PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 79, Number 1, May 1980

A LINEARLY ORDERED RING WHOSE THEORY ADMITS ELIMINATION OF QUANTIFIERS IS A REAL CLOSED FIELD

L. P. D. VAN DEN DRIES

ABSTRACT. Linearly ordered rings and preordered fields whose first order theory admits quantifier elimination are shown to be real closed fields.

Introduction. An important result of A. Tarski states that the elementary theory of a real closed ordered field admits quantifier elimination. In [1] the following converse of Tarski's theorem was proved: an ordered field whose elementary theory admits quantifier elimination is real closed. In this note we strengthen this converse to the statement of the title. We also generalize in another direction (see Remark 2).

Conventions. Rings are assumed to be associative with unit 1, and are considered as L-structures with $L = \{+, \cdot, -, 0, 1\}$. A linearly ordered ring is by definition a structure $(R, \leqslant)$ with R a ring and $\leqslant$ a linear order on R such that for all $a, b, c \in R$:

$$a \leqslant b \Rightarrow a + c \leqslant b + c, \qquad (a \leqslant b \text{ and } c \geqslant 0) \Rightarrow ac \leqslant bc.$$

To avoid the trivial case we will also assume that $0 \neq 1$. It follows that the linearly ordered ring $(\mathbf{Z}, \leqslant)$ is uniquely embedded in any linearly ordered ring. A linearly ordered ring is considered as an $L(\leqslant)$-structure, where $L(\leqslant) = \{+, \cdot, -, 0, 1, \leqslant\}$.

The following easy lemma is basic.

LEMMA. *Let $\phi(x)$ be an open $L(\leqslant)$-formula in one free variable x, and let $(R, \leqslant)$ be a linearly ordered ring. Then there is $n \in \mathbf{N}$ such that*

$$\begin{array}{ll} \textit{either} & \forall r \in R(r \geqslant n \Rightarrow (R, \leqslant) \models \phi(r)) \\ \textit{or} & \forall r \in R(r \geqslant n \Rightarrow (R, \leqslant) \models \neg\phi(r)). \end{array}$$

PROOF. The property stated for $\phi(x)$ is clearly preserved under taking boolean combinations, so it suffices to consider the case that $\phi(x)$ is a formula $p(x) \geqslant 0$, where $p(x) \in \mathbf{Z}[X]$. If $p(x)$ is the zero polynomial, the first alternative holds with $n = 1$, so suppose $p(x) = a_d x^d + \cdots + a_0$, $a_d, \ldots, a_0 \in \mathbf{Z}$, $a_d \neq 0$, say $a_d > 0$ (the case $a_d < 0$ is treated similarly).

Then we show that the first alternative holds for n any integer larger than $\max(|a_0|, \ldots, |a_d|)$: let $r \geqslant |a_i| + 1$ for $i = 0, \ldots, d$. Then by induction on $i \leqslant d$

Received by the editors February 28, 1979.
AMS (MOS) subject classifications (1970). Primary 02G20; Secondary 02H05, 06A70, 12J15.

$$r^i \geqslant |a_{i-1}|r^{i-1} + \cdots + |a_0| + 1. \qquad (*)$$

This is trivially true for $i = 0$. So suppose $i < d$ and $(*)$ holds. Then

$$r^{i+1} = r \cdot r^i \geqslant (|a_i| + 1) \cdot r^i = |a^i|r^i + r^i$$
$$\geqslant |a^i|r^i + |a_{i-1}|r^{i-1} + \cdots + |a_0| + 1.$$

So $(*)$ is proved for $i \leqslant d$. Taking $i = d$ in $(*)$ we get

$$a_d r^d \geqslant r^d \geqslant |a_{d-1}|r^{d-1} + \cdots + |a_0| + 1 > a_{d-1}r^{d-1} + \cdots + a_0,$$

so $p(r) > 0$, for all $r \geqslant \max(|a_0|, \ldots, |a_d|) + 1$. □

THEOREM. *Let $(R, \leqslant)$ be a linearly ordered ring such that* $\mathrm{Th}(R, \leqslant)$ *admits elimination of quantifiers. Then $(R, \leqslant)$ is a real closed ordered field.*

PROOF. By Theorem 2 of [1], mentioned in the introduction, we have only to show that R is a (commutative) field. Let $Z(x)$ be an open $L(\leqslant)$-formula defining the centre $Z(R)$ of R, i.e. $(R, \leqslant) \models Z(x) \leftrightarrow \forall y(yx = xy)$. Because $\mathbf{N} \subset Z(R)$, the lemma implies that there is $n \in \mathbf{N}$ such that $\forall r \geqslant n$, $r \in Z(R)$. Given any $r \in R$ we have either $r + n \geqslant n$ (if $r \geqslant 0$), so $r + n \in Z(R)$, or $-r + n \geqslant n$ (if $r \leqslant 0$), so $-r + n \in Z(R)$, and in both cases it follows that $r \in Z(R)$, hence R is commutative.

Similarly, let $\mathrm{sq}(x)$ be an open $L(\leqslant)$-formula defining the set of squares $\mathrm{sq}(R)$ of R, i.e. $(R, \leqslant) \models \mathrm{sq}(x) \leftrightarrow \exists y(y^2 = x)$. Because $n \leqslant n^2$ for $n \in \mathbf{N}$, the lemma implies:

(1) there is $M_1 \in \mathbf{N}$ such that $\forall r \in R(r \geqslant M_1 \Rightarrow r \in \mathrm{sq}(R))$.

For $n \geqslant M_1$, let $\sqrt{n}$ be a positive solution of $x^2 = n$ in R. Then $(\sqrt{n+1} + \sqrt{n})(\sqrt{n+1} - \sqrt{n}) = 1$, but the invertible element $\sqrt{n+1} + \sqrt{n}$ takes values larger than any natural number as n varies over the natural numbers $\geqslant M_1$.

So again the lemma implies:

(2) there is $M_2 \in \mathbf{N}$ such that $\forall r \in R(r \geqslant M_2 \Rightarrow r$ is invertible in $R)$.

In particular M_2 is invertible, and if $r \geqslant 1$, then $rM_2 \geqslant M_2$, so by (2) rM_2 is invertible, which by the preceding remark implies that r is invertible. So we may even assume that $(\mathbf{Q}, \leqslant) \subset (R, \leqslant)$, and a similar argument as above shows

(3) each $r \in R$ with $|r| \geqslant q$ for some positive rational q is invertible.

We will now show

(4) each noninvertible element of R is nilpotent.

Suppose that r is not invertible and $r > 0$ (so r is infinitesimal by (3)), and let $p(x) \in \mathbf{Z}[x] - \{0\}$, say $p(x) = a_d x^d + \cdots + a_e x^e$ with $d \geqslant e$, $a_d, \ldots, a_e \in \mathbf{Z}$, $a_d \neq 0$, $a_e \neq 0$.

Then $p(r) = r^e(a_d r^{d-e} + \cdots + a_e)$ and $a_d r^{d-e} + \cdots + a_e$ is infinitely close to a_e, so is invertible by (3). Hence

$p(r) > 0 \Leftrightarrow a_e > 0$ *and* $r^e \neq 0$,

$p(r) = 0 \Leftrightarrow r^e = 0$,

$p(r) < 0 \Leftrightarrow a_e < 0$ *and* $r^e \neq 0$.

But the noninvertibles in R can be defined by an open $L(<)$-formula which may be taken as a disjunction of formulas

$$p_1(x) = \cdots = p_k(x) = 0 \wedge q_1(x) > 0 \wedge \cdots \wedge q_l(x) > 0,$$

with $k + l > 0, p_1, \ldots, p_k, q_1, \ldots, q_l, \mathbf{Z}[x] \setminus \{0\}$.

So r has to realize such a disjunction. Combining this fact with the above observation leads to:

r is nilpotent or each sufficiently small positive rational number is not invertible in R. Using (3) we obtain that r is nilpotent, and we have finished the proof of (4).

Before taking the final step in the proof, i.e. (5), we need some preparations. Let p be some prime number larger than M_2 and let $\sqrt{p}$ be the unique positive solution in R of $x^2 = p$, which exists by (2), and is unique, because, if $r > 0$, then $(\sqrt{p} + r)^2 = p + 2r\sqrt{p} + r^2 > p$. Replacing $(R, <)$, if necessary, by a suitable elementary extension, we may assume that R contains an *invertible* infinitesimal δ, i.e. $|\delta| < q$ for each rational $q > 0$.

Now we can prove

(5) R has no nilpotent other than zero.

Suppose that R has a nilpotent $\neq 0$. Then there is $\varepsilon > 0$ in R with $\varepsilon^2 = 0$. Consider now the two ordered subrings $(\mathbf{Z}[\varepsilon, \varepsilon \cdot \sqrt{p}\,], <)$ and $(\mathbf{Z}[\varepsilon, \varepsilon \cdot (\sqrt{p} + \delta)], <)$ of $(R, <)$. Each element of $\mathbf{Z}[\varepsilon, \varepsilon \cdot \sqrt{p}\,]$ can be written uniquely in the form $a + b\varepsilon + c\varepsilon\sqrt{p}$ with $a, b, c \in \mathbf{Z}$, and similarly an element of $\mathbf{Z}[\varepsilon, \varepsilon \cdot (\sqrt{p} + \delta)]$ equals $a + b\varepsilon + c\varepsilon(\sqrt{p} + \delta)$ for a unique triple $(a, b, c) \in \mathbf{Z}^3$. For such $a, b, c \in \mathbf{Z}$ we have

$$\begin{aligned} a + b\varepsilon + c\varepsilon\sqrt{p} > 0 &\Leftrightarrow a > 0 \text{ or } \big(a = 0 \text{ and } b + c\sqrt{p} > 0\big) \\ &\Leftrightarrow a > 0 \text{ or } \big(a = 0 \text{ and } b + c\big(\sqrt{p} + \delta\big) > 0\big) \\ &\Leftrightarrow a + b\varepsilon + c\varepsilon\big(\sqrt{p} + \delta\big) > 0. \end{aligned}$$

This argument shows that there is an isomorphism of $(\mathbf{Z}[\varepsilon, \varepsilon \cdot \sqrt{p}\,], <)$ onto $(\mathbf{Z}[\varepsilon, \varepsilon \cdot (\sqrt{p} + \delta)], <)$ mapping ε and $\varepsilon\sqrt{p}$ onto ε and $\varepsilon(\sqrt{p} + \delta)$, respectively. By assumption there is an open formula $\psi(y, z)$ such that $(R, <) \models \psi(y, z) \leftrightarrow \exists x(x^2 = p \wedge xy = z)$. Then it follows from $(R, <) \models \psi(\varepsilon, \varepsilon\sqrt{p}\,)$ and the above isomorphism that $(R, <) \models \psi(\varepsilon, \varepsilon(\sqrt{p} + \delta))$. But this means that $\varepsilon\sqrt{p} = \varepsilon(\sqrt{p} + \delta)$, so $\varepsilon\delta = 0$, contradicting $\varepsilon \neq 0$ and the invertibility of δ. So (5) is proved.

It is clear that (4) and (5), together with the commutativity of R, imply that R is a field. $\square$

Remarks.

(1) Improving at some points the proof of the theorem we see that in fact the following is true.

Let $(R, <)$ *be a linearly ordered ring. Then* A *and* B *below are equivalent*:

A. $(R, <)$ is a euclidean ordered field, i.e. an ordered field such that $\{r \in R \mid r \geqslant 0\} = \mathrm{sq}(R) \overset{\text{def}}{=} \{r^2 \mid r \in R\}$.

B. The centre $Z(R)$ of R, $\mathrm{sq}(R)$, the set of invertible elements of R are each definable by an open $L(\leqslant)$-formula, and the formula $\exists x(x^2 = 2 \wedge xy = z)$ is equivalent to an open $L(\leqslant)$-formula with respect to $\mathrm{Th}(R, \leqslant)$.

That the last condition in B cannot be omitted is shown by the following example: endow $\mathbf{R}[X]$ with the linear order $\leqslant$ which extends the usual order on $\mathbf{R}$ and makes X a positive infinitesimal.

Let $R = \mathbf{R}[X]/(X^2)$ and endow R with the linear order $\leqslant$ making the canonical map $\mathbf{R}[X] \to R$ a morphism of $(\mathbf{R}[X], \leqslant)$ onto $(R, \leqslant)$. Then R is not a field, but $Z(R)$, $\mathrm{sq}(R)$, and the set of invertible elements of R are each definable by an open $L(\leqslant)$-formula.

(2) We can extend Theorem 2 of [1] also in another direction: recall that a preordered field is a structure $(K, \leqslant)$ with K a field and $\leqslant$ a (partial) order on K such that for all $a, b, c \in K$:

$$0 \leqslant a^2, \quad a \leqslant b \Rightarrow a + c \leqslant b + c, \quad \text{and} \quad (a \leqslant b \wedge c \geqslant 0) \Rightarrow ac \leqslant bc.$$

Then we have

A preordered field $(K, \leqslant)$ with the property that $Th(K, \leqslant)$ admits elimination of quantifiers is real closed.

Sketch of proof. The lemma and its proof go through for $(K, \leqslant)$. As in the proof of the theorem one can then show that for some $M \in \mathbf{N}$ each $r \geqslant M$ is a square, from which one easily derives (using multiplication with a suitable square) that each $r \geqslant 0$ is a square. Similarly, one shows that each $r \geqslant 0$ is a fourth power. Now, given any $r \in K$, one can then write $r^2 = s^4$ for some $s \in K$, so $r = s^2$ or $r = -s^2$, i.e. $r \geqslant 0$ or $r \leqslant 0$. Hence the preorder is a linear order, and we are reduced to Theorem 2 of [1].

I thank M. Boffa for reviving my interest in the subject.

References

1. A. Macintyre, K. McKenna and L. van den Dries, *Quantifier elimination in algebraic structures*, Advances in Math. (to appear).

Department of Mathematics, University of Utrecht, Utrecht, The Netherlands

Current address: Department of Mathematics, Yale University, New Haven, Connecticut 06520