

AMALGAMATION AND ELIMINATION OF QUANTIFIERS FOR THEORIES OF FIELDS¹

WILLIAM H. WHEELER

ABSTRACT. The universal theories of integral domains and of ordered integral domains which have the amalgamation property are characterized via their existentially complete models. The results of A. Macintyre, K. McKenna, and L. van den Dries on fields and ordered fields whose complete theories permit elimination of quantifiers are then derived as easy corollaries.

A. Macintyre, K. McKenna, and L. van den Dries [5] have shown that the only theories of fields which permit elimination of quantifiers (in their natural languages) are those which previously had been known to do so. Namely, the only infinite fields whose theories permit elimination of quantifiers are the algebraically closed fields. The only ordered fields whose theories permit elimination of quantifiers are the real closed ordered fields. Analogous statements hold for valued fields, formally p -adic fields, and formally π -adic fields. These assertions are converses to well-known results of A. Tarski and A. Robinson and more recent results of A. Macintyre.

The purpose of this paper is to show that these converses follow from more general results concerning which universal theories of integral domains have the amalgamation property. For the case of ordinary fields, the crux of the matter is that if a universal theory T of integral domains has the amalgamation property, then the infinite, existentially complete models of T are algebraically closed. The result on elimination of quantifiers then follows from the connection between amalgamation and elimination of quantifiers and from standard facts about model-companions.

§1 contains preliminary information and the connection between amalgamation and elimination of quantifiers. §2 considers the case of fields and integral domains. §3 considers the case of ordered fields and ordered integral domains. §4 contains comments on the other cases and also raises a question for further investigation. Not surprisingly the proofs in §§2 and 3 use some of the techniques developed in [5].

Received by the editors July 31, 1978.

AMS (MOS) subject classifications (1970). Primary 02H05, 02H15, 02G20; Secondary 12L99.

Key words and phrases. Theories of fields, elimination of quantifiers, amalgamation, algebraically closed fields, real closed order fields.

¹The results in this paper were presented to the Association for Symbolic Logic in December 1977 [10].

© 1979 American Mathematical Society
0002-9939/79/0000-0515/\$03.00

1. Preliminaries. The symbols x, y and z will be used both as variable symbols in first order languages and as variables for forming polynomials over rings. The symbols a, b, c, r, s, t, α and β will be used both as constant symbols in first order languages and as symbols to denote elements of structures with the convention that b as a constant symbol is assigned to the element b of a structure. The notation $\phi(\mathbf{x})$ for a formula ϕ indicates that the free variable of ϕ are among x_1, \dots, x_n .

The reader is referred to [2] and [3] for relevant facts about model-companions and existentially complete structures.

A first order theory T has the *amalgamation property* if whenever a model \mathfrak{M} of T is a submodel of models \mathfrak{M}_1 and \mathfrak{M}_2 of T , then there is a model \mathfrak{M}_3 of T and embeddings f of \mathfrak{M}_1 into \mathfrak{M}_3 and g of \mathfrak{M}_2 into \mathfrak{M}_3 such that $f(a) = g(a)$ for each element a of \mathfrak{M} .

P. Bacsich [1] has shown that a universal theory T has the amalgamation property if and only if whenever $\phi(\mathbf{x})$ is an existential formula, $\psi(\mathbf{x})$ is a universal formula, and $T \vdash \forall \mathbf{x}(\phi \rightarrow \psi)$, then there is a quantifier free formula $\chi(\mathbf{x})$ such that $T \vdash \forall \mathbf{x}(\phi \rightarrow \chi)$ and $T \vdash \forall \mathbf{x}(\chi \rightarrow \psi)$.

The following lemma is essential to this paper.

LEMMA 1.1. *Assume that T is a universal theory with the amalgamation property. For each universal formula $\psi(\mathbf{x})$, let $\Delta = \Delta(\psi) = \{\chi(\mathbf{x}): \chi \text{ is quantifier free and } T \vdash \forall \mathbf{x}(\chi \rightarrow \psi)\}$. If \mathfrak{M} is an existentially complete model of T , then $\mathfrak{M} \models \forall \mathbf{x}(\psi \leftrightarrow \bigvee \Delta)$, where $\bigvee \Delta$ denotes the possibly infinite disjunction of the formulas in Δ .*

PROOF. Let $\Delta' = \{\phi(\mathbf{x}): \phi \text{ is existential and } T \vdash \forall \mathbf{x}(\phi \rightarrow \psi)\}$. Let \mathfrak{M} be an existentially complete model of T . It is well known (see the proof of Proposition 6.1(i) in [3]) that $\mathfrak{M} \models \forall \mathbf{x}(\psi \leftrightarrow \bigvee \Delta')$. For each ϕ in Δ' there is a χ in Δ such that $T \vdash \forall \mathbf{x}(\phi \rightarrow \chi)$ and $T \vdash \forall \mathbf{x}(\chi \rightarrow \psi)$. Hence $\mathfrak{M} \models \forall \mathbf{x}(\psi \leftrightarrow \bigvee \Delta)$.

Since each formula in Δ may be put into disjunctive normal form, one may assume, and hereafter it will be assumed, that each formula in $\Delta(\psi)$ is a conjunction of atomic formulas and negated atomic formulas.

The set of universal formulas deducible from a theory T will be denoted by T_{\forall} and will be called the universal subtheory of T .

The following proposition (noted independently by L. van den Dries [9]) follows readily from P. Bacsich's result or from results of A. Robinson and L. Blum [7].

PROPOSITION 1.2. *The following are equivalent for a first order theory T :*

- (1) T permits elimination of quantifiers;
- (2) T satisfies the submodel condition [8, §5.5] and T_{\forall} has the amalgamation property.

2. Theories of fields and integral domains. In this section, the first order language \mathcal{L} will have nonlogical symbols $0, 1, +, -, \cdot$.

THEOREM 2.1. *Assume that S is a universal theory of integral domains,*

$S \vdash \neg(0 = 1)$, and S has the amalgamation property. If \mathfrak{M} is an existentially complete model of S , then \mathfrak{M} is either a finite field or an algebraically closed field.

PROOF. If \mathfrak{M} is finite, then it is a field since every finite integral domain is a field. Assume then that \mathfrak{M} is infinite. Then \mathfrak{M} has an extension which is existentially complete for S and which contains an infinite set of elements which are algebraically independent over the quotient field K of the prime subring R of \mathfrak{M} (take a suitable ultrapower of \mathfrak{M} and then extend to an existentially complete model of S). Now \mathfrak{M} is algebraically closed if this extension is, so one may assume without loss of generality that \mathfrak{M} itself contains such a set of elements.

SUBLEMMA 2.2. *If $\psi(\mathbf{x})$ is a universal formula, a_1, \dots, a_n are elements of \mathfrak{M} which are algebraically independent over K , and $\mathfrak{M} \models \neg\psi(\mathbf{a})$, then $\mathfrak{M} \models \neg\psi(\mathbf{b})$ whenever b_1, \dots, b_n are algebraically independent over K .*

PROOF OF SUBLEMMA. According to Lemma 1.1, $\mathfrak{M} \models \forall \mathbf{x}(\psi \leftrightarrow \bigvee \Delta(\psi))$ and by assumption each formula in $\Delta(\psi)$ is a conjunction of atomic formulas and negated atomic formulas. Now each atomic formula has the form $p(\mathbf{x}) = 0$ where $p(\mathbf{x})$ is a polynomial with integer coefficients. Since $\mathfrak{M} \not\models \chi(\mathbf{a})$ for any $\chi \in \Delta(\psi)$, each χ in $\Delta(\psi)$ has a conjunct $p(\mathbf{x}) = 0$ where $p(\mathbf{x})$ is a nontrivial polynomial. Therefore, $\mathfrak{M} \not\models \chi(\mathbf{b})$ for any χ in $\Delta(\psi)$, so $\mathfrak{M} \models \neg\psi(\mathbf{b})$.

PROOF OF 2.1 (CONTINUED).

(1) Each transcendental element of \mathfrak{M} has an n th root in \mathfrak{M} for each $n > 2$. To verify this, let $t \in \mathfrak{M}$ be transcendental and apply Sublemma 2.2 to the formula $\forall y(\neg y^n = x)$ and the element t^n .

(2) Each transcendental element of \mathfrak{M} has a multiplicative inverse. To verify this, let $\psi(x)$ be the formula $\forall y \neg(xy = 1)$. Let t be a transcendental element of \mathfrak{M} . Then $t^2 + 1$ is transcendental, so it has a square root s by (1). Then $(s + t)(s - t) = s^2 - t^2 = t^2 + 1 - t^2 = 1$. Also $s + t$ is transcendental, so one can apply Sublemma 2.2 to ψ and $s + t$.

(3) Each nonzero element of \mathfrak{M} has a multiplicative inverse. To show this, let $0 \neq a \in \mathfrak{M}$ and let t be an element of \mathfrak{M} which is transcendental over the quotient field of $R[a]$. Then at is transcendental, so by (2) it has an inverse s . Then $a(ts) = 1$. Hence \mathfrak{M} is a field.

(4) Each element of \mathfrak{M} has an n th root for each $n > 2$. Let $0 \neq a \in \mathfrak{M}$ and let t be an element of \mathfrak{M} which is transcendental over the quotient field of $R[a]$. Then at^n is transcendental, so it has an n th root s , i.e., $s^n = at^n$. Then $(st^{-1})^n = a$. Thus \mathfrak{M} is perfect.

(5) If elements b_1, \dots, b_n of \mathfrak{M} are algebraically independent over K , then the polynomial $y^n + b_1y^{n-1} + \dots + b_n$ has a zero in \mathfrak{M} . To prove this, let t_1, \dots, t_n be elements of \mathfrak{M} which are algebraically independent over K . Let $s_1(\mathbf{x}) = x_1 + \dots + x_n, \dots, s_n(\mathbf{x}) = x_1 \cdot \dots \cdot x_n$ be the elementary symmetric functions. Then

$$\prod_{i=1}^n (y - t_i) = y^n + (-1)s_1(\mathbf{t})y^{n-1} + \cdots + (-1)^n s_n(\mathbf{t}).$$

The elements $-s_1(\mathbf{t}), \dots, (-1)^n s_n(\mathbf{t})$ are algebraically independent over K . Thus, one can apply Sublemma 2.2 to the formula

$$\forall y \neg (y^n + x_1 y^{n-1} + \cdots + x_n = 0)$$

and the elements $-s_1(\mathbf{t}), \dots, (-1)^n s_n(\mathbf{t})$.

(6) \mathfrak{M} is algebraically closed. Suppose not. Then there is an $\alpha \in \tilde{\mathfrak{M}} - \mathfrak{M}$, where $\tilde{\mathfrak{M}}$ is the algebraic closure of \mathfrak{M} . Let n be the degree of an irreducible polynomial of α over \mathfrak{M} , and let $\alpha = \alpha_1, \dots, \alpha_n$ be the distinct conjugates of α over \mathfrak{M} (recall that \mathfrak{M} is perfect by (4)). Let t_1, \dots, t_n be elements of \mathfrak{M} which are algebraically independent over the quotient field L of the subring of \mathfrak{M} generated by the prime subring and the coefficients of the monic irreducible polynomial for α over \mathfrak{M} . Let

$$\begin{aligned} f(y, \mathbf{t}) &= \prod_{i=1}^n (y - (t_1 + t_2 \alpha_i + \cdots + t_n \alpha_i^{n-1})) \\ &= y^n + g_1(\mathbf{t})y^{n-1} + \cdots + g_n(\mathbf{t}). \end{aligned}$$

In the proof of Theorem 1 of [5], it is shown in essence that $g_1(\mathbf{t}), \dots, g_n(\mathbf{t})$ are elements of \mathfrak{M} and are algebraically independent over L and hence over K . Therefore, by (5), there is a $c \in \mathfrak{M}$ such that $f(c, \mathbf{t}) = 0$, so $c = t_1 + t_2 \alpha_i + \cdots + t_n \alpha_i^{n-1}$ for some i , $1 \leq i \leq n$. But this contradicts that α has degree n over \mathfrak{M} , for α must have the same degree as its conjugate α_i and α_i cannot have degree n over \mathfrak{M} if $c = t_1 + t_2 \alpha_i + \cdots + t_n \alpha_i^{n-1}$ is in \mathfrak{M} . Hence, \mathfrak{M} is algebraically closed.

COROLLARY 2.3. *If T is a theory of integral domains in the language \mathcal{L} , $T \vdash \neg(0 = 1)$, T permits elimination of quantifiers, and \mathfrak{M} is a model of T , then \mathfrak{M} is either a finite field or an algebraically closed field. Moreover, if \mathfrak{M} is a finite field, then it is the only model of T of its characteristic.*

PROOF. Since T permits elimination of quantifiers, T_{\forall} has the amalgamation property. Furthermore, T is the model-companion of T_{\forall} , so each model of T is an existentially complete model of T_{\forall} . The main conclusion now follows from Theorem 2.1. If moreover \mathfrak{M} is finite, then it cannot be embedded in any larger model of T . Yet since T_{\forall} has amalgamation, \mathfrak{M} can be jointly embedded with any other model of T of the same characteristic as \mathfrak{M} into a third model of T . Hence \mathfrak{M} must be the only model of T of its characteristic.

COROLLARY 2.4 (A. MACINTYRE [4], B. ROSE [6]). *If \mathfrak{M} is an integral domain and the complete theory of \mathfrak{M} in the language \mathcal{L} permits elimination of quantifiers, then \mathfrak{M} is either a finite field or an algebraically closed field.*

3. Theories of ordered fields and ordered integral domains. In this section the first order language \mathcal{L} will have nonlogical symbols $0, 1, +, -, \cdot, <$.

THEOREM 3.1. *Assume that S is a universal theory of ordered integral domains, $S \vdash \neg(0 = 1)$, and S has the amalgamation property. If \mathfrak{M} is an existentially complete model of S , then \mathfrak{M} is a real closed field.*

PROOF. \mathfrak{M} has characteristic 0 and so is infinite. By forming a suitable ultrapower of \mathfrak{M} and then extending to an existentially complete model of S if necessary, one may assume that \mathfrak{M} contains an infinite set V of elements which are algebraically independent over the rational numbers Q and have the property that the integers Z are not cofinal in the subring $Z[t]$ for any $t \in V$. An element s of \mathfrak{M} will be called positive infinite if $s > n$ for each $n \in Z$. An element s of \mathfrak{M} will be called an infinitesimal if $0 < s < 1/n$ for all $n \in Z$ or if $-1/n < s < 0$ for all $n \in Z$.

SUBLEMMA 3.2. *If $\psi(x)$ is a universal formula, $a \in \mathfrak{M}$ is positive infinite (or positive infinitesimal) and $\mathfrak{M} \vdash \neg\psi(a)$, then $\mathfrak{M} \vDash \neg\psi(b)$ for each positive infinite (positive infinitesimal, respectively) $b \in \mathfrak{M}$.*

PROOF OF SUBLEMMA. As before, $\mathfrak{M} \vDash \forall x(\psi \leftrightarrow \bigvee \Delta(\psi))$ and each formula in $\Delta(\psi)$ is a quantifier free conjunction. In the case of ordered integral domains, the conjuncts can be assumed to have the form $p(x) = 0$ or $0 < q(x)$ where $p(x)$ and $q(x)$ are polynomials with integer coefficients. Since $\mathfrak{M} \not\vDash \psi(a)$, each formula χ in $\Delta(\psi)$ has a conjunct $p(x) = 0$ for a nontrivial polynomial $p(x)$ or a conjunct $0 < q(x)$ where the coefficient of the highest power of x in q (the coefficient of the least power of x in q with a nonzero coefficient when a is positive infinitesimal) is negative. Hence, if b is positive infinite (positive infinitesimal, respectively), then $\mathfrak{M} \not\vDash \chi(b)$ for any χ in $\Delta(\psi)$, so $\mathfrak{M} \vDash \neg\psi(b)$.

PROOF OF THEOREM 3.1 (CONTINUED).

(1) Each positive infinite element has an n th root for each $n \geq 2$. To verify this, let $t \in \mathfrak{M}$ be positive infinite, and apply the sublemma to the formula $\forall y \neg(y^n = x)$ and the element t^n .

(2) Each infinite element has a multiplicative inverse. To verify this, let t be a positive infinite element. Then $t^2 + 1$ is positive infinite and so by (1) has a square root s which is positive infinite. Then $s + t$ is positive infinite and $(s + t)(s - t) = 1$. Now apply the sublemma to the formula $\forall y \neg(xy = 1)$ and the element $s + t$.

(3) Each nonzero, noninfinitesimal element has a multiplicative inverse. To prove this, let $b \neq 0$ be a noninfinitesimal element. If b is negative, then one can replace b by $-b$ to obtain a positive element. Let t be a positive infinite element. Then bt is positive infinite so it has an inverse c . Then $b(tc) = 1$.

(4) Each infinitesimal element has a multiplicative inverse. To show this, let $\psi(x)$ be the formula $\forall y \neg(xy = 1)$. Suppose that b is a positive infinitesimal and $\mathfrak{M} \vDash \psi(b)$. Then there is a $\chi(x)$ in $\Delta(\psi)$ for which $\mathfrak{M} \vDash \chi(b)$. Since b is

positive infinitesimal, χ has only conjuncts of the form $p(x) = 0$ for the trivial polynomial $p(x)$ and the form $0 < q(x)$ where the coefficient of the least power of x with a nonzero coefficient (including possibly the zeroth power) is positive. Then there is a positive rational number r close to zero such that $\mathfrak{N} \models \chi(r)$, but then $\mathfrak{N} \models \psi(r)$ contradicting (3) that r has a multiplicative inverse. Hence $\mathfrak{N} \models \neg\psi(b)$. Therefore each positive infinitesimal and so each infinitesimal have multiplicative inverses.

(5) Each positive element has a square root. To verify this, let b be a positive element. If b is infinitesimal, then one may replace b by b^{-1} . Let t be a positive infinite element. Then bt^2 is positive infinite and so has a square root by (1). Then $(st^{-1})^2 = b$.

(6) If $t_1, \dots, t_n \in \mathfrak{N}$ are algebraically independent over Q and n is odd, then the polynomial $y^n + t_1 y^{n-1} + \dots + t_n$ has a zero in \mathfrak{N} . Suppose this is false. Then there are algebraically independent elements t_1, \dots, t_n for which $\mathfrak{N} \models \psi(\mathbf{t})$ where $\psi(\mathbf{x})$ is the formula

$$\forall y \neg (y^n + x_1 y^{n-1} + \dots + x_n = 0).$$

There is a formula $\chi(\mathbf{x})$ in $\Delta(\psi)$ for which $\mathfrak{N} \models \chi(\mathbf{t})$. As before, χ may be assumed to be a conjunction of formulas of the form $p(\mathbf{x}) = 0$ and $0 < q(\mathbf{x})$ since S is a theory of ordered integral domains. Moreover, for each conjunct of the form $p(\mathbf{x}) = 0$ the polynomial $p(\mathbf{x})$ must be trivial. Let $0 < q_i(\mathbf{x})$ for $i = 1, \dots, k$ be the remaining conjuncts of χ , so

$$\mathfrak{N} \models \bigwedge_{i=1}^k 0 < q_i(\mathbf{t}).$$

Then the real closure $\overline{\mathfrak{N}}$ of \mathfrak{N} satisfies $\exists \mathbf{x} (\bigwedge_{i=1}^k 0 < q_i(\mathbf{x}))$ so the real closure \overline{Q} of Q satisfies $\exists \mathbf{x} (\bigwedge_{i=1}^k 0 < q_i(\mathbf{x}))$. Clearly,

$$\mathfrak{U} = \left\{ (b_1, \dots, b_n) \in \overline{Q}^n : \overline{Q} \models \bigwedge_{i=1}^k 0 < q_i(\mathbf{b}) \right\}$$

is an open set in \overline{Q}^n . Let $(b_1, \dots, b_n) \in \mathfrak{U}$. Let $\beta \in \overline{Q}$ be a zero of $y^n + b_1 y^{n-1} + \dots + b_n = h(y, \mathbf{b})$, so that

$$h(y, \mathbf{b}) = (y - \beta)(y^{n-1} + c_1 y^{n-2} + \dots + c_{n-1})$$

for some $c_1, \dots, c_{n-1} \in \overline{Q}$. Choosing rational numbers $\beta', c'_1, \dots, c'_{n-1}$ sufficiently close to $\beta, c_1, \dots, c_{n-1}$, respectively, and setting

$$\begin{aligned} h(y, \mathbf{b}') &= y^n + b'_1 y^{n-1} + \dots + b'_n \\ &= (y - \beta')(y^{n-1} + c'_1 y^{n-2} + \dots + c'_{n-1}), \end{aligned}$$

one has that $(b'_1, \dots, b'_n) \in \mathfrak{U}$. Then $\mathfrak{N} \models \chi(b'_1, \dots, b'_n)$ so $\mathfrak{N} \models \psi(\mathbf{b}')$, but this contradicts that $y^n + b'_1 y^{n-1} + \dots + b'_n$ has the zero β' in \mathfrak{N} . Hence, $y^n + t_1 y^{n-1} + \dots + t_n$ has a zero in \mathfrak{N} .

(7) \mathfrak{N} is real closed. Suppose that $a_1, \dots, a_n \in \mathfrak{N}$, n is odd, and $y^n + a_1 y^{n-1} + \dots + a_n$ does not have a zero. Then proceeding as in step

(6) in the proof of Theorem 2.1, one obtains a contradiction. Hence \mathfrak{M} is real closed.

COROLLARY 3.3. *If T is a theory of ordered integral domains, $T \vdash \neg(0 = 1)$ and T permits elimination of quantifiers, then each model of T is a real closed ordered field.*

PROOF. The proof is analogous to that of Corollary 2.3.

COROLLARY 3.4 (A. MACINTYRE, K. MCKENNA, AND L. VAN DEN DRIES [5]). *If \mathfrak{M} is a nontrivial, ordered integral domain and the complete theory of T in the language \mathcal{L} permits elimination of quantifiers, then \mathfrak{M} is a real closed ordered field.*

4. Remarks. Theorems 5 and 6 of [5] concerning formally p -adic integral domains and π -adic integral domains whose theories permit elimination of quantifiers can be proved in a manner analogous to 3.1–3.4.

The theory of valued fields is the only remaining case in [5] as yet unmentioned here. In view of the preceding results, it seems reasonable that if T is a theory of valued integral domains (or more technically, integral domains with a linear divisibility relation as in [5]) and T has the amalgamation property, then the existentially complete models of T are algebraically closed, valued fields. However, this remains unproved because of technical difficulties in proving Lemma 11 of [5] in the absence of an analogue of Lemma 9 of [5].

B. Rose [6] has proved several results concerning rings (not necessarily commutative or domains of integrity) whose theories permit elimination of quantifiers. It would be interesting to know whether there are corresponding results on rings whose universal subtheories have the amalgamation property as in the cases discussed in this paper.

NOTE ADDED IN PROOF. B. Rose has pointed out that in the proof of Theorem 2.1, if \mathfrak{M} has characteristic 2, then part (2) must be modified as follows: Let s be a cube root of $t^3 + 1$. Then $(s - t)(s^2 + ts + t^2) = 1$. The element $s - t$ is transcendental, because t is a zero of the polynomial $(x + (s - t))^3 - x^3 - 1$. Therefore, one can apply Sublemma 2.2 to the ψ of part (2) and the element $s - t$.

BIBLIOGRAPHY

1. P. Bacsich, *Amalgamation properties and interpolation theorems for equational theories*, Algebra Universalis 5 (1975), 45–55.
2. G. Cherlin, *Model theoretic algebra—selected topics*, Lecture Notes in Math., vol. 521, Springer-Verlag, Berlin, 1976.
3. J. Hirschfeld and W. H. Wheeler, *Forcing, arithmetic, division rings*, Lecture Notes in Math., vol. 454, Springer-Verlag, Berlin, 1975.
4. A. Macintyre, *On ω_1 -categorical theories of fields*, Fund. Math. 71 (1971), 1–25.
5. A. Macintyre, K. McKenna and L. P. D. van den Dries, *Elimination of quantifiers in algebraic structures* (to appear).

6. B. Rose, *Rings which admit elimination of quantifiers*, J. Symbolic Logic **43** (1978), 92–112.
7. G. Sacks, *Saturated model theory*, W. A. Benjamin, Inc., Reading, Mass., 1972.
8. J. R. Shoenfield, *Mathematical logic*, Addison-Wesley Publishing Co., Reading, Mass., 1967.
9. L. P. D. van den Dries, *Model theory of fields*, Dissertation, Utrecht, 1978.
10. W. H. Wheeler, *Amalgamation, elimination of quantifiers, and theories of fields*, Abstract, J. Symbolic Logic (to appear).

DEPARTMENT OF MATHEMATICS, INDIANA UNIVERSITY, BLOOMINGTON, INDIANA 47401