Chapter 2

Quantifier Elimination

2.1 Elimination sets

Let L be a language. It may happen that two different L-formulas $\varphi(\vec{v})$ and $\varphi'(\vec{v})$ admit the same meaning in a structure $\mathcal{A}$ of L, or in a class of L-structures, for instance among the models of a given L-theory T. For example, in the ordered field of reals (and even in every real closed field), the formula $\varphi(v) : v \geq 0$ (being nonnegative) is the same thing as $\varphi'(v) : \exists w(v = w^2)$ (being a square). Similarly, in the ordered domain of integers, $\varphi(v) : v \geq 0$ (being positive) has the same interpretation as $\varphi'(v) : \exists w_1 \exists w_2 \exists w_3 \exists w_4 \, (v = \sum_{1 \leq i \leq 4} w_i^2)$ (being the sum of four squares): this is a celebrated theorem of Lagrange, already mentioned in the last chapter.

So, fix a consistent, possibly incomplete theory T in a countable L. We shall say that two L-formulas $\varphi(\vec{v})$ and $\varphi'(\vec{v})$ are equivalent with respect to T, and we shall write $\varphi(\vec{v}) \sim_T \varphi'(\vec{v})$, when

$$\forall \vec{v}(\varphi(\vec{v}) \leftrightarrow \varphi'(\vec{v})) \in T,$$

equivalently when

$$\varphi(\mathcal{A}^n) = \varphi'(\mathcal{A}^n)$$

for all models $\mathcal{A}$ of T.

The notion of elimination set arises quite naturally at this point. An elimination set for T is a set F of L-formulas such that every L-formula $\varphi(\vec{v})$ is T-equivalent to a suitable Boolean combination of formulas of F.

Clearly the set of all the L-formulas is an elimination set for T. But, of course, this is not an interesting case, and we reasonably expect simpler sets

F. In particular, when the set of atomic formulas in L is an elimination set for T, we say that T has the *quantifier elimination* in L. In detail

Definition 2.1.1 *Let T be a theory in a language L. T has the* **elimination of quantifiers** *(q.e.) in L if and only if every formula $\varphi(\vec{v})$ of L is equivalent in T to a quantifier free L-formula $\varphi'(\vec{v})$ (so to a finite Boolean combination of atomic formulas).*

One easily realizes that every T gets the elimination of quantifiers in a suitable language extending L. In fact, put $L = L_0$, $T = T_0$, and enlarge L_0 to a language L_1 containing an n-ary relation symbol R_φ for every formula $\varphi(\vec{v})$ of L_0 (n is the length of $\vec{v}$, of course); then add the following sentences to T_0

$$\forall \vec{v}(\varphi(\vec{v}) \leftrightarrow R_\varphi(\vec{v}))$$

for every $\varphi(\vec{v})$, and get a new theory T_1; it is clear that the atomic formulas of L_1 form an elimination set in T_1 for the formulas in L_0. By repeating this procedure countably many times, one eventually defines a language $L' \supseteq L$ and a theory T' of L' "naturally" extending T and having the elimination of quantifiers in L'.
Unfortunately this procedure has a quite artificial and abstract flavour. Indeed, what we would like to obtain, given a theory T in a language L, is showing that T has the quantifier elimination directly in L or, otherwise, determining a smallest extension $L' \supseteq L$, possibly suggested by the algebraic analysis of the models of T, where T (or, more exactly, its natural extension to L') has the elimination of quantifiers, or also a reasonably simple elimination set of formulas, in L'. In fact, there are good reasons to believe that such a language L' is, in some some, "the" proper language of T.

Which are the main advantages of an elimination set, in particular of quantifier elimination? They concern several applications.

1. The main one (at least from a historical point of view) is *decidability*. Actually the first and most celebrated quantifier elimination results are related to the decision theme. Let us explain why. Recall that a theory T is decidable if there is an algorithm checking in finitely many steps, for every sentence α in the language L of T, whether α is in T or not. Now suppose that F is an elimination set for T and that the following are available:

    - an *effective* procedure translating any L-sentence into a T-equivalent Boolean combination of sentences in F (or even an effective

reduction of any L-formula into a T-equivalent Boolean combination of formulas in F);

- an algorithm to decide, for every Boolean combination α of sentences of F, whether α is or not in T.

Then, clearly, T is decidable, and actually we have got a decision algorithm (by successively applying the previous two procedures).

2. Another noteworthy application of quantifier elimination concerns *definability*. In fact, if F is an elimination set for T, then the definable sets of a model $\mathcal{A}$ of T reduce to

$$\varphi(\mathcal{A}^n, \vec{x})$$

where $\varphi(\vec{v}, \vec{w})$ is a finite Boolean combination of formulas of F and $\vec{x} \in A$; in particular, if T has the quantifier elimination in L, then the definable sets of $\mathcal{A}$ are just the ones of the form

$$\varphi(\mathcal{A}^n, \vec{x})$$

where $\varphi(\vec{v}, \vec{w})$ is a quantifier free formula and $\vec{x}$ in A.

3. A third application regards the classification of *completions* of T. Recall that T is possibly incomplete; but we know that T has some (non-unique!) complete extension in L. So we are led to consider the problem of finding all the complete extensions of T in L, in other words classifying the isomorphism classes of models of T up to elementary equivalence. Now, if $\mathcal{A}$ and $\mathcal{B}$ are two models and $\mathcal{A}$ is not elementarily equivalent to $\mathcal{B}$, then there is some sentence φ in L such that $\mathcal{A} \models \varphi$ and $\mathcal{B} \models \neg\varphi$. As F is an elimination set for T in L, we can assume that φ is a Boolean combination of sentences in F. Indeed, one easily realizes that one can choose φ directly in F.

   For instance, we will see in this chapter that the theory ACF of algebraically closed fields has the quantifier elimination in $L = \{+, \cdot, -, 0, 1\}$. Consequently the classification of algebraically closed fields up to elementary equivalence depends on the quantifier free sentences in L, which are of the form $m = n$, where m and n are integers (m abbreviates in the previous formula the addition of m summands equal to 1 if $m > 1$, and $-(-m)$ if $m < -1$; similarly for n). This implies that the complete extensions of ACF are fully determined by the characteristic of their models, and hence coincide with the theories ACF_p where p is 0, or a prime.

4. Finally, let us deal with *model completeness*. Assume that T has quantifier elimination in L. We claim that, in this case, every embedding between models of T is elementary, in other words T is model complete. In fact, let $\mathcal{A}$ and $\mathcal{B}$ be models of T, f be an embedding of $\mathcal{A}$ into $\mathcal{B}$. Given a formula $\varphi(\vec{v})$ in L, let $\varphi'(\vec{v})$ a quantifier free formula equivalent to $\varphi(\vec{v})$ in L. Take $\vec{a}$ in A. As f is an embedding,

$$\mathcal{A} \models \varphi'(\vec{a}) \quad \Leftrightarrow \quad \mathcal{B} \models \varphi'(f(\vec{a})).$$

As $\forall \vec{v}(\varphi(\vec{v}) \leftrightarrow \varphi'(\vec{v})) \in T$,

$$\mathcal{A} \models \varphi(\vec{a}) \quad \Leftrightarrow \quad \mathcal{B} \models \varphi(f(\vec{a})).$$

Hence f is elementary.

This chapter is devoted to illustrating several key examples of quantifier elimination, starting from the earliest (Langford's results on discrete or dense linear orders) to include those perhaps most classical and celebrated (Tarski's elimination procedures for the real and the complex fields). We shall treat other eliminations sets as well (most notably, Baur-Monk's *pp*-elimination theorem for modules over a given ring).

These examples will lead us to introduce two basic notions in Model Theory, strong minimality and o-minimality respectively. We shall discuss them at the end of the chapter. The final section will be devoted to some computational aspects of the quantifier elimination procedures.

It should be underlined that the interest in quantifier elimination arose several years before the official birth of Model Theory. In fact it was at the beginning of the twentieth century that Löwenheim and, later, Skolem provided some procedures translating formulas into a simpler form avoiding quantifiers (they are, more or less, the artificial method we sketched at the beginning of this section). Moreover, the earliest explicit examples of quantifier elimination in some specific algebraic structures treat discrete and dense linear orders and date back to the twenties (they were obtained by Langford in 1927). In these results, as well as in Tarski's theorems, the major emphasis seems to be on decidability: the elimination of quantifiers is a step towards decidability, just as described before. But over the years this emphasis on decidability reduced and was replaced by an increasing interest in definability. Actually, definability is the main theme where Model Theory and quantifier elimination meet.

2.2 Discrete linear orders

We begin here our analysis of quantifier eliminable theories. First we treat infinite linear orders. Accordingly our basic language is $L = \{\leq\}$. More precisely we deal with:

- theories of discrete linear orders (in this section),
- theories of dense linear orders (in the next one).

As already said, the quantifier elimination results in these cases were firstly shown by Langford in 1927; Tarski pursued the analysis to get decidability and to classify the complete theories of infinite discrete and dense total orders.
Recall that a(n infinite) linear order $\mathcal{A} = (A, \leq)$ is **discrete** if and only if

(i) $\forall a \in A$, if there is some $a' \in A$ such that $a < a'$, then there exists a least $b \in A$ for which $a < b$ (b is called the *successor* of a and is denoted $s(a)$);

(ii) $\forall a \in A$, if there is some $a' \in A$ such that $a' < a$, then there exists a maximal $b \in A$ for which $b < a$ (b is called the *predecessor* of a; obviously $a = s(b)$).

Accordingly we can distinguish 4 classes of (infinite) discrete linear orders:

1. the class of discrete linear orders with a least, but no last element (like $(\mathbf{N}, \leq)$);
2. the class of discrete linear orders with a last, but no least element (for instance, $\mathbf{N}$ with respect to the relation reversing its usual order);
3. the class of (infinite) discrete linear orders with both a least and a last element (like the disjoint union of two discrete linear orders $(A, \leq)$, $(B, \leq)$, the former in 1, the latter in 2, with $a < b$ for all $a \in A$ and $b \in B$);
4. the class of discrete linear orders without endpoints (like $(\mathbf{Z}, \leq)$).

Each of these classes is elementary. Moreover one can show that its theory has the elimination of quantifiers in a suitable language extending L, and is complete even in L. Here we limit ourselves to prove, for simplicity, these results in the case 1, in other words for discrete linear orders with a least but no last element.

Accordingly consider the language $L' = \{\leq, 0, s\}$ where 0 is a constant (to be interpreted in the least element) and s is a 1-ary operation symbol (to be interpreted in the function mapping any element into its successor).
It is easy to write down a first order set of axioms for our class in L'. Let dLO^+ denote the corresponding theory. By the way, notice that suitable formulas in the restricted language L define the minimal element and the successor function in every model of dLO^+. This implies that the axioms of dLO^+ can be rewritten also in L, at the cost of some more complications (and quantifiers). For instance, expressing the existence of a minimal element requires the L-sentence

$$\exists w \forall v (w \leq v)$$

instead of

$$\forall v (0 \leq v).$$

But we momentarily prefer to treat dLO^+ in L'. Observe that:

- $(\mathbf{N}, \leq, 0, s)$ is a model of dLO^+;
- if $\mathcal{A}$ is another model of dLO^+, then $\mathcal{A}$ contains a substructure $(\{s^n(0^{\mathcal{A}}) : n \in \mathbf{N}\}, \leq, 0^{\mathcal{A}}, s^{\mathcal{A}})$ isomorphic to a $(\mathbf{N}, \leq, 0, s)$, and moreover some further copies of $(\mathbf{Z}, \leq, s)$ (as $0^{\mathcal{A}}$ is the only element without any predecessor).

Theorem 2.2.1 *dLO^+ has the elimination of quantifiers in L'.*

Proof. Take a formula $\varphi(\vec{v})$ in our language L'; we look for an equivalent formula $\varphi'(\vec{v})$ without quantifiers.
Our first step is to show that we can assume that $\varphi(\vec{v})$ is of the form

$$\exists w \bigwedge_{i \leq r} \alpha_i(\vec{v}, w)$$

where each $\alpha_i(\vec{v}, w)$ is an atomic formula, or its negation, and w actually occurs in $\alpha_i(\vec{v}, w)$ for every $i \leq r$.
We wish to underline that this step is quite general, and does not depend on our particular language L'. Let us see why. First of all, we can tacitly assume that $\varphi(\vec{v})$ is of the form

$$Q_1 w_1 \ldots Q_m w_m \alpha(\vec{v}, \vec{w})$$

where the Q_j's $(1 \leq j \leq m)$ denote quantifiers $\forall$ or $\exists$, $\alpha(\vec{v}, \vec{w})$ is a quantifier free formula, and even a disjunction of conjunctions of atomic formulas and

negations (and $\vec{w}$ abridges $(w_1, \ldots, w_m)$, of course). The strategy at this point is first to eliminate Q_m, and then to repeat the procedure and remove the quantifier string completely. We recall that $\forall$ is equivalent to $\neg\exists\neg$ and consequently agree that it is enough to deal with the case when Q_m is $\exists$, namely with

$$\exists w\, \alpha(\vec{v}, w)$$

where α is a disjunction of conjunctions of atomic formulas or negations, $w = w_m$ and $\vec{v}$ is possibly enlarged to include $w_1, \ldots, w_{m-1}$. As $\exists$ is distributive with respect to $\vee$, namely $\exists w(\alpha' \vee \alpha'')$ is equivalent to $(\exists w\alpha') \vee (\exists w\alpha'')$, there is no loss of generality for our purposes in assuming that α is just a conjunction of atomic formulas or negations. In conclusion we are dealing with

$$\exists w \bigwedge_{i \leq r} \alpha_i(\vec{v}, w)$$

where each $\alpha_i(\vec{v}, w)$ is an atomic formula, or its negation. We can also assume that w actually occurs in $\alpha_i(\vec{v}, w)$ for every $i \leq r$; otherwise let $j \leq r$ deny this condition and notice that our formula

$$\exists w \bigwedge_{i \leq r} \alpha_i(\vec{v}, w)$$

is equivalent to

$$\alpha_j(\vec{v}) \wedge \exists w \bigwedge_{i \neq j} \alpha_i(\vec{v}, w);$$

at this point it suffices to eliminate the quantifier $\exists$ in the latter part of the formula

$$\exists w \bigwedge_{i \neq j} \alpha_i(\vec{v}, w).$$

This completes our preliminary step. As already said, this does not depend on our particular framework.
Now let us work with our formula

$$\exists w \bigwedge_{i \leq r} \alpha_i(\vec{v}, w)$$

and our language L'. We wonder which is the form of any α_i. A look at L' shows that α_i is $t = t'$, or $t \leq t'$, or the negation of one of these formulas, where t and t' are terms in 0, w, $\vec{v}$ (and w actually occurs in t or t'). Recall that $\neg(t \leq t')$ means $t > t'$, and so on. Deduce that α_i is, with no loss of generality, either $t = t'$ or $t > t'$, with t and t' as before. Notice that t and

t' are of the form $s^p(u)$ where p is a nonnegative integer and u ranges over 0, w, $\vec{v}$. Now recall that s is injective and deduce that the formula under exam ensures that there is a solution w for a finite set of conditions saying that w or a successor $s^q(w)$ (q a nonnegative integer) is equal, or bigger, or smaller than a term $s^p(u)$ where p is, again, a nonnegative integer and u ranges over w, 0, $\vec{v}$: as s is injective, we can assume that, in each of these equations and inequations, s occurs only in one side (on the left, or on the right). Our aim is to translate this formula into an equivalent one avoiding w and simply stating quantifier free conditions on $\vec{v}$ (and 0).
To obtain this, proceed as follows. Trivialities like $w = w$ or $w < s^p(w)$ for a positive p can be ignored and deleted (they can be preliminarily listed and hence are easily recognized); if nothing else occurs, then replace the whole formula by $0 = 0$. On the contrary, when meeting a condition that cannot be satisfied by any w, like $w = s^p(w)$, or $0 = s^p(w)$ for a positive p (also these conditions can be preliminarily listed), then replace our formula with $\neg(0 = 0)$ (or with $\neg(v_1 = v_1)$ if you like and $\vec{v}$ is not empty).
Otherwise, as soon as you meet one equation like $w = s^p(v_i)$, delete w and $\exists$, and replace w with $s^p(v_i)$ throughout our formula. Proceed in the same way if an equation $w = s^p(0)$ occurs. Similarly, when meeting a condition $s^q(w) = v_i$, consider any further occurrence of w in the formula and, again using the injectivity of s, represent it as $s^{q'}(w)$ for a suitable nonnegative integer $q' \geq q$; finally delete w and $\exists$ and replace each occurrence $s^{q'}(w)$ by $s^{q-q'}(v_i)$.
At last, assume that only disequations occur. Again using the injectivity of s, we can suppose that all of them concern the same term $s^q(w)$ in w. So our formula states that $s^q(w)$ is smaller that certain terms $t_0, \ldots, t_h$ in 0 and $\vec{v}$, and larger that some other terms $t_{h+1}, \ldots, t_k$. We obtain an equivalent formula avoiding w and its quantifier in the following way. List (in a suitable disjunction) all the possible orderings of $t_0, \ldots, t_k$ in $\leq$ according to which $t_0, \ldots, t_h$ precede $t_{h+1}, \ldots, t_k$; for every ordering, let t, t' denote respectively the greatest element among $t_0, \ldots, t_h$ and the least among $t_{h+1}, \ldots, t_k$; add $s(t) < t'$ (in order to provide $s^q(w)$ with suitable room).
This concludes the elimination procedure. ♣

Corollary 2.2.2 *dLO^+ is model complete (in L') and complete (both in L' and L).*

Proof. Clearly dLO^+ is model complete in L'. Moreover $(\mathbf{N}, \leq, 0, s) \models dLO^+$, and $(\mathbf{N}, \leq, 0, s)$ is embeddable in every model of dLO^+. As dLO^+ is

model complete, all the corresponding embeddings are elementary. Accordingly all the models of dLO^+ are elementarily equivalent to $(\mathbf{N}, \leq, 0, s)$ and hence to each other. This shows that dLO^+ is complete in L'. Now recall that both the minimal element and the successor function (so the interpretations of the symbols in $L' - L$) are $\emptyset$-definable by L-formulas in the models of dLO^+. Then it is an easy exercise to deduce that dLO^+ is complete in L, too. ♣

Corollary 2.2.3 *dLO^+ is decidable (in L' and in L).*

Proof. Reduce any sentence of L' into an equivalent quantifier free statement. This is a Boolean combination of formulas $s^m(0) \geq s^n(0)$ where m and n are non-negative integers, and dLO^+ can easily check its membership. This procedure works even for L-sentences. ♣

Corollary 2.2.4 *Let $\mathcal{A} \models dLO^+$. The subsets of A definable in $\mathcal{A}$ (in L or in L') are just the finite unions of (open or closed) intervals in $\mathcal{A}$ (possibly having $+\infty$ as a right endpoint).*

Proof. Let $\varphi(v, \vec{w})$ be a L'-formula. As dLO^+ has the elimination of quantifiers in L', we can assume thant $\varphi(v, \vec{w})$ is quantifier free; owing to Theorem 2.2.1 (and its proof), for every $\vec{a}$ in A, $\varphi(\mathcal{A}, \vec{a})$ is a union of intersections of intervals, and hence a union of intervals. ♣

This accomplishes our analysis of discrete linear orders with a last but no least elements. How to deal with the other three cases of infinite discrete linear orders listed before? They can be handled in a similar way to get quantifier elimination and consequently completeness. In particular it turns out that the four cases exhaust all the possible completions of the theory of infinite discrete linear orders; in other words, these completions are fully characterized by saying if the corresponding models admit or lack a least and a greatest element.
Actually the case without endpoints deserves some more comments. In fact, in this framework, the enlarged language L' needs no natural "constant" symbol (just because endpoints are lacking), and takes the only additional operation symbol s. Accordingly, properly speaking, the elimination of quantifiers fails in this extended language, because we have no constant to build atomic sentences. For instance the (true) sentence $\exists w(w = w)$ cannot be translated into an equivalent quantifier free sentence; the same happens for the (false) sentence $\exists w(s(w) = w)$. So the right statement here is as

follows: an elimination set for the theory of discrete linear orders without endpoints is the set of atomic formulas *plus* a unique sentence (such as "there is no least element", or "there is no last element"). We do not discuss the proof here. In fact, we shall treat this case in detail when considering dense linear orders in the next section.
Finally, notice that decidability can be shown (in L) in the 4 possible cases. Consequently the (incomplete) theory dLO of infinite discrete linear orders is decidable, too; in fact, a sentence φ of L belongs to dLO if and only if it is in each of its 4 completions.

2.3 Dense linear orders

Now we deal with dense linear orders. The plan here is exactly the same as in the discrete case. We use the language $L = \{\leq\}$ and we distinguish 4 possible cases:

1. there is a least element, but no last element (just as among non-negative rationals with respect to the usual order);

2. there is a last element, but no least element (now non-positive rationals provide an example);

3. there are both a least element and a last element (look at the rationals, or even at the reals, in the closed interval $[0, 1]$);

4. there are no endpoints (this is the case of $(\mathbf{Q}, \leq)$).

In 1, 2, 3 one shows elimination of quantifiers in a language with one or two additional constants to be intepreted into the endpoints; 4 deserves a more specific treatment, because quantifier free formulas need an auxiliary single L-sentence to form an elimination set (even in L): we provide full details below. In all these cases it is easy to deduce completeness in L. This implies that these 4 classes exhaust all the possible completions of the theory of dense linear orders.
As already said, here we limit our analysis to dense linear orders without endpoints. We just met their theory in Chapter 1; we called it DLO^- and we observed that it is $\aleph_0$-categorical, hence complete. We treat now quantifier elimination (in L), and in this way we provide an alternative and detailed proof of its completeness.

Theorem 2.3.1 *The quantifier free formulas of L together with a single sentence of DLO^- (such as $\exists v(v = v)$) are an elimination set of DLO^-.*

Proof. We follow the same approach as in the discrete case. But now the successor symbol does not make sense, our language is smaller and hence our setting is simpler: L-terms are just variables (no constant arises because there are no endpoints). Accordingly what we have to do is to eliminate the quantifier in a formula

$$\exists w\, \alpha(\vec{v}, w)$$

where $\alpha(\vec{v}, w)$ is a conjunction of conditions saying that w is equal, or smaller, or larger than some v in $\vec{v}$. To obtain this, proceed as follows. Again ignore trivialities like $w = w$ (they can be preliminarily listed and easily recognized); if nothing else occurs, just replace our formula with $\exists v(v = v)$. On the contrary, when meeting a condition that cannot be satisfied by any w, like $w < w$ (also these negative statements can be preliminarily listed), replace our formula with $\neg\exists v(v = v)$. Otherwise, as soon as you meet one equation $w = v_i$, delete w and $\exists$, and replace w with v_i throughout our formula. At last, if only disequations occur and hence our formula states that w is smaller than certain variables ($v_1, \ldots, v_h$ with no loss of generality) and larger that others ($v_{h+1}, \ldots, v_k$), then get the required quantifier free formula in the following way. List (in a suitable disjunction) all the possible orderings of $v_1, \ldots, v_k$ in $\leq$ according to which $v_1, \ldots, v_h$ precede $v_{h+1}, \ldots, v_k$; for every ordering, let v, v' denote respectively the maximal element among $v_1, \ldots, v_h$ and the least among $v_{h+1}, \ldots, v_k$; $v < v'$ and the density assumption are sufficient to ensure that an intermediate w exists. When $h = 0$ or $h = k$, one uses the lack of endpoints.
This concludes the elimination procedure. ♣

Corollary 2.3.2 *DLO^- is model complete and complete.*

Proof. Model completeness is a straightforward consequence. Completeness can be deduced as follows, using model completeness. First notice that any two dense linear orders with no endpoints $(A, \leq)$ and $(B, \leq)$ embed in a common extension (for instance, their sum $(A + B, \leq)$, where $A + B$ is the disjoint union of A and B, $\leq$ enlarges the orderings in A and B and, in addition, satisfies $a < b$ for every choice of $a \in A$ and $b \in B$). As DLO^- is model complete, each of these embeddings is elementary, in particular $(A, \leq)$ and $(B, \leq)$ are elementarily equivalent to their sum, and hence to each other. ♣

As already recalled, completeness was also observed in the previous chapter via $\aleph_0$-categoricity and the Vaught criterion. By the way, notice that the

Vaught Theorem provides a completeness proof even when endpoints arise. In fact, also the remaining classes of dense linear orders (with least and/or last element) have an $\aleph_0$-categorical theory.
The decidability of DLO^- can be easily shown. Indeed, by proceeding as in the discrete case, one sees that even the theory of arbitrary dense orders (with or without endpoints) is decidable.
Now let us deal with definability.

Corollary 2.3.3 *Let $\mathcal{A} \models DLO^-$. The subsets of A definable in $\mathcal{A}$ are just the finite unions of (open or closed) intervals, possibly with infinite endpoints.*

Proof. Proceed as for dLO^+. ♣

2.4 Algebraically closed fields (and Tarski)

Tarski obtained his celebrated quantifier elimination procedures for the complex field and the ordered field of reals in the thirties. Owing to the stop due to the World War, he published his results only in 1948. We consider here the complex case, and we delay the real one to the next section. We should underline that Tarski dealt with theories of single structures (the complex field, the ordered field of reals) rather than on axiomatizable classes (ACF, RCF). But a careful analysis of the proofs singles out which kind of algebraic conditions are necessary to ensure the quantifier elimination result: so one realizes that what makes the machinery work is just being algebraically closed in the complex case, and the intermediate value property for polynomials in the real case. This is a crucial result, specially towards the aim of finding a nice axiomatization for the theory of the complex field, or of the ordered field of reals.
As promised, here we consider the complex case, but we prefer an approach dealing with the whole class of algebraically closed fields.

Theorem 2.4.1 (Tarski) *The theory ACF of algebraically closed fields has the elimination of quantifiers in the language $L = \{+, \cdot, -, 0, 1\}$.*

Proof. Take a formula $\varphi(\vec{v})$ of L, we are looking for an equivalent quantifier free formula $\varphi'(\vec{v})$. As before, we can limit our analysis to the case when $\varphi(\vec{v})$ is of the form

$$\exists w\, \alpha(\vec{v}, w)$$

where $\alpha(\vec{v}, w)$ is a finite conjunction of atomic formulas and negations, all containing w. In our language, atomic formulas are just equalities of terms, hence equations. Using $-$, one can express each of them as

$$p(\vec{v}, w) = 0$$

where $p(\vec{y}, x)$ is a polynomial with integer coefficients. Accordingly $\varphi(\vec{v})$ is

$$\exists w \, (\bigwedge_{i \leq k} p_i(\vec{v}, w) = 0 \wedge \bigwedge_{j \leq h} \neg(q_j(\vec{v}, w) = 0))$$

where the p_i's and the q_j's are polynomials with integer coefficients, all having a positive degree, n_i and m_j respectively, in x, hence with respect to w.

Basic field theory tells us that a sequence of elements in a field excludes 0 if and only if its product is not 0. Accordingly, we can assume that at most one inequation occurs in $\varphi(\vec{v}, w)$, say

$$\neg(q(\vec{v}, w) = 0).$$

where $q(\vec{y}, x)$ is the product of the polynomials $q_j(\vec{y}, x)$ when $j \leq h$; let m denote the degree in x of $q(\vec{y}, x)$.

At this point one might wonder whether we can reduce the number of equations in our formula $\varphi(\vec{v}, w)$ to get at most a single equation. This is true, and can be shown by using again pure field theory (so without appealing to algebraic closure), but requires some more subtlety. The idea is that, for a given field K and a sequence $\vec{b}$ in K, the common roots of the polynomials $p_i(\vec{b}, x)$ are just the roots of their greatest common divisor, and that there is a quantifier free formula in $\vec{v}$, defining the coefficients (in x) of this greatest common divisor, and independent of K and $\vec{b}$. The former claim is clear. Let us explain the details of the latter.

Consider $p_i(\vec{y}, x)$ for $i \leq k$. For every i, write $p_i(\vec{y}, x)$ as a polynomial in x with coefficients in $\mathbf{Z}[\vec{y}]$

$$p_i(\vec{y}, x) = \sum_{r \leq n_i} p_{i,r}(\vec{y}) x^r.$$

Take two of these polynomials, for instance p_0 and p_1, and suppose for simplicity $n_0 \geq n_1$. We claim that there is quantifier free formula in $\vec{v}$ yielding, whenever $p_1(\vec{v}, x)$ is not the null polynomial (in x), the coefficients in x of the quotient and the remainder of the division of $p_0(\vec{v}, x)$ by $p_1(\vec{v}, x)$. To get this formula, just follow the usual division procedure for polynomials.

This is a tedious but straightforward exercise. For instance, the first step is to write that either

$$p_{1,n_1}(\vec{v}) = 0$$

or the coefficients of $p_0(\vec{v}, x)$ and $p_1(\vec{v}, x)$ satisfy

$$p_{1,n_1}(\vec{v})\, p_0(\vec{v}, x) = p_{0,n_0}(\vec{v}) p_1(\vec{v}, x) x^{n_0 - n_1} + P(\vec{v}, x),$$

where $P(\vec{v}, x)$ is a polynomial of degree $< n_0$ in x, and, in the latter case, the required quotient admits

$$p_{0,n_0}(\vec{v})(p_{1,n_1}(\vec{v}))^{-1} x^{n_0 - n_1}$$

as a coefficient of maximal degree.
At this point, recall the Euclidean algorithm of repeated divisions, yielding the greatest common divisor (in x) of our polynomials $p_i(\vec{y}, x)$ $(i \leq k)$ as the last nonzero remainder in a finite sequence of successive divisions. Again, a suitable quantifier free formula in $\vec{v}$ determines the coefficients in x of our greatest common divisor, whenever the $p_i(\vec{v}, x)$'s $(i \leq k)$ are not all zero.
In conclusion, we can assume that our formula $\varphi(\vec{v}, w)$ has one of the following three forms:

1. $\exists w(p(\vec{v}, w) = 0)$,
2. $\exists w \neg(q(\vec{v}, w) = 0)$,
3. $\exists w(p(\vec{v}, w) = 0 \wedge \neg(q(\vec{v}, w) = 0))$

where p and q are as before.
First consider 1. In any field, 1 is equivalent to say that, if $\vec{v}$ annihilates all the coefficients of $p(\vec{y}, x)$ in x of positive degree in x, then $\vec{v}$ assigns the value 0 also to the term of degree 0 in x; this can be written as a suitable quantifier free formula in $\vec{v}$.
Now consider 2. In any infinite field, 2 is equivalent to say that $\vec{v}$ does not annihilate the coefficients of the polynomial $p(\vec{y}, x)$ in x. Again, the latter statement can be expressed by a quantifier free formula in $\vec{v}$.
Finally let us deal with 3. We claim that, in any algebraically closed field, 3 is equivalent to the statement

$$(\star) \qquad p(\vec{v}, x) \text{ does not divide } q(\vec{v}, x)^n;$$

recall that n is the degree of $p(\vec{y}, x)$ with respect to x, and notice that $(\star)$ can be expressed as a quantifier free formula in $\vec{v}$ (just use the previous remarks

about divisibility, and write that the remainder of the division in $(\star)$ is not 0). The direction from left to right is true in every field K: if, for a given sequence $\vec{b}$ in K, the annihilator of $p(\vec{b}, x)$ is not included in the annihilator of $q(\vec{b}, x)$, then $p(\vec{b}, x)$ cannot divide $q(\vec{b}, x)$ and $(q(\vec{b}, x))^n$. Conversely, take K and $\vec{b}$ as before; assume that every root of $p(\vec{b}, x)$ annihilates $q(\vec{b}, x)$, too; for K algebraically closed, this implies that every linear factor of $p(\vec{b}, x)$ divides $q(\vec{b}, x)$ and hence that $p(\vec{b}, x)$ divides $q(\vec{b}, x)^n$.
This accomplishes our proof. ♣

Now let us comment this quantifier elimination result, and propose some noteworthy consequences. First of all, we want to emphasize that the quantifier elimination property characterizes the algebraically closed fields among infinite fields. In fact, it is a profound result of Macintyre, McKenna e Van den Dries that an infinite field whose theory eliminates the quantifiers in the language $L = \{+, -, \cdot, 0, 1\}$ must be algebraically closed.
An obvious consequence of quantifier elimination is the following.

Corollary 2.4.2 *ACF is model complete.*

Clearly ACF is not complete. In fact, for every prime p, the sentence $p = 0$ is true in every algebraically closed field of characteristic p and false in every algebraically closed field of characteristic $\neq p$. However, as we already showed in Chapter 1,

Corollary 2.4.3 *For every $p = 0$ or prime, the theory ACF_p is complete.*

Proof. In Chapter 1 we provided a proof founded on Vaught's Theorem. An alternative approach, using quantifier elimination (indeed model completeness), is the following. Fix p. There is a minimal algebraically closed field $\mathcal{K}_p$ of characteristic p: this is the algebraic closure of the prime subfield. $\mathcal{K}_p$ is embeddable in every algebraically closed field of the same characteristic. Owing to the model completeness of ACF_p, all these embedding are elementary. In particular, all the algebraically closed fields of characteristic p are elementarily equivalent to $\mathcal{K}_p$, and consequently to each other. ♣

As we already observed in section 2.1, the theories ACF_p exhaust all the possible completions of ACF in L when p ranges over the primes and 0 (furthermore, each of them has the quantifier elimination in L, just because it extends ACF).
An application of the Compactness Theorem lets us say even more. In fact, we have seen that the theory of the complex field is just ACF_0, and so is axiomatized by ACF and, in addition, by the infinitely many sentences stating

$\neg(p = 0)$ for every prime p. Let σ be any sentence in ACF_0. Compactess tells us that σ is a consequence of ACF and finitely many sentences concerning the characteristic. Hence σ is true in every algebraically closed field of prime characteristic p for all but finitely many p's. So we have shown the following result.

Theorem 2.4.4 *Let σ be a sentence of the language L. σ is true in some (equivalently every) algebraically closed field of characteristic 0 if and only if σ is true in some (equivalently every) field of characteristic p for all but finitely many primes p.*

Hence what is true in the complex field (and in any algebraically closed field of characteristic 0) is satisfied by the algebraically closed fields of characteristic p for almost all primes p. We'll see later in this section a nice application of this model theoretic transfer principle to Algebra.
Now let us deal briefly with decision problems. As already said, decidability follows in a very simple way from quantifier elimination.

Corollary 2.4.5 *The theory ACF of algebraically closed fields is decidable.*

Proof. It suffices to decide if a given quantifier free sentence σ of L is in ACF or not. With no loss of generality, σ is a conjunction of disjunctions of atomic sentences and negations. As a conjunction is in a theory if and only if each conjunct is, we can write σ (up to equivalence, using $-$) as

$$(\bigvee_i m_i = 0) \vee (\bigvee_j \neg(n_j = 0)).$$

where the m_i's and the n_j's are positive integers. So our sentence just says that the characteristic divides $\prod_i m_i$ or is coprime with some n_j (or suitable variants when no equation, or inequation arises). This can be easily checked in the fixed framework. ♣

We shall add some more comments about the decidability of ACF in the last section of this chapter.
Now let us deal with definability. We have seen in Chapter 1 that, in any field K, constructible sets (in particular algebraic varieties) are definable. Theorem 2.4.1 implies that, within algebraically closed fields, the converse is also true.

Corollary 2.4.6 *In an algebraically closed field K, for every positive integer n, a subset of K^n is definable if and only if is constructible.*

Proof. It suffices to show that, if $X \subseteq K^n$ is definable, then X is constructible. Let $\varphi(\vec{v}, \vec{w})$ be a formula of L and $\vec{a}$ be a sequence in K satisfying

$$X = \varphi(\mathcal{K}^n, \vec{a})$$

where n is the length of $\vec{v}$. Using quantifier elimination, we can replace $\varphi(\vec{v}, \vec{w})$ by an equivalent formula which excludes quantifiers and consequently is a finite Boolean combination of equations

$$q(\vec{v}, \vec{w}) = 0$$

where $q(\vec{x}, \vec{y})$ is a polynomial with coefficients in the subring generated by 1. Hence $X = \varphi(\mathcal{K}^n, \vec{a})$ is the Boolean combination of the algebraic varieties defined by the formulas

$$q(\vec{v}, \vec{a}) = 0,$$

and so is a constructible set. ♣

Notice that in every field $\mathcal{K}$ the subsets of K^n definable by quantifier free formulas are constructible. Quantifier elimination ensures that, when $\mathcal{K}$ is algebraically closed, no further definable set arises.
The following proposition underlines the geometrical content of Tarski's Theorem.

Theorem 2.4.7 (Chevalley) *Let $\mathcal{K}$ be an algebraically closed field, n be a positive integer, $X \subseteq K^{n+1}$, X' be the projection of X onto the first n coordinates. If X is constructible, then X' is also constructible.*

Proof. If $\varphi(\vec{v}, w)$ defines X, then $\exists w \varphi(\vec{v}, w)$ defines X'. ♣

Now let us consider 1-ary definable sets in an algebraically closed field $\mathcal{K}$. In this restricted framework, the following proposition holds.

Corollary 2.4.8 *Let $\mathcal{K}$ be an algebraically closed field, $X \subseteq K$ be definable in $\mathcal{K}$. Then X is either finite or cofinite.*

Proof. For every $q(x, \vec{a}) \in K[x]$, $q(v, \vec{a}) = 0$ defines K if $q(x, \vec{a})$ is zero, and a finite set otherwise. A finite Boolean combination of finite or cofinite sets is still finite or cofinite. ♣

Actually we can say even more. Indeed, in any (possibly non-algebraically closed) field $\mathcal{K}$, a subset X of K definable by a quantifier free formula is either

finite or cofinite. Quantifier elimination extends this property to arbitrary 1-ary subsets when $\mathcal{K}$ is algebraically closed.
To conclude this section, we want to propose a nice application of Model Theory to Algebra within algebraically closed fields. This is the so called *injectivity-implies-surjectivity* Theorem, due to J. Ax [3]. Compactness, and the consequent remark that the sentences true in the complex field are just those satisfied by the algebraically closed fields of characteristic p for almost all primes p, are used to deduce

Theorem 2.4.9 *Any injective morphism f from an algebraic variety V over the complex field into V itself is surjective.*

Proof. We already noticed that any algebraic variety is a definable set, and is even defined by a finite conjunction of equations (possibly with parameters). In particular let the formula

$$\bigwedge_{j \leq t} p_j(\vec{v}, \vec{a}) = 0$$

give V in this way (the p_j's are polynomials with integer coefficients, and $\vec{a}$ denotes a sequence of complex parameters). Analogously, a morphism between varieties is a map defined by a finite conjunction of equations. Accordingly let

$$\bigwedge_{i \leq s} q_i(\vec{v}, \vec{w}, \vec{a}) = 0$$

yield f (the q_i's are again polynomials with integer coefficients; we can freely use here the same parameters $\vec{a}$ as before; if necessary, we extend $\vec{a}$ to include new complex numbers). At this point it is an easy exercise to write a first order sentence in the language L (without parameters) saying:

> *for all $\vec{z}$, if $\bigwedge_{i \leq s} q_i(\vec{v}, \vec{w}, \vec{z}) = 0$ defines a morphism from the variety given by $\bigwedge_{j \leq t} p_j(\vec{v}, \vec{z}) = 0$ into itself, and this morphism is injective, then it is also surjective.*

Let n denote, as usual, the length of $\vec{v}$. What we have to show is that the complex field is a model of all these sentences when the p_j's and the q_i's range over the polynomials with integer coefficients, equivalently that ACF_0 includes these statements. Using compactness, we can alternatively check what happens in ACF_p when p is a prime, and so if the previous sentences are true in every algebraically closed field of characteristic p; as ACF_p is complete, it suffices to look at the behaviour of a single model of ACF_p,

for instance of the algebraic closure $\overline{\mathbf{F}_p}$ of the field $\mathbf{F}_p$ with p elements: a positive answer in $\overline{\mathbf{F}_p}$ for sufficiently many p implies a positive answer for the complex field. So take an algebraic variety V over $\overline{\mathbf{F}_p}$ and an injective morphism f from V to V over $\overline{\mathbf{F}_p}$. Use the algebraic fact that $\overline{\mathbf{F}_p}$ is locally finite and represent V as the union of its intersections with F^n where F ranges over the finite subfields of $\overline{\mathbf{F}_p}$ (containing the parameters defining V and f). Recall the trivial principle that any injective function from a finite set to itself is also surjective. Deduce that the restriction of f to $V \cap F^n$ is surjective for every F. Extend this result to f: f is surjective, as required. ♣

2.5 Tarski again: Real closed fields

In this section we deal with the quantifier elimination theorem for real closed fields. This is the main result of Tarski in this framework, not only because, as we shall see, the proof is deeper and more complicated than in the complex case, but also because the ordered field of reals is intrinsecally related to geometry. It is certainly needless to recall that, for instance, in the Euclidean plane equipped with some fixed Cartesian axes, every point is essentially an ordered pair of reals, every straight line is the variety given by a polynomial with degree 1 and 2 unknowns over the reals, and so on. Accordingly, statements about points, lines, ... can be easily translated into statements about reals, addition, multiplication (often in a first order way). In particular, a decision algorithm about the theory of the ordered field of reals (the *elementary algebra* according to Tarski's terminology) should work for (first order) Euclidean geometry as well.
Actually Tarski's quantifier elimination procedure dealt with the reals rather than with the theory RCF. But, just as in the complex case, one can realize that the basic ingredients of the proof concern arbitrary real closed fields. So we state (and show) the result in this (seemingly enlarged) setting; but we shall deduce quickly that RCF is complete and hence equals the theory of $(\mathbf{R}, +, -, \cdot, 0, 1, \leq)$. We follow the elegant approach of Cohen [27] rather than Tarski's original proof.

Theorem 2.5.1 *The theory RCF of reals closed fields has the elimination of quantifiers in the language $L = \{+, -, \cdot, 0, 1, \leq\}$.*

Proof. By proceeding as in the case of algebraically closed fields, one preliminarily realizes that the heart of the matter is to eliminate the quantifier

$\exists$ in a formula

$$\exists w \alpha(w, \vec{v})$$

where $\alpha(w, \vec{v})$ is the conjunction of at most one equation $p(w, \vec{v}) = 0$ and a finite (possibly empty) set of disequations $q_j(w, \vec{v}) > 0$ (with $j \leq m$), where $p(x, \vec{y})$ and $q_j(x, \vec{y})$ $(j \leq m)$ are polynomials with integer coefficients.
So let us open a (long) parenthesis and examine an arbitrary polynomial $f(x) = \sum_{i \leq t} f_i x^i$ with coefficients in a real closed field K. It is known that, if f_i is not 0 for all $i \leq t$, then $f(x)$ has at most t roots in the field. Fix t. Then it is easily seen that

1) the function calculating, for every polynomial $f(x)$ as before, equivalently for every non-zero sequence $(f_0, \ldots, f_t)$ in K^{t+1}, how many roots $f(x)$ admits

as well as, for every r and s with $1 \leq r \leq s \leq t$,

2) the set of non-zero sequences $(f_0, \ldots, f_t)$ in K^{t+1} such that $f(x)$ has exactly s roots,

3) the function mapping any nonzero $(f_0, \ldots, f_t)$ into the r-th root of $f(x)$

are definable in any ordered field K in a uniform way (independent of K). We claim that, within real closed fields, for every t, these objects are definable by quantifier free formulas, still in a uniform way (independent of the underlying field). To see this, one uses the Sturm theory of real root counting. We proceed by induction on t.
The case $t = 0$ is clear: the number of roots is 0 if $f_0 \neq 0$, and undefined otherwise; 2 and 3 are empty objects.
So assume $t > 0$ and suppose our claim true for every natural value $< t$, in order to extend it to t. The idea here is to relate the zeroes of $f(x)$ to the roots of its derivative and the sign of $f(x)$ in these roots. Hence build the formal derivative $f'(x)$ of $f(x)$ with respect to x

$$f'(x) = \sum_{0 < i \leq t} i f_i x^{i-1}.$$

Preliminarily, notice that $f'(x) = 0$ if and only if $(f_1, \ldots, f_t) = (0, \ldots, 0)$. Except this case, induction equips us with quantifier free formulas defining (with respect to $(f_0, \ldots, f_t)$ via $(f_1, 2f_2, \ldots, tf_t)$)

1) the function counting, for every sequence $(f_0, \ldots, f_t)$ with $(f_1, \ldots, f_t) \neq (0, \ldots, 0)$, how many roots $f'(x)$ admits,

and, for $1 \leq r \leq s < t$,

2) the set of the sequences $(f_0, \ldots, f_t)$ in K^{t+1} such that $(f_1, \ldots, f_t)$ is not zero and $f'(x)$ has exactly s roots,

3) the function mapping any (suitable) non-zero $(f_0, \ldots, f_t)$ into the r-th root of $f'(x)$.

Now order the roots of $f'(x)$

$$\rho_1 < \ldots < \rho_s.$$

The intermediate value property, holding in every real closed field, ensures that $f'(x)$ cannot change its sign between two successive roots. Can we deduce that $f(x)$ is monotone (increasing or decreasing according to the sign of $f'(x)$) in the same interval? Certainly yes in the case of the real field: this is a well known result in elementary real analysis. But a complete algebraic (although non trivial) proof can be done for polynomials by using only the axioms of RCF. Consequently, in every real closed field K, $f(x)$ is monotone (increasing or decreasing according to the sign -positive or negative- of its derivative) in each interval (ρ_i, ρ_{i+1}), $1 \leq i < s$. Now look at $f(\rho_i)$ and $f(\rho_{i+1})$.

(i) If they are not 0 and their sign is the same, then (ρ_i, ρ_{i+1}) does not contain any root of $f(x)$ because $f(x)$ is monotone in the interval (notice that the cases when exactly one between ρ_i and ρ_{i+1} annihilates $f(x)$ can be handled in a similar way).

(ii) If $f(\rho_i)$ and $f(\rho_{i+1})$ admit opposite signs, then (ρ_i, ρ_{i+1}) does contain a root of $f(x)$ by the intermediate value property. The uniqueness of this root might follow from Rolle's Theorem (two distinct roots of $f(x)$ $\rho_i < a < b < \rho_{i+1}$ determine a new intermediate root of $f'(x)$, and this is impossible). Elementary analysis ensures that Rolle's Theorem is certainly true for the reals; but, again, one can give an alternative algebraic and non trivial proof (for polynomials) holding in every real closed field.

(iii) Assume at last $f(\rho_i) = f(\rho_{i+1}) = 0$. The argument in 2 again excludes any additional intermediate root of $f(x)$.

This machinery lets us count the roots in the interval $[\rho_1, \rho_s]$. But what can we say in $(-\infty, \rho_1)$ and $(\rho_s, +\infty)$? The same arguments as before ensure

that $f(x)$ is monotone, and at least one root occurs in each of these half-lines. But our setting changes when we examine the existence of this root. For, every interval (ρ_i, ρ_{i+1}) $(1 \leq i \leq s)$ is bounded, while our half-lines are not. However the following algebraic fact helps us.

> Let $f(x) = \sum_{i \leq t} f_i x^i$ as before. Then $f(x)$ has no roots out of the interval $[-a, a]$ where $a = 3t\, max\{(|f_{t-i} f_t^{-1}| : 0 < i \leq t\} + 1$.

(The proof only uses the axioms of ordered fields). So a possible root less than ρ_1 should lie in $[-a, \rho_1)$, and a possible root greater than ρ_s should belong to $(\rho_s, a]$; moreover the absolute value function $|\ |$ can be defined in a quantifier free way, because, for every $b \in K$, $|b|$ is b when $b \geq 0$ and $-b$ otherwise. Hence we are led to a bounded framework, and we can proceed as in the previous cases.

In conclusion, we have provided a uniform procedure counting, for every nonzero $(f_0, \ldots, f_t)$ in K, how many roots $f(x)$ admits. The function calculating their number s is defined by a quantifier free formula (essentially checking the sign of $f(x)$ in the roots of its derivative and in $\pm a$). Similarly the set of non-zero sequences $(f_0, \ldots, f_t)$ in K for which $f(x)$ has exactly s roots can be defined by checking these sign relations and forming a suitable first order disjunction to list the cases when s occurs. Finally, the function producing, for every non-zero $(f_0, \ldots, f_t)$ and $1 \leq r \leq s$, the r-th root of $f(x)$ is easily defined on the same basis.

This accomplishes the proof of the claim and ends our parenthesis. Now we come back to quantifier elimination. Recall that we are considering a formula

$$(a) \qquad \exists w (p(w, \vec{v}) = 0 \wedge \bigwedge_{j \leq m} q_j(w, \vec{v}) > 0)$$

or

$$(b) \qquad \exists w \bigwedge_{j \leq m} q_j(w, \vec{v}) > 0$$

where $p(x, \vec{y})$ and $q_j(x, \vec{y})$ $(j \leq m)$ are polynomials with integer coefficients. Each of them can be written as a polynomial with coefficients in $\mathbf{Z}[\vec{y}]$ in the following way

$$p(x, \vec{y}) = \sum_{i \leq t} p_i(\vec{y}) x^i,$$

$$q_j(x, \vec{y}) = \sum_{i \leq t_j} q_{j,i}(\vec{y}) x^i.$$

(a) is quickly reduced to (b) because its formula is equivalent to

$$(\bigwedge_{i\leq t} p_i(\vec{v}) = 0 \wedge \exists w \bigwedge_{j\leq m} q_j(w, \vec{v}) > 0) \vee$$

$$\bigvee_{1\leq r\leq s\leq t} (\text{"}p(x, \vec{v}) \text{ has } s \text{ roots"} \wedge$$

$$\wedge \text{"the } r\text{-th root } \rho_r(\vec{v}) \text{ satisfies } \bigwedge_{j\leq m} q_j(\rho_r(\vec{v}), \vec{v}) > 0\text{"}),$$

where the latter disjunct can be expressed by a quantifier free first order formula. So look at (b). For every $j \leq m$ and for every $s_j \leq t_j$, there are quantifier free formulas defining, for every real closed field K, the set of the sequences $\vec{b}$ such that $q(x, \vec{b})$ has s_j roots in x, and listing these roots

$$\rho_{j,1}(\vec{b}) < \ldots < \rho_{j,s_j}(\vec{b}).$$

One can compute the sign of $q_j(x, \vec{b})$ in the intervals

$$(-\infty, \rho_{j,1}(\vec{b})),$$

$$(\rho_{j,i}(\vec{b}), \rho_{j,i+1}(\vec{b})) \quad (1 \leq i < s_j),$$

$$(\rho_{j,s_j}(\vec{b}), +\infty)$$

in a uniform way (independent of K and $\vec{b}$) by looking at the (sign) value of

$$q_j(\rho_{j,1}(\vec{b}) - 1, \vec{b})$$

$$q_j(\frac{\rho_{j,i}(\vec{b}) + (\rho_{j,i+1}(\vec{b})}{2}, \vec{b})$$

$$q_j(\rho_{j,s_j}(\vec{b}) + 1, \vec{b})$$

respectively. List all the possible orderings of the roots (in x) of the $q_j(x, \vec{b})$'s when j ranges over the natural numbers $\leq m$, and divide in every case K into finitely many intervals such that the $q_j(x, \vec{b})$'s have a constant sign (with respect to x) in each of them; check these signs (in the way suggested before) and form a suitable disjunction picking the intervals where all these signs are positive. This procedure is independent of K and $\vec{b}$ and provides the required quantifier free formula. ♣

Corollary 2.5.2 *RCF is model complete.*

Corollary 2.5.3 *RCF is complete; in particular, RCF is the theory of the ordered field of reals (as well as of every real closed field).*

Proof. There is a minimal ordered real closed field, embedded in any model of RCF. This is the ordered field $\mathbf{R}_0$ of real algebraic numbers. The model completeness of RCF ensures that every real closed field is an elementary extension of $\mathbf{R}_0$. In particular all the real closed fields are elementarily equivalent to $\mathbf{R}_0$ and, consequently, to each other. ♣

This is the first completeness proof we give about RCF; in fact Vaught's criterion does not apply because RCF is not categorical in any infinite power.

We have seen that real closed fields eliminate quantifiers in their language $L = \{+, -, \cdot, 0, 1, \leq\}$. Notably, they are fully characterized by this property: for, Macintyre, McKenna and Van den Dries showed that an ordered field, whose theory has the quantifier elimination in L, must be real closed. We also notice that RCF does not preserve quantifier elimination in the restricted language $L' = \{+, -, \cdot, 0, 1\}$ without order. Actually one can remember that, even in checking solvability of the popular equation $ax^2 + bx + c = 0$ with degree 2 and 1 unknown over the reals (or over any real closed field), one needs a disequation $b^2 - 4ac \geq 0$ to ensure roots, and hence to eliminate $\exists$ in the formula $\exists w(v_2 w^2 + v_1 w + v_0 = 0)$. More formally, recall that, with respect to the theory of the real field, the formulas

$$\varphi(v) : \ v \geq 0,$$

$$\varphi'(v) : \ \exists w(v = w^2)$$

are equivalent. As RCF is complete and hence equals the theory of the real field, the same holds in every real closed field. Consequently the L'-formula (with the quantifier $\exists$)

$$\varphi'(v) : \ \exists w(v = w^2)$$

defines the set of non-negative elements in every real closed field. However $\varphi(v)$ cannot be equivalent in RCF to any quantifier free L'-formula $\varphi''(v)$. In fact $\varphi(\mathbf{R})$ is the half-line $[0, +\infty)$ of $\mathbf{R}$, and so is both infinite and coinfinite, while $\varphi''(\mathcal{K})$ is either finite or cofinite for every field $\mathcal{K}$: see the proof of Corollary 2.4.8.

Now we discuss decidability: as already said, this was the main consequence of elimination of quantifiers, according to the general feeling in the fourties.

Corollary 2.5.4 *RCF is decidable.*

Proof. Owing to quantifier elimination, every L-sentence σ is equivalent in RCF to a Boolean combination of sentences $m = n$ or $m < n$ where m and

n are integers. This quantifier free statement can be easily checked in our framework. ♣

We shall comment this result later in 2.9. Now we examine another remarkable consequence of quantifier elimination, namely definability. Recall that, in an ordered field $\mathcal{K}$, every semialgebraic set (in other words, every finite Boolean combination of sets of solutions of disequations

$$q(\vec{x}) \geq 0$$

with $q(\vec{x}) \in \mathcal{K}[\vec{x}]$) is definable.

Corollary 2.5.5 *In a real closed ordered field $\mathcal{K}$, the definable sets are exactly the semialgebraic ones.*

Proof. Let n be a positive integer, $X \subseteq K^n$ be a set definable in $\mathcal{K}$. So there are a formula $\varphi(\vec{v}, \vec{w})$ of L and a sequence $\vec{a} \in K$ such that

$$X = \varphi(K^n, \vec{a}).$$

Owing to Tarski's quantifier elimination theorem, we can assume that $\varphi(\vec{v}, \vec{w})$ has no quantifier and hence is a finite Boolean combination of disequations

$$q(\vec{v}, \vec{w}) \geq 0$$

with $q(\vec{x}, \vec{y}) \in \mathbf{Z}[\vec{x}, \vec{y}]$. Consequently X is a finite Boolean combination of sets of solutions of disequations

$$q(\vec{v}, \vec{a}) \geq 0,$$

and so is a semialgebraic set. ♣

Here is a geometric restatement of Tarski's Theorem.

Theorem 2.5.6 (Tarski-Seidenberg) *Let $\mathcal{K}$ be a real closed ordered field, n be a positive integer, $X \subseteq K^{n+1}$, X' be the projection of X onto the first n coordinates. If X is semialgebraic, then X' is semialgebraic, too.*

This formulation is due to Thom, who also coined the name *semialgebraic set*. It has a more geometric flavour. Some mathematicians might appreciate this alternative terminology, for instance because it allows to state several results in a (seemingly) more agreable way (avoiding logic). Nevertheless, Tarski's original approach (via quantifier elimination and formulas) often provides quicker proofs, even in this geometric framework. Let us quote the following example from [168].

Example 2.5.7 Consider the following statement: *For a semialgebraic function f from $\mathbf{R}^{n+1}$ to $\mathbf{R}$, the set A of the sequences $\vec{x}$ in $\mathbf{R}^{n+1}$ such that*

$$lim_{y\to\infty} f(\vec{x}, y) \text{ is in } \mathbf{R}$$

is semialgebraic.

If one replaces everywhere *semialgebraic* by *definable*, this proposition may lose part of its (mathematical) glamour. But, using logic, one obtains a short proof: A is definable via the formula

$$\varphi(\vec{v}) \quad : \quad \exists w \forall \epsilon(\epsilon > 0 \longrightarrow \exists r \forall y(y > r \longrightarrow$$

$$\longrightarrow \exists z(f(\vec{v}, y) = z \wedge |z - w| < \epsilon)))$$

(recall that both f and the absolute value are definable). A direct approach via semialgebraic sets and projections is longer.
In a real closed field $\mathcal{K}$, the definable subsets $X \subseteq K$ have a very simple form.

Corollary 2.5.8 *Let $\mathcal{K}$ be a real closed field, X be a definable subset of $\mathcal{K}$. Then X is a finite union of intervals (closed or open, possibly with infinite endpoints).*

Proof. Let $q(x) \in K[x]$. We know that $q(v) = 0$ defines K if $q(x) = 0$ and a finite set (that is, the set of the roots $a_0 < \ldots < a_s$ of $q(x)$ in $\mathcal{K}$) otherwise. On the other hand, $q(v) > 0$ defines $\emptyset$ if $q(x) = 0$; otherwise $q(v) > 0$ defines the union of some intervals among $]-\infty, a_0[$, $]a_0, a_1[$, $\ldots$, $]a_s, +\infty[$ (recall that $\mathcal{K}$ satisfies the intermediate value property for polynomials). Hence any definable (equivalently, semialgebraic) set $X \subseteq K$ is a finite Boolean combination of intervals, and so a finite union of intervals. ♣

2.6 pp-elimination of quantifiers and modules

In this section we deal with (left) modules over a (countable) ring $\mathcal{R}$ with identity. In Chapter 1, we introduced a suitable language $L_R = \{0, +, -, r\ (r \in R)\}$ for these structures, and we saw how to axiomatize their class by first order sentences in L_R. Let $_{\mathcal{R}}T$ denote the corresponding theory. A quick look at the axioms of $_{\mathcal{R}}T$ shows that each of them is a universal sentence $\forall \vec{v} \alpha(\vec{v})$ where $\alpha(\vec{v})$ is an atomic formula of L_R; this confirms that the class of the models of $_{\mathcal{R}}T$ (namely of the $\mathcal{R}$-modules) is closed under

substructures. Now we wonder whether ${}_{\mathcal{R}}T$ has quantifier elimination in L_R. A trivial example shows that this is false even in the simple case when $\mathcal{R}$ is the ring $\mathbf{Z}$ of integers. In fact, just consider $\mathbf{Z}$ as a module over itself. In $\mathbf{Z}$ the formula

$$\varphi(v) : \exists w(v = 2w)$$

defines the set $2\mathbf{Z}$ of even integers. On the other side, every atomic formula $\varphi'(v)$ in $L_{\mathbf{Z}}$ is equivalent within ${}_{\mathbf{Z}}T$, and hence in the theory of the $\mathbf{Z}$-module $\mathbf{Z}$, to

$$rv = 0$$

for some non-negative integer r. This formula defines in $\mathbf{Z}$ $\{0\}$ if $r \neq 0$ and $\mathbf{Z}$ otherwise. No Boolean combination of these sets can equal $2\mathbf{Z}$. Therefore no quantifier free formula $\varphi'(v)$ of $L_{\mathbf{Z}}$ is equivalent to $\varphi(v)$ in $Th(\mathbf{Z})$, and so in ${}_{\mathbf{Z}}T$. It follows that ${}_{\mathbf{Z}}T$ does not eliminate the quantifiers in $L_{\mathbf{Z}}$.
However notice that $\varphi(v)$ is a typical pp-formula in $L_{\mathbf{Z}}$. Indeed we will see that, for any R, the pp-formulas of L_R are just the only obstruction to the elimination of quantifiers of ${}_{\mathcal{R}}T$ in L_R. Let us see why.
Take any (countable) ring $\mathcal{R}$ with identity. Recall that a pp-formula of L_R is an existential formula of the form

$$\varphi(\vec{v}) : \exists \vec{w}(A \cdot \vec{v} = B \cdot \vec{w})$$

where A and B are matrices with coefficients in R with suitable sizes, $\cdot$ denotes the usual row-by-column product between matrices, and $\vec{v}$, $\vec{w}$ should be viewed as column vectors (with suitably many rows). So, when $\vec{w} = \emptyset$, pp-formulas include the atomic formulas of L_R.
In Chapter 1 we pointed out that, for every pp-formula $\varphi(\vec{v})$ of L_R and every $\mathcal{R}$-module $\mathcal{M}$, $\varphi(\mathcal{M}^n)$ is a subgroup of $\mathcal{M}^n$ (called a pp-definable subgroup), but is not in general a submodule. Let us add here some more remarks about pp-formulas.

Remark 2.6.1 1. If $\varphi(\vec{v})$, $\psi(\vec{v})$ are pp-formulas of L_R, then also $\varphi(\vec{v}) \wedge \psi(\vec{v})$ is (equivalent in ${}_{\mathcal{R}}T$ to) a pp-formula.

2. Let $\varphi(\vec{v}, \vec{z})$ be a pp-formula of L_R, $\varphi(\vec{v}, \vec{z}) : \exists \vec{w}\,(A\,{}^t(\vec{v}, \vec{z}) = B\,\vec{w})$. Then $\varphi(\vec{v}, \vec{0})$ is a pp-formula, and hence, for every $\mathcal{R}$-module $\mathcal{M}$, $\varphi(\mathcal{M}^n, \vec{0})$ is a pp-definable subgroup of $\mathcal{M}^n$. Furthermore, for every $\vec{a} \in M$, $\varphi(\mathcal{M}^n, \vec{a}) = \emptyset$ or $\varphi(\mathcal{M}^n, \vec{a})$ is a coset of $\varphi(\mathcal{M}^n, 0)$ in M (in fact, given $\vec{b} \in \varphi(\mathcal{M}^n, \vec{a})$, it is easy to check $\varphi(\mathcal{M}^n, \vec{a}) = \varphi(\mathcal{M}^n, 0) + \vec{b}$).

3. Let $\varphi(\vec{v})$, $\psi(\vec{v})$ be pp-formulas of L_R with n free variables, and let k be a positive integer. It is simple to write a sentence in L_R ensuring that, in a given $\mathcal{R}$-module $\mathcal{M}$, the index of $\varphi(\mathcal{M}^n) \cap \psi(\mathcal{M}^n)$ in $\varphi(\mathcal{M}^n)$ is $\geq k$; in detail this sentence says

$$\exists \vec{v}_0 \ldots \exists \vec{v}_{k-1} \left(\bigwedge_{i<k} \varphi(\vec{v}_i) \wedge \bigwedge_{i<j<k} \neg\psi(\vec{v}_i - \vec{v}_j) \right).$$

We will denote it by $(\varphi : \psi) \geq k$. Any sentence of this form is called an *invariant statement* (we will see later the reason why). Notice that the finite Boolean combinations of invariant statements include the sentences saying:

- the index of $\varphi(\mathcal{M}^n) \cap \psi(\mathcal{M}^n)$ in $\varphi(\mathcal{M}^n)$ is k (" $= k$" means " $\geq k$" but " $\not\geq k+1$"); we will denote this formula by $(\varphi : \psi) = k$;
- the index of $\varphi(\mathcal{M}^n) \cap \psi(\mathcal{M}^n)$ in $\varphi(\mathcal{M}^n)$ is $\leq k$ (" $\leq k$" means " $\not\geq k+1$"); we shall denote this formula by $(\varphi : \psi) \leq k$.

At this point we can state and show the following fundamental theorem (of *pp-elimination of quantifiers* for modules).

Theorem 2.6.2 (Baur - Monk) *Let $\mathcal{R}$ be a (countable) ring with identity. Then the pp-formulas of L_R together with the invariant statements form an elimination set for ${}_{\mathcal{R}}T$ in L_R. More precisely: for every formula $\alpha(\vec{v})$ of L_R, there are a Boolean combination β of invariant statements and a Boolean combination $\gamma(\vec{v})$ of pp-formulas such that*

$$\forall \vec{v}(\alpha(\vec{v}) \leftrightarrow \beta \wedge \gamma(\vec{v})) \in {}_{\mathcal{R}}T.$$

We shall use in our proof the following result of group theory.

Lemma 2.6.3 (B. H. Neumann) *Let $\mathcal{G}$ be a group, a, $a_i \in G$, $\mathcal{H}$, $\mathcal{H}_i$ be subgroups of $\mathcal{G}$ (where i ranges among the naturals less than some fixed N), $aH \subseteq \bigcup_{i<N} a_i H_i$. Let I be the set of the naturals $i < N$ for which $|H : H \cap H_i| \leq N!$. Then $aH \subseteq \bigcup_{i \in I} a_i H_i$.*

Now let us begin the proof of the theorem.

Proof. We proceed by induction on $\alpha(\vec{v})$. If $\alpha(\vec{v})$ is an atomic formula, then $\alpha(\vec{v})$ is directly a pp-formula. The cases $\neg$ and $\wedge$ are easy to handle. So suppose that $\alpha(\vec{v})$ is of the form $\forall w \alpha'(w, \vec{v})$, where the induction hypothesis

ensures that there exist an invariant statement β' and a Boolean combination $\gamma'(w, \vec{v})$ of pp-formulas such that

$$\forall w \forall \vec{v}(\alpha'(w, \vec{v}) \leftrightarrow \beta' \wedge \gamma'(w, \vec{v})) \in {}_RT.$$

1^{st} reduction: without loss of generality, $\alpha'(w, \vec{v})$ is a disjunction of pp-formulas or negations. In fact, $\forall \vec{v}(\alpha(\vec{v}) \leftrightarrow \beta' \wedge \forall w \gamma'(w, \vec{v})) \in {}_{\mathcal{R}}T$. Accordingly we can replace $\alpha'(w, \vec{v})$ by $\gamma'(w, \vec{v})$, which is a Boolean combination of pp-formulas, and hence is equivalent to a conjunction of disjunctions of pp-formulas or negations. Correspondingly put $\alpha'(w, \vec{v}) : \bigwedge_{j \leq s} \alpha'_j(w, \vec{v})$ where, for every $j \leq s$, $\alpha'_j(w, \vec{v})$ is a disjunction of pp-formulas or negations. $\forall w \alpha'(w, \vec{v})$ is equivalent in ${}_RT$ to $\bigwedge_{j \leq s} \forall w \alpha'_j(w, \vec{v})$. Then we can handle $\alpha'_j(w, \vec{v})$ (with $j \leq s$) instead of $\alpha'(w, \vec{v})$.
2^{nd} reduction: $\alpha'(w, \vec{v})$ is of the form $\theta(w, \vec{v}) \rightarrow \bigvee_{i<N} \theta_i(w, \vec{v})$ where N is a positive integer, $\theta(w, \vec{v})$ and $\theta_i(w, \vec{v})$ (with $i < N$) are pp-formulas. In fact $\alpha'(w, \vec{v})$ is a single disjunction of pp-formulas and negations. But we know that any conjunction of pp-formulas is (equivalent in ${}_RT$ to) a pp-formula, and hence any disjunction of negations of pp-formulas is the negation of a single pp-formula. This clearly implies our claim.
Let us summarize the situation. We want to find β and $\gamma(\vec{v})$ such that, for every $\mathcal{R}$-module $\mathcal{M}$ and every sequence $\vec{a}$ in M,

$$(1) \qquad \theta(\mathcal{M}, \vec{a}) \subseteq \bigcup_{i<N} \theta_i(\mathcal{M}, \vec{a}).$$

if and only if $\mathcal{M} \models \beta \wedge \gamma(\vec{a})$. We know that, given $\mathcal{M}$ and $\vec{a}$, either $\theta(\mathcal{M}, \vec{a}) = \emptyset$ or $\theta(\mathcal{M}, \vec{a})$ is a coset of the pp-definable subgroup $\theta(\mathcal{M}, \vec{0})$. The same can be said about $\theta_i(\mathcal{M}, \vec{a})$ for every $i < N$. By the way, notice that $\exists w \theta(w, \vec{v})$, $\exists w \theta_i(w, \vec{v})$ (with $i < N$) are pp-formulas. (1) is certainly true when $\vec{a}$ satisfies $\neg \exists w \theta(w, \vec{v})$ (the negation of a pp-formula) in $\mathcal{M}$, and certainly false when $\vec{a}$ satisfies

$$\exists w \theta_i(w, \vec{v}) \wedge \bigvee_{i<N} \neg \exists w \theta_i(w, \vec{v})$$

in $\mathcal{M}$. So there is no loss of generality for our purposes in assuming $\theta(\mathcal{M}, \vec{a}) \neq \emptyset$ and $\theta_i(\mathcal{M}, \vec{a}) \neq \emptyset$ for every $i < N$. Let S be the set of the indices $i < N$ satisfying

$$|\theta(\mathcal{M}, \vec{0}) : \theta(\mathcal{M}, \vec{0}) \cap \theta_i(\mathcal{M}, \vec{0})| \leq N! \, .$$

Notice that S depends on $\mathcal{M}$ (and on $\vec{a}$, of course). However there are only finitely many possible ways of choosing S, and each of them is described by

a suitable invariant statement. Let us assume, with no loss of generality, that S is just the set of the positive integers $\leq m$ for some $m \leq N$. We can apply B. H. Neumann's Lemma and deduce that (1) is equivalent to

$$(2) \qquad \theta(\mathcal{M}, \vec{a}) \subseteq \bigcup_{i<m} \theta_i(\mathcal{M}, \vec{a}).$$

Put $K = \theta(\mathcal{M}, \vec{0}) \cap \bigcap_{i<m} \theta_i(\mathcal{M}, \vec{0})$. As $\theta(\mathcal{M}, \vec{a})$ and $\theta_i(\mathcal{M}, \vec{a})$ for $i < m$ are union of cosets of K in M, (2) can be equivalently written

$$(3) \qquad \theta(\mathcal{M}, \vec{a})/K \subseteq \bigcup_{i<m} \theta_i(\mathcal{M}, \vec{a})/K.$$

As $\theta(\mathcal{M}, \vec{a})/K$ is finite, we can use some (hopefully) well known combinatorial arguments and restate (3) in the equivalent form

$$(4) \quad \sum_X (-1)^{|X|} |(\theta(\mathcal{M}, \vec{a}) \cap \bigcap_{i \in X} \theta_i(\mathcal{M}, \vec{a}))/K| = 0$$

where X ranges over the subsets of $\{0, 1, \ldots, m-1\}$. For every X, put

$$k(X) = |\theta(\mathcal{M}, \vec{0}) \cap \bigcap_{i \in X} \theta_i(\mathcal{M}, \vec{0}) : K|;$$

notice that, when $\theta(\mathcal{M}, \vec{a}) \cap \bigcap_{i \in X} \theta_i(\mathcal{M}, \vec{a}) \neq \emptyset$,

$$k(X) = |(\theta(\mathcal{M}, \vec{a}) \cap \bigcap_{i \in X} \theta_i(\mathcal{M}, \vec{a}))/K|.$$

Moreover $k(X) \leq N!^N$. Hence we have shown that $\mathcal{M}$ satisfies $\alpha(\vec{a})$ if and only if $\sum (-1)^{|X|} k(X) = 0$, where the sum concerns all the subsets X of $\{0, 1, \ldots, m-1\}$ such that $\mathcal{M} \models \exists w(\theta(w, \vec{a}) \wedge \bigwedge_{i \in X} \theta_i(w, \vec{a}))$, and hence if and only if $\mathcal{M}$ satisfies a convenient disjunction of conjunctions of invariant statements and pp-formulas. This is what happens for a given S. As there are only finitely many possible S's, one can find some suitable β and $\gamma(\vec{v})$, valid for every $\mathcal{R}$-module $\mathcal{M}$. ♣

Remark 2.6.4 1. Notice that the procedure given in the proof of Theorem 2.6.3 is effective, and provides explicitly for every $\alpha(\vec{v})$ the required formulas β and $\gamma(\vec{v})$. Furthermore β is actually a finite Boolean combination of invariant statements concerning pp-formulas $\varphi(v)$, $\psi(v)$ (with at most one free variable).

2. In particular, when α is a sentence of L_R, what the previous procedure produces is just a Boolean combination β of invariant statements (concerning pp-formulas $\varphi(v)$, $\psi(v)$ with at most one free variable) such that $\alpha \leftrightarrow \beta \in {}_{\mathcal{R}}T$.

3. Now fix an $\mathcal{R}$-module $\mathcal{M}$. Then, for every formula $\alpha(\vec{v})$ of L_R, there exists a Boolean combination $\gamma(\vec{v})$ of pp-formulas such that $\mathcal{M} \models \forall\vec{v}\,(\alpha(\vec{v}) \leftrightarrow \gamma(\vec{v}))$ (in fact, we know that $\alpha(\vec{v})$ is equivalent to $\beta \wedge \gamma(\vec{v})$ for some Boolean combination $\gamma(\vec{v})$ of pp-formulas and some sentence β; so, if $\mathcal{M} \models \beta$, then $\alpha(\vec{v})$ is equivalent to $\gamma(\vec{v})$, while, if $\mathcal{M} \models \neg\beta$, then $\alpha(\mathcal{M}^n)$ is empty and consequently $\alpha(\vec{v})$ is equivalent to $\delta(\vec{v}) \wedge \neg\delta(\vec{v})$, where $\delta(\vec{v})$ is an arbitrary pp-formula).

With respect to definable sets in modules, this is what Theorem 2.6.3 implies.

Corollary 2.6.5 *Let $\mathcal{M}$ be an $\mathcal{R}$-module, n be a positive integer. Then every set $X \subseteq M^n$ definable in $\mathcal{M}$ is a finite Boolean combination of cosets of pp-definable subgroups.*

Proof. There exist an L_R-formula $\alpha(\vec{v}, \vec{w})$ and a sequence $\vec{a}$ in M such that $X = \alpha(\mathcal{M}^n, \vec{a})$. We can assume that $\alpha(\vec{v}, \vec{w})$ is a Boolean combination of pp-formulas, and we know that, for every pp-formula $\varphi(\vec{v}, \vec{w})$, $\varphi(\mathcal{M}^n, \vec{a})$, when it is not empty, is a coset of the pp-definable subgroup $\varphi(\mathcal{M}^n, \vec{0})$. ♣

We can also characterize the complete extensions of ${}_{\mathcal{R}}T$ (and hence the $\equiv$-classes of $\mathcal{R}$-modules).

Corollary 2.6.6 *Let $\mathcal{M}, \mathcal{M}'$ be two R-modules. Then $\mathcal{M} \equiv \mathcal{M}'$ if and only if, for every choice of two pp-formulas $\varphi(v)$, $\psi(v)$, the indices of $\varphi(\mathcal{M}) \cap \psi(\mathcal{M})$ in $\varphi(\mathcal{M})$ and $\varphi(\mathcal{M}') \cap \psi(\mathcal{M}')$ in $\varphi(\mathcal{M}')$ are either finite and equal, or both infinite.*

Proof. It is clear that, if $\mathcal{M}$ and $\mathcal{M}'$ are elementarily equivalent, then, for every $\varphi(v), \psi(v)$ as before, and for every positive integer k,

$$\mathcal{M} \models (\varphi : \psi) \geq k \quad \Leftrightarrow \quad \mathcal{M}' \models (\varphi : \psi) \geq k.$$

The inverse implication follows from Remark 2.6.4,2. ♣

The previous result explains why "*invariant statements*" are called in this way: actually these sentences fully characterize any $\mathcal{R}$-module $\mathcal{M}$ up to elementary equivalence.

Now let us discuss the content of the previous results in some particular case. We deal with a principal ideal domain $\mathcal{R}$ (this setting includes the ring $\mathbf{Z}$ of integers, as well as any field). First let us examine a generic pp-formula of L_R

$$\alpha(\vec{v}) : \exists \vec{w} \, (A\vec{v} = B\vec{w}).$$

A and B can obtain a simpler form when $\mathcal{R}$ is a principal ideal domain. For, it is a fact of Algebra that, in this framework, there are two invertible matrices X, Y with coefficients in R such that the product $B' = XBY$ is diagonal. So $\alpha(\vec{v})$ is equivalent to

$$\exists \vec{w} \, (XA\vec{v} = B'Y^{-1}\vec{w})$$

and, unless replacing $\vec{w}$ by $Y^{-1}\vec{w}$, A by XA and B by B', one can suppose B diagonal in $\alpha(\vec{v})$. Consequently $\alpha(\vec{v})$ becomes of the form

$$\exists w_1 \ldots \exists w_m \, (\bigwedge_{1 \leq i \leq m} (\sum_{j=1}^{n} a_{ij} v_j = b_{ii} w_i)).$$

Now let us momentarily restrict our analysis to a smaller setting.

Case 1: $\mathcal{R} = \mathcal{K}$ is a field (so we are dealing with vectorspaces over $\mathcal{K}$). Assume that, for some i with $1 \leq i \leq m$, $b_{ii} \neq 0$. Then we can divide the i-th equation in $\alpha(\vec{v})$ by b_{ii} and consequently assume $b_{ii} = 1$. At this point it is easy to show that $\alpha(\vec{v})$ is equivalent to

$$\bigwedge_{1 \leq i \leq m, b_{ii} = 0} (\sum_{j=1}^{n} a_{ij} v_j = 0),$$

which is a conjunction of atomic formulas.

Combine this observation and Baur-Monk's Theorem, and deduce that every L_K-formula is equivalent in ${}_{\mathcal{K}}T$ to a conjunction of a quantifier free formula and a Boolean combination of invariant statements.

Moreover the pp-formulas with a unique free variable v reduce to $rv = 0$ for some $r \in K$, and hence to either $v = 0$ when $r \neq 0$ or to $v = v$ when $r = 0$. Consequently the only pp-definable subgroups of a vectorspace $\mathcal{V}$ are $\{0\}$ and V. Owing to Corollary 2.6.5, the subsets of V definable in $\mathcal{V}$ are just the finite Boolean combinations of the cosets of these subgroups, and so reduce to the finite or cofinite subsets.

Now let us examine invariant statements. In particular we direct our attention on the sentences of the form

$$(\star) \qquad (v = v : v = 0) \geq k$$

where k is a positive integer. In any given vectorspace $\mathcal{V}$ over $\mathcal{K}$, they witness if the size $|V|$ di V is finite or not, and, in the positive case, its value. We claim that they can even determine the $\equiv$-type of the vectorspace. Let us see why.

First assume K infinite. We know that, in this case, all the nonzero vectorspaces over $\mathcal{K}$ are elementarily equivalent (for, their theory is complete). In other words, when K is infinite, there are only two $\equiv$-classes of $\mathcal{K}$-vectorspaces: the former contains all the nonzero vectorspaces, and the latter reduces to the zero space. But a vectorspace $\mathcal{V}$ is $\{0\}$ if and only if $\mathcal{V} \models (v = v : v = 0) = 1$. In particular, the statements $(\star)$ determine the $\equiv$-type of any vectorspace.

Now assume K finite (say of size q). Now we meet infinitely many $\equiv$-classes of $\mathcal{K}$-vectorspaces. In fact, there is a class for every natural n, consisting of the (pairwise isomorphic) vectorspaces of dimension n over $\mathcal{K}$ (hence size q^n), while infinite vectorspaces form again a unique class. The sentences $(v = v : v = 0) \geq k$ can obviously distinguish these classes.

One can deduce that every invariant statement in L_K is a Boolean combination of sentences $(v = v : v = 0) \geq k$ where k ranges over the positive integers.

In conclusion, given a field $\mathcal{K}$, the atomic formulas of L_K together with the invariant statements $(v = v : v = 0) \geq k$, with k a positive integer, form an elimination set for ${}_{\mathcal{K}}T$. In particular this yields quantifier elimination in L_K for the theory of infinite $\mathcal{K}$-vectorspaces.

Case 2: Now let us enlarge our setting to arbitrary principal ideal domains $\mathcal{R}$. First let us examine a pp-formula $\alpha(\vec{v})$. We cannot expect any longer that, whenever $b_{ii} \neq 0$ in the i-th equation of $\alpha(\vec{v})$, one can divide the whole equation by b_{ii} and so obtain $b_{ii} = 1$. However $\alpha(\vec{v})$ is equivalent in ${}_{\mathcal{R}}T$ to a conjunction of formulas

(1) $\sum_{j=i}^{n} a_{ij}v_j = 0$ (for $b_{ii} = 0$),

(2) $\exists w(\sum_{j=i}^{n} a_{ij}v_j = qw)$ (where $q = b_{ii} \neq 0$).

The latter ones are divisibility conditions: we can abbreviate each of them by

(2) $q \mid \sum_{j=i}^{n} a_{ij}v_j$.

Of course, when q is a unit in $\mathcal{R}$, this is a trivial condition and can be forgotten. In the remaining cases, recall that q decomposes (uniquely) as a product of powers of pairwise distinct primes in $\mathcal{R}$, and q divides an element

$r \in R$ if and only if all these prime powers divide r. So there is no loss of generality in assuming that, in (2), q is a prime power.
The situation becomes clearer if we restrict our analysis to formulas having only one free variables. In fact, in this case, our pp-formula $\alpha(v)$ gets equivalent in ${}_{\mathcal{R}}T$ to a conjunction of formulas

(1)' $rv = 0$ (a torsion condition),

(2)' $p^l \mid sv$ (a divisibility condition);

here p, r, $s \in R$, p is a prime and l is a non-negative integer. Again, simple algebraic facts about principal ideal domains let us assume that s itself is a power of p, $s = p^h$ for some non-negative integer $h < l$. Every pp-formula in at most one free variable is a conjunction of torsion and divisibility conditions as before.
This result helps also the analysis of invariant statements $(\varphi(v) : \psi(v)) \geq k$. We avoid here too many details. However we wish to mention the following sentences (r, p are elements of R, p is prime, n, k are positive integers):

(3) $(pv = 0 \wedge p^{n-1}|v : pv = 0 \wedge p^n|v) \geq k$,

(4) $(pv = 0 \wedge p^n|v : v = 0) \geq k$,

(5) $(p^{n-1}|v : p^n|v) \geq k$,

(6) $(v = v : rv = 0) \geq k$.

The reader may check their truth (at least when $\mathcal{R}$ is the ring of integers) in some familiar abelian groups, like $\mathbf{Z}/q^h\mathbf{Z}$, the Prüfer groups $\mathbf{Z}/q^\infty\mathbf{Z}$, the localizations of $\mathbf{Z}$ at q (when q ranges over the primes, and h over the natural numbers), and the additive group of rationals, and realize in this way their meaning.
Indeed Wanda Szmielew (a student of Tarski's) showed that, for every $\mathcal{R}$-module $\mathcal{M}$, the $\equiv$-type of $\mathcal{M}$ is fully determined by the invariant statements (3)-(6) satisfied by $\mathcal{M}$.
In conclusion, owing to Baur-Monk's theorem, the formulas (1)-(6) are an elimination set for the theory ${}_{\mathcal{R}}T$ when $\mathcal{R}$ is a principal ideal domain.

2.7 Strongly minimal theories

We saw in 2.4 that the only (1-ary) definable sets in an algebraically closed field are the finite and cofinite ones. 2.6 told us that the same happens, for

instance, in every (infinite) vectorspace over a fixed countable field. One can also check that even pure sets (in a language with no symbols besides equality $=$) enjoy this feature; again, every definable set is either finite or cofinite (this was implicitly shown when we treated definable sets in 1.7, in particular when we provided an example of an infinite coinfinite non definable set).
So we find some non-trivial algebraic structures $\mathcal{A}$ whose definable 1-ary subsets reduce to the ones definable in the pure set A (with the equality relation $=$) by quantifier free formulas. Let us name these structures in the following way.

Definition 2.7.1 *An infinite structure $\mathcal{A}$ is said to be* **minimal** *if and only if the only definable subsets of A are those finite or cofinite. A complete theory T is said to be* **strongly minimal** *if and only if every model $\mathcal{A}$ of T is minimal.*

Hence any algebraically closed field is a minimal structure, and any theory ACF_p (with $p = 0$ or prime) is strongly minimal. The same is true for infinite vectorspaces, or pure sets.
It should be underlined that the minimality of a structure is not preserved by elementary equivalence. In other words there are minimal structures $\mathcal{A}$ such that the theory of $\mathcal{A}$ is not strongly minimal, and so admits some non-minimal models. Here is an example.

Example 2.7.2 Consider the theory dLO^+ of discrete orders with a least element 0 but no last element. We know that dLO^+ is complete, and has quantifier elimination in a language L with a constant (for 0) and a 1-ary operation symbol (for the successor function s) in addition to the relation symbol $\leq$. Consequently every definable subset of a model of T is a finite Boolean combination of intervals (possibly with an infinite right endpoint). Therefore $(\mathbf{N}, \leq, 0, s)$ is a minimal model of T, because every interval in $(\mathbf{N}, \leq, 0, s)$ is either finite or cofinite. However no other model $\mathcal{A} = (A, \leq, 0^{\mathcal{A}}, s^{\mathcal{A}})$ of T is minimal. In fact, let $a \in A$ satisfy $a \neq (s^{\mathcal{A}})^n(0^{\mathcal{A}})$ for any natural n. Then both $[0^{\mathcal{A}}, a[$ and $[a, +\infty[$ are infinite intervals in $\mathcal{A}$.

We shall examine again strongly minimal theories in the next chapters. In particular, with respect to algebraically closed fields, we will prove a theorem of Macintyre showing (among other things) that the only integral domains with indentity having a strongly minimal complete theory are just the algebraically closed fields.

2.8 o-minimal theories

Turning now to linearly ordered structures $\mathcal{A} = (A, \leq, \ldots)$, we met in the previous sections some examples where the definable subsets of A reduce to the finite unions of intervals (possibly with infinite endpoints) in $(A, \leq)$. This is what happens in real closed fields (as observed in 2.5), but also in dense or discrete (infinite) linear orders (see the sections 2.2 and 2.3). This suggests the following definition.

Definition 2.8.1 *An infinite linearly ordered structure $\mathcal{A} = (A, \leq, \ldots)$ is called* **o-minimal** *if and only if every subset of A definable in $\mathcal{A}$ is a finite union of intervals (closed or open, possibly with infinite endpoints). A complete theory T of infinite linearly ordered structures is called* **o-minimal** *if and only if every model of T is o-minimal.*

"o" abridges "order", of course. This o-minimal setting clearly reminds minimality. In fact the minimal structures (and the strongly minimal theories) are the ones where every definable (1-ary) set is already defined by a quantifier free formula involving the only (language) symbol $=$. Similarly the o-minimal structures (and theories) are just those admitting a total order relation $\leq$ such that every definable (1-ary) is already defined by a quantifier free formula involving the only (language) symbol $\leq$.
In this sense the o-minimal structures and theories are the simplest ones in the presence of a total order relation. Nevertheless they include several non-trivial algebraic examples. We will study in more detail these structures and theories in the last chapter of this book.
But it is worth emphasizing since now that, in spite of the similarities underlined above between minimality and o-minimality, a relevant difference arises. In fact, we noticed that the theory of a minimal structure may admit some non-minimal models, and so fail to be strongly minimal. This does not happen in the o-minimal setting. In fact the following theorem hold.

Theorem 2.8.2 (Knight - Pillay - Steinhorn) *If T is the theory of a linearly ordered o-minimal structure, then every model of T is o-minimal.*

Accordingly, we can spare the adverb "strongly" in defining a theory with o-minimal models.
Coming back to real closed fields, we would like to mention here a result quite similar to the one recalled at the end of the previous section on algebraically closed fields. In fact, it was shown by Pillay and Steinhorn that the only

ordered rings (with identity) having an o-minimal theory are the real closed fields.
The proofs of these theorems will be provided in Chapter 9.

2.9 Computational aspects of q. e.

In this section we shortly discuss the quantifier elimination procedures with respect to effectiveness and fastness. Actually these criteria did not correspond to the spirit of the forties (and some decades later), when the main quantifier elimination results were proved. For, those times lived the influence of Gödel incompleteness and undecidability phenomena; so, according to that feeling, any decision algorithm (such as Tarski's method for real elementary algebra), or even a decidability theorem simply ensuring the existence of such a procedure without explicitly exhibiting it, were exactly the best answer one might expect. But later, in the seventies, the birth of modern computers and the beginning of their science changed this setting and inspired a prevalent interest in quickly running algorithms. Hence complexity theory introduced

⋆ the class P of the problems having a fast procedure to find solutions,

⋆ the class NP of the problems having a fast procedure to verify solutions (namely to check that a solution works).

We agree that a problem has a solving procedure when there is a Turing machine handling it and that an algorithm is fast when it runs in a polynomial time with respect to the length of the input. To realize the difference between finding or verifying solutions, look at the problem of factoring integers. To decompose a natural number ≥ 2 into its prime factors -more precisely, to find these factors- can be significantly slower (at least with respect to the currently available algorithms) than to check this decomposition when done. Just to quote a famous historical example, F. Cole announced during an AMS meeting in 1903 that the Mersenne number $2^{67} - 1$ is not prime. Factoring $2^{67} - 1$ is not easy (and certainly it was not in 1903, when computers were not available). But Cole's proof is quite short to write and needs only one line

$$2^{67} - 1 = 193797721 \times 761838257287$$

and can be checked very quickly.

Coming back to P and NP, it is trivial to observe that $P \subseteq NP$, because a procedure yielding solutions implicitly confirms these solutions. A fundamental problem in complexity theory (and, more generally, in the area linking computer science and mathematics) asks whether $P = NP$, hence whether, whenever a problem has a fast procedure verifying solutions, then it admits a (possibly slower but still) fast (=polynomial) procedure finding solutions.
According to the new spirit, what is primary even in quantifier elimination, mainly towards decidability, is to get fast methods. Let us discuss this feature for the elimination of quantifiers of real closed fields: this is perhaps the most interesting case, owing to its connection with elementary geometry. However a devastating result of Fischer and Rabin shows

Theorem 2.9.1 *Any algorithm deciding, or even verifying membership to RCF for sentences in the language of ordered fields requires a running time at least exponential with respect to the length of the input sentence.*

Algorithm still means Turing machine. Notice that Fischer-Rabin's Theorem only refers to the additive structure of the reals $(\mathbf{R}, +, -)$; recall that, in this restricted language, the reals inherit in an obvious way a structure of $\mathbf{Q}$-vectorspace, because the scalar multiplication by any rational can be defined using $+$, and so form a structure elementarily equivalent to $(\mathbf{C}, +, -)$. In this sense, the theorem applies also to the complex field, yielding the same negative lower bound for the decision procedures concerning algebraically closed fields.
By the way, it is not known any decidable theory with infinite models and a decision procedure running in polynomial time. Indeed, if such a theory exists, then $P = NP$.
In particular, Tarski's original elimination procedure is very inefficient and slow. However, recently faster and more powerful elimination methods for real closed fields have been introduced. We wish to quote the Collins procedure, called *cylindrical algebraic decomposition CAD*, working in the worst cases in a doubly exponential time with respect to the number of variables in the input formula. Implementations of CAD, and other real quantifier elimination methods are discussed, for instance, in [33].

But now we want to treat briefly another intriguing relationship between complexity theory and quantifier elimination (for arbitrary theories and structures). A few lines ago we have said *algorithm = Turing machine*, in accordance with the Church-Turing Thesis. But the Turing model of computation has an intrinsic discrete character, so that its applications to

a continous framework (like $\mathbf{R}$ or $\mathbf{C}$) seem laborious and unnatural (however, see [121] for a discussion of this point). Consequently, new models of computation, including real and complex numbers as possible inputs, and even working in arbitrary structures, have been introduced. We quote the Blum-Shub-Smale BSS model ([14], [13]), or also the Poizat approach [133]. These new perspectives extend the Turing point of view: the classical computability is just the computability over the field $\mathbf{F}_2$ with 2 elements; but now computability over arbitrary structures is allowed. In particular, for every structure $\mathcal{A}$, one can define in a suitable sense the classes P and NP (over $\mathcal{A}$), one can compare these classes and check if $P = NP$ over $\mathcal{A}$. To introduce these matters in detail would require a long time, so we refer the interested reader to the bibliography quoted at the end of the chapter. Remarkably, quantifier elimination arises in this setting. In fact, Poizat observed

Theorem 2.9.2 *If $P = NP$ over $\mathcal{A}$, then the theory of $\mathcal{A}$ eliminates the quantifiers.*

It is comparatively easy to realize why. Let us refer for simplicity to the Cole example quoted before. To prove that $2^{67} - 1$ is composite requires to find a non trivial divisor, and hence to obtain some witnesses of the (existential) sentence $\exists u \exists v (2^{67} - 1 = uv)$. But, after Cole, we have simply to check the quantifier free sentence

$$2^{67} - 1 = 193797721 \times 761838257287.$$

In other words, what $P = NP$ asks here is a procedure (indeed a quick procedure) of elimination of quantifiers. Theorem 2.9.2 provides several examples of structures for which $P \neq NP$. For instance, recall the Macintyre-McKenna-Van den Dries theorems characterizing the infinite fields whose theory eliminates the quantifiers in the language for fields (they are the algebraically closed fields), or the ordered fields whose theory eliminates the quantifiers in the language for ordered fields (the real closed fields). One easily deduces

Corollary 2.9.3 *1. $P \neq NP$ over the field of rationals, or over the field of reals (without the order relation).*

2. $P \neq NP$ over the ordered field of rationals.

On the other side, quantifier elimination is only a necessary condition towards $P = NP$ over a given structure. There do exist quantifier eliminable

structures $\mathcal{A}$ such that $P \neq NP$ over $\mathcal{A}$: this is the content of the following nice result of Meer.

Theorem 2.9.4 *$P \neq NP$ over $(\mathbf{R}, +, -)$.*

In fact the theory of $(\mathbf{R}, +, -)$ is essentially the theory of nonzero vectorspaces over the rational field, and so admits the elimination of quantifiers in the language $L_{\mathbf{Q}}$ and even in $\{+, -\}$ because the action of any rational is easily defined by the additive structure without using quantifiers.
What can we say about the complex field, or the ordered field of reals? Their theories eliminate the quantifiers in the corresponding language. Nevertheless $P = NP$ is still an open question over these structures. Notably, in the complex case, a key (NP-complete) problem towards a definitive answer is related to the celebrated Hilbert Nullstellensatz (a classical algebraic result closely related to Model Theory, as we will see in the next chapter): in fact, it asks a quick procedure checking the solvability of a given finite system of polynomials over $\mathbf{C}$ (in arbitrarily many variables). One shows that $P = NP$ over the complex field if and only if this fast procedure exists. NP-complete problems over the ordered field of reals are discussed in the references quoted below.

2.10 References

Van den Dries [168] and Doner-Hodges [34] are two excellent and enjoyable expository papers, explaining Tarski's work on the quantifier elimination and, more generally, the history of this matter. They also include a rich list of references. Here let us mention [87] and [154] on the pioneeristic contributions of Löwenheim and Skolem to the elimination of quantifiers. Langford's elimination methods for dense or discrete orders are in [81] and in [82], while Tarski's subsequent contributions in this setting are in [160]. Tarski's elimination procedures for the real field and the complex field are given in [157], while Cohen's method in the real case is in [27]. [98] contains the Macintyre-McKenna-Van den Dries theorems saying that algebraically closed fields are the only infinite fields whose first order theory eliminates the quantifiers, and real closed fields are the only ordered fields with the same feature. Let us mention that R. Thom coined the word "semialgebraic" in [162].
Some more details about pp-elimination in modules (and a proof of Neumann's Lemma 2.6.3) can be found in M. Prest's book [136]; the Eklof-Fisher

paper [40] deals with the particular case of abelian groups (and modules over Dedekind domains).
The computational aspects of the quantifier elimination for the real field are discussed in [33], while the cylindrical algebraic decomposition algorithm CAD is in the Collins paper [29]. The Fisher-Rabin theorem ensuring that no decision algorithm for the real field runs in polynomial time is in [47].
[13], [14] describe the new Blum-Shub-Smale model of computation; [133] provides Poizat's approach to this theme. K. Meer's theorem that $P \neq NP$ over $(\mathcal{R}, +, -)$ (although the corresponding theory eliminates the quantifiers) is in [112].