, v_m)$ is $\exists w, \psi(w, v_1, \dots, v_m)$ and ψ is equivalent to a q.f. formula ψ_0. Then

$$T \models (\exists w, \psi(w, v_1, \dots, v_m) \leftrightarrow \overbrace{\exists w, \psi_0(w, v_1, \dots, v_m)}^{q.f.})$$

which by assumption is equivalent to a q.f. formula.

(2) The fact that q.e. implies the stated

property is left as an exercise (it is not the interesting part anyway; see Th. 3.1.4 in Marker's book if needed).

Consider the converse.

Step 1. If either $T \models \forall v, \phi(v)$ or $T \models \forall v, \neg \phi(v)$, then there is nothing to prove.

(Formally, in the first case, ϕ is equivalent to $c = c$, where c is a constant symbol, and in the second, to $\neg c = c$.)

Let then $\mathcal{L}^\circ = \mathcal{L} \cup \{c_1, \dots, c_m\}$ be the language with m new constants c_i. By Step 1, we may assume that the $\mathcal{L}^\circ$-theories $\mathcal{L} \cup \{\phi(c_1, \dots, c_m)\}$ and $\mathcal{L} \cup \{\neg \phi(c_1, \dots, c_m)\}$ are both satisfiable.

We further define

$$\Gamma = \{ \psi(v_1, \dots, v_m) \mid \psi \text{ q.f. and } T \models (\forall v, \phi(v) \to \psi(v)) \}$$

[all q.f. consequences of ϕ; for instance, in the case of real closed fields, if $\phi(a,b) = $ "$\exists x,\ x^2+ax+b=0$"

then Γ contains "$a^2-4b+1 \geq 0$", ...] and

$$\Gamma_c = \{\ \psi(c_1,\dots,c_m) \mid \psi \in \Gamma \}$$

(these are $\mathcal{L}^\circ$ - sentences now).

Step 2. $\quad T \cup \Gamma_c \models \phi(c_1,\dots,c_m) \qquad (*)$.

(Intuitively, T and q.f. consequences of ϕ imply ϕ; this is clearly what we want.)

To conclude formally from this (once it is proved), note that by the Compactness Theorem, it follows that there are q.f. formulas $\psi_1(c_1,\dots,c_m),\dots,$ $\psi_k(c_1,\dots,c_m)$ such that

$$T \models \forall v_1 \dots \forall v_m \left(\psi_1(v) \wedge \dots \wedge \psi_m(v) \longrightarrow \phi(v)\right)$$

(apply compactness to the unsatisfiable theory

$$T \cup \Gamma_c \cup \{\neg \phi(c)\}$$

to find a finite unsatisfiable subset Δ; let $\{\psi_1,\dots,\psi_k\} = \Gamma_c \cap \Delta$; then $T \models \forall v,\ \bigwedge_i \psi_i(v) \to \phi(v)$)

because otherwise Δ would have a model: take a model M of T such that there is $x \in M^m$ with all $\psi_i(x)$ satisfied but not $\phi(x)$; then M with c_i interpreted as x_i is a model of Δ) and since (by definition of Γ)

$$T \models \forall v, \quad \phi(v) \longrightarrow (\psi_1(v) \wedge \cdots \wedge \psi_m(v))$$

we have found the desired q.f. formula

$$\psi(v) = (\psi_1(v) \wedge \cdots \wedge \psi_m(v)).$$

We now prove $(*)$: $T \cup \Gamma_c \models \phi(c)$.

By contradiction, if this fails, there exists an $\mathcal{L}^\circ$-model M of $T \cup \Gamma_c \cup \{\neg \phi(c)\}$.

Let $x_i = c_{i,M} \in M$ be the interpretation of c_i.

Now let A be the $\mathcal{L}^\circ$-substructure of M generated by $(x_1, \dots, x_m)$ [i.e. the intersection of all substructures containing $x_1, \dots, x_m$; it is again an $\mathcal{L}^\circ$-substructure]. Extend further the language to $\mathcal{L}^\circ_A = \mathcal{L}^\circ \cup \{\tilde{c}_a \mid a \in A\}$, with one new constant for each element of A. Let

$$D = \{ \text{sentences } \phi(\tilde{c}_{a_1}, \dots, \tilde{c}_{a_\ell}) \text{ for atomic formulas } \phi \text{ s.t. } A \models \phi(a_1, \dots, a_\ell) \}$$

[$\ell \geq 0$ arbitrary]

$$\cup \{ \text{sentences } \phi(\tilde{c}_{a_1}, \dots) \text{ for atomic formulas s.t. } A \models \neg \phi(a_1, \dots) \}$$

(where an atomic formula is of the form $t_1 = t_2$ or $r(t_1, \dots, t_k)$ for relations r, terms t_i).

[So D is an $\mathcal{L}_A^\circ$-theory; it contains e.g. the formulas $(\tilde{c}_{a_1} \neq \tilde{c}_{a_2})$ if $a_1 \neq a_2$, or $(\tilde{c}_a = \tilde{c}_a)$ if $a \in A$, and also $(\tilde{c}_{x_i} = c_i)$.]

$\tilde{c}_{x_i}$ "$t_1(v)$", c_i "$t_2(v)$"

Claim: the $\mathcal{L}_A^\circ$-theory $T \cup D \cup \phi(c)$ is satisfiable.

Assuming this, let N be a model of this theory. Because N is a model of D, we have a map

$$f \begin{cases} A \longrightarrow N \\ a \longmapsto \tilde{c}_{a,N} \end{cases}$$

(interpretation of $\tilde{c}_a$ in N)

and it is straightforward from the definition of

D that f is an $\mathcal{L}^\circ$-embedding. So A can be identified, via f, as a common $\mathcal{L}^\circ$-substructure of M and N. We can now apply the assumption! Since $M \models \neg\phi(c)$ and x_i is the interpretation of c_i in M, we must have

$\neg\phi((x_i))$ in M, so also in N, which contradicts $N \models \phi(c)$ and the fact that $f(x_i) = \tilde{c}_{x_i}$ is also the interpretation of c_i in N. (This holds because "$\tilde{c}_{x_i} = c_i$" $\in D$)

To finally prove the last claim, we use Compactness again. If $T \cup D \cup \{\phi(\underline{c})\}$ has no model, there is a finite subset which has no model.

It follows that there are q.f. formulas $\tilde{\psi}_i(\underline{v})$, (see below) $1 \leq i \leq l$, such that

$$T \models \forall \underline{v}, \left(\tilde{\psi}_1(\underline{v}) \wedge \dots \wedge \tilde{\psi}_l(\underline{v}) \longrightarrow \neg\phi(\underline{v})\right)$$

so also

$$T \models \forall \underline{v}, \left[\phi(\underline{v}) \longrightarrow (\neg \tilde{\psi}_1(\underline{v})) \vee \cdots \vee (\neg \tilde{\psi}_k(\underline{v})) \right]$$

which would mean that

$$(\neg \tilde{\psi}_1(\underline{c})) \vee \cdots \vee (\neg \tilde{\psi}_k(\underline{c})) \in \Gamma_{\underline{c}},$$

and in particular

$$A \models (\neg \tilde{\psi}_1(\underline{c})) \vee \cdots \vee (\neg \tilde{\psi}_k(\underline{c}))$$

(since $M \models \Gamma_{\underline{c}}$ and $A \subset M$) which contradicts the fact that

$$A \models \psi_i(\underline{c})$$

for all i by definition of D.

To get the ψ_i's, we find a finite subset

$$\Delta' \subset T \cup D \cup \phi(\underline{c})$$

which has no model. Let $\{\psi_1, \ldots, \psi_\ell\} = D \cap \Delta'$.

Each ψ_i involves some constants $\tilde{c}_a$, $a \in A$, and because A is generated by $x_1, \ldots, x_m$, this implies that each a that appears is of the form $t(x_1, \ldots, x_m)$ for some term $t(v_1, \ldots, v_m)$ (not necessarily unique). So, for each ψ_i, we find a formula $\tilde{\varphi}_i(v_1, \dots, v_m)$ by substituting each $\tilde{c}_0$ with the corresponding term, and we then have $\varphi_i \longleftrightarrow \tilde{\varphi}_i(\underline{c})$.

Now if there is a model of T and $(y_i) \in M^m$ such that all $\tilde{\varphi}_i(\underline{y})$ hold as well as $\phi(\underline{y})$ then we obtain a model of Δ' by interpreting c_i as y_i, $\tilde{c}_a$ as $t(y)$, where t is a term corresponding to $a \in A$. Hence the claim.

3 _ Application to real - closed fields

We now prove q.e. for RCF, the theory of real closed fields in the language $\mathcal{L}_{ring,ord}$ of ordered rings.

By the previous section, it is enough to prove:

Proposition - Let F_1, F_2 be real closed fields and $A \subset F_1 \cap F_2$ an $\mathcal{L}_{ring,ord}$ - substructure. Let

$\varphi(v, \underbrace{\underline{w}}_{m \text{ variables}})$ be a q.f. formula. If there exists $\underline{a}$ in A^m and $x \in F_1$ such that $\varphi(x, \underline{a})$ holds (in F_1) then there exists $y \in F_2$ such that $\varphi(y, \underline{a})$ holds in F_2.

We will do this in a few steps.

Step 1 – $A \subset F_1$ (or F_2) is a subring of F_1, it is ordered, and the inclusions are compatible with the ordering.

Indeed, A being a substructure of F_1 in $\mathcal{L}_{\text{ring, ord}}$ equips A with $+, \cdot, -, \leq$, with the same interpretation as those of F_1, so $+, \cdot, -,$ 0_A and 1_A satisfy the axioms of commutative rings with unit (and $0_{F_1} = 0_A$, $0_{F_2} = 0_{A_2}$) because those say e.g. that $a_1 a_2 = a_2 a_1$ for $a_i \in A$, and this holds (because $M \models RCF$) in F_1, hence in A (because $\cdot_A = \cdot_{F_1}$ on $A \times A$).

etc ... Similarly, $\leq_A$ is an order compatible with that of F_1.

Step 2 - It is enough to treat the case where the q.f. formula has the form:

$$\varphi \quad : \quad \varphi_1 \vee \varphi_2 \vee \dots \vee \varphi_k$$

where $\varphi_i = \varphi_{i,1} \wedge \dots \wedge \varphi_{i,k_i}$, each $\varphi_{i,j}$ being $t_1 = t_2$ or $\neg(t_1 = t_2)$ or $(t_1 \leq t_2)$ or $\neg(t_1 \leq t_2)$. [t_i are terms]

This is a general syntactical fact ("reduction to disjunctive normal form"), together with the general form of terms and their negations in $\mathcal{L}_{ring,ord}$.

Step 3 - It is even enough to assume that φ is $\tilde{\varphi}_1 \wedge \dots \wedge \tilde{\varphi}_k$ with $\tilde{\varphi}_i$ either $t_i = 0$ or $t_i > 0$

Here we use the fact that if there is some x in F_1 with $\varphi(x, \underline{a})$, then $\varphi_i(x, \underline{a})$ holds for some i. We replace $(t_1 = t_2)$ by $(t_1 - t_2 = 0)$ and $\neg(t_1 \leq t_2)$ by $(t_2 - t_1 > 0)$ first. Then we might still have some φ_{ij} of the form $\neg(t_1 = t_2)$, in which case we note that

$$\varphi \iff \varphi_{i_1} \wedge \dots \wedge \varphi_{i_{j-1}} \wedge (t_1 < t_2 \vee t_2 < t_1) \wedge \dots$$

$$\iff (\varphi_{i_1} \wedge \dots \wedge \varphi_{i_{j-1}} \wedge (t_1 < t_2)) \vee (\dots)$$

and we "pick" one of the two alternatives; or we might have some $t_1 \leq t_2$ remaining and we replace this similarly by

$$(t_2 - t_1 > 0) \vee (t_2 - t_1 = 0)$$

and "distribute", and pick up some alternative.

Step 4 - Conclusion. Pick $\underline{a} \in A^k$.

Each term $t_i(v, \underline{w})$ in the q.f. formula becomes interpreted as a polynomial $f_i \in A[X]$ (with coefficients coming from the assignment $w_i = a_i$).

So we finally are in the situation where we have

$$\{f_1, \ldots, f_n\}^{n \geq 0}, \{g_1, \ldots, g_m\}^{m \geq 0} \quad \text{in} \quad A[X]$$

and an $x \in F_1$ such that

$$f_i(x) = 0 \quad \forall i, \qquad g_j(x) > 0, \quad \forall j$$

and we must prove the existence of $y \in F_2$ with the same properties.

Case 1 – If some f_i is non-zero, then $f_i(x) = 0$ implies that x is algebraic over A. So x belongs to the algebraic closure K_1 of A in F_1; but this is a real closure of A, and we have a strong uniqueness property:

Theorem – Let A be an ordered ring, K_1 and K_2 two extensions of A with compatible order. If K_1, K_2 are algebraic over A and real closed, then there is a unique order-compatible A-isomorphism $K_1 \xrightarrow{\sim} K_2$.

We apply this to K_1 and to the closure K_2

of A in F_2, obtaining an isomorphism

$$\varphi : K_1 \longrightarrow K_2$$

which is the identity on A and is order compatible. But then $y = \varphi(x)$ satisfies $f_i(y) = 0$ and all other equations / inequations.

Case 2. If all f_i are zero, then x satisfies

$$g_j(x) > 0 \ , \qquad \forall j.$$

Now each g_j is $\neq 0$ and is (in $F_1[X]$) a product of

a constant $\alpha \neq 0$

some monic linear polynomials $X + \beta$ $(\beta \in K_1)$

some monic irreducible polynomials of degree 2 $X^2 + \beta X + \gamma$ $(\beta, \gamma \in K_1,\ \beta^2 - 4\gamma > 0)$

[This is because $g_j \in K_1[X]$ and $K_1(\sqrt{-1})$ is algebraically closed.]

It follows that for each j, the set of x such that $g_j(x) > 0$ is a finite union of open intervals $]a, b[$ with a, b in K_1 (α gives a constant sign, monic quadratic are always > 0, and $X + \beta$ is > 0 exactly if $x > -\beta$; then we combine the various linear factors).

Since $g_j(x) > 0$ for all j, there is an open interval $]a', b'[$, a', b' in K_1, such that

$$\begin{cases} a' < x < b', \\ g_j(t) > 0 \quad \text{if} \quad a' < t < b'. \end{cases}$$

We can then find $x' \in K_1$ such that $a' < t < b'$, so $g_j(x') > 0$ for all j [for instance $x' = \frac{a'+b'}{2}$] and then $y = \varphi(x')$, where $\varphi : K_1 \xrightarrow{\sim} K_2$ is the isomorphism of Case 1, will satisfy the same inequalities (because $g_j \in A[X]$).

This concludes the proof.

$\square$

4. Applications of q.e. for RCF

Proposition. Consider RCF in the language $\mathcal{L}_{ring,ord}$.

(1) Any model of RCF is o-minimal. (We also say that the theory itself is o-minimal.)

(2) RCF is complete: for any sentence ϕ, either $T \models \phi$ or $T \models \neg\phi$ (any sentence is either true in all real closed fields, or in none; compare e.g. with the theory of fields: $\exists x,\ x^2+1=0$ may hold or not depending on the model).

(3) RCF is model-complete: if $F_1 \subset F_2$ is an embedding of RCF-models, then the embedding is elementary ($Th(F_1) = Th(F_2)$).

Proof.

(1) was already explained: by q.e., a definable subset $\phi(F) \subset F$, for $RCF \models F$, is a boolean combination of sets

$$\{x \mid f(x)=0\}, \quad \{x \mid f(x)>0\}$$

with $f \in F[X]$. Each is a finite union of points and open intervals $\{x \mid a < x < b\}$.

(3) This is true whenever q.e. holds because if $M \subset N$ is an embedding and $\phi(\underline{v})$ is q.f. then for any $\underline{a} \in M^m$, we have

$$M \models \phi(\underline{a}) \longleftrightarrow N \models \phi(\underline{a})$$

(because relations are preserved in embeddings, plus induction on complexity). Since every ϕ is equi-valent to a q.f. formula, the same holds for these.

(2) Any real closed field F has characteristic zero, so contains $\mathbb{Q}$, hence also the algebraic closure of $\mathbb{Q}$ in F. The latter field $\mathbb{Q}^{real}$ is a real closed field independent of F up to unique isomorphism preserving order, i.e. up to RCF-isomorphism.

So for any F there is an embedding

$$f: \mathbb{Q}^{real} \longrightarrow F$$

and by (2), it follows that $Th(\mathbb{Q}^{real}) = Th(F)$, so $T \models \phi \iff \mathbb{Q}^{real} \models \phi$, which implies the completeness.

$\square$

Example. ("Hilbert's 17th Problem")

Let $F = \mathbb{R}$, and let $f \in \mathbb{R}[x_1, \dots, x_n]$ be a polynomial such that $f(x) \geq 0$ for all $x \in \mathbb{R}^n$. Can one represent f as a sum of squares of polynomials? Hilbert showed that the answer is No in general (if $n \geq 2$; a simple example was given by Motzkin: $f = x_1^2 x_2^2 (x_1^2 + x_2^2 - 3) + 1$), and asked whether this could be done as a sum of squares of rational functions.

This is indeed true, as proved by Artin. One can give a proof using model-completeness: if f is not a sum of squares, then one can show that there is an ordering of $\mathbb{R}(X_i)$ such that $f < 0$; one knows then that $\mathbb{R}(X_i)$ has a real-closed extension F extending this ordering, so that $f < 0$ in F. Hence

$$F \models \exists \underline{v},\ f(\underline{v}) < 0$$

[take $\underline{v} = (X_i)$]

so, by model-completeness, also

$$\mathbb{R} \models \exists \underline{v},\ f(\underline{v}) < 0,$$

which means that f is not ≥ 0 as a function on $\mathbb{R}^n$.

Another classical consequence is the following:

Proposition. Let $X \subset \mathbb{R}^m$ be semi-algebraic (finite boolean combination of sets $\{x \mid f(x) > 0\}$, $f \in \mathbb{R}[X_1, \dots, X_m]$) and $f : \mathbb{R}^m \longrightarrow \mathbb{R}^p$ a polynomial map (e.g. $f(x_i) = (x_1, \dots, x_p)$ if $p \leq m$).

Then $f(X) \subset \mathbb{R}^p$ is semi-algebraic.

<u>Proof.</u> Indeed, X is definable in RCF, say $X = \phi(\mathbb{R}^m)$, and then

$$f(X) = \{ y \in \mathbb{R}^p \mid \exists x \in X, f(x) = y \}$$

is also definable, namely $f(X) = \psi(\mathbb{R}^p)$ with

$$\psi(y_1, \dots, y_p) : \text{"} \exists x_1 \dots \exists x_m, (\phi(\underline{x}) \wedge f(\underline{x}) = y) \text{"}.$$

By q.e., $\psi(\mathbb{R}^p)$ is semi-algebraic.

$\square$