Algebraically Closed Fields with Distinguished Subfields

By

Moshe Jarden *)

There is a strong feeling among field theorists that every elementary statement which can be made about a field and its algebraic closure can be reformulated in terms of the field itself. Thus, the statement that a polynomial $f(x_1, \ldots, x_n)$ with coefficients in a field K is irreducible over the algebraic closure, $\tilde{K}$, of K (i.e. f is absolutely irreducible) is known to be equivalent to an elementary statement about K alone. In this note we make this feeling precise and we prove it. From now on the field theorists can freely use the algebraic closure of a field when they make elementary statements about the field and they do not have to make efforts to translate their statements into the language of the field itself. Use of this principle will be made in a later paper.

Let p be either a prime number or zero. Consider the prime field F_p of characteristic p and let $t_1, t_2, t_3, \ldots$ be a sequence of algebraically independent elements over F_p. Put $K_p = F_p(t_1, t_2, t_3, \ldots)$. Then every denumerable field of characteristic p is isomorphic to a subfield of $\tilde{K}_p$. By the Skolem-Löwenheim theorem every field is elementarily equivalent to a denumerable field (c.f. Bell and Slomson [2], p. 82). It follows that the collection, I, of all elementarily equivalent classes (for all characteristics) is a set of cardinallity $\leqq 2^{\aleph_0}$. From [4, § 7] it follows that $|I| \geqq 2^{\aleph_0}$. Hence $|I| = 2^{\aleph_0}$. We choose for every $i \in I$ a representative K_i.

Let $\mathscr{L}$ be the first order language of the theory of fields. For every sentence Θ of $\mathscr{L}$ we write

$$A(\Theta) = \{i \in I \mid K_i \models \Theta\}.$$

Then $A(\Theta)$ does not depend on the specific representatives K_i. If Θ is another sentence of $\mathscr{L}$, then

$$A(\Theta \vee \Theta') = A(\Theta) \cup A(\Theta') \quad \text{and} \quad A(\sim \Theta) = I - A(\Theta).$$

It follows that the set of all $A(\Theta)$ is a sub-boolean algebra $\mathscr{A}$, of the boolean algebra of all subsets of I, and the map $\Theta \mapsto A(\Theta)$ is an epimorphism of the boolean algebra of the sentences of $\mathscr{L}$ onto $\mathscr{A}$.

We add now a new unary predicate symbol P to $\mathscr{L}$ and denote the new language by $\mathscr{L}(P)$. Models of $\mathscr{L}(P)$ will be written as pairs (K', K), where K' is the domain and K is the subset which corresponds to P. We shall be primarily interested in

*) This work was done while the author was in Heidelberg University.

the case where K' is an algebraically closed field, K is a subfield and $[K' : K] = \infty$. In accordance with this convention we choose, for every $i \in I$, an algebraically closed extension, K_i', of K_i such that $[K_i' : K_i] = \infty$. For every sentence Λ of $\mathscr{L}(P)$ we write

$$B(\Lambda) = \{i \in I \mid (K_i', K_i) \models \Lambda\}.$$

Then $B(\Lambda)$ does not depend on the K_i' and K_i. This follows from the following theorem, which is a combination of two theorems of A. Robinson and a theorem of J. Keisler (see [5], p. 71, II, IV and theorem A).

Keisler-Robinson-Theorem. *Let K, L be fields and let K', L' be respectively, algebraically closed extension of them such that $[K' : K] = \infty$ and $[L' : L] = \infty$. Then*

$$K \equiv L \Rightarrow (K', K) \equiv (L', L)$$

($\equiv$ denotes elementary equivalence).

Our main theorem is the following.

Theorem 1. *If Λ is a sentence of $\mathscr{L}(P)$, then $B(\Lambda) \in \mathscr{A}$. In other words, there exists a sentence Θ of $\mathscr{L}$ such that for every field K and for every algebraically closed infinite extension K' of K we have*

$$K \models \Theta \Leftrightarrow (K', K) \models \Lambda.$$

Proof. Assume that $B(\Lambda) \notin \mathscr{A}$. Then there exist two ultra-filters $\mathscr{D}_1$ and $\mathscr{D}_2$ of I such that

(1) $$D_1 \cap \mathscr{A} = \mathscr{D}_2 \cap \mathscr{A},$$

(2) $$B(\Lambda) \in \mathscr{D}_1 - \mathscr{D}_2.$$

(see Ax [1], p. 256). Put $F_j = \prod_{i \in I} K_i/\mathscr{D}_j$ and $F_j' = \prod_{i \in I} K_i'/\mathscr{D}_j$, $j = 1, 2$; then $F_1 \equiv F_2$ (by (1)), the F_j' are algebraically closed and $[F_j' : F_j] = \infty$. Hence, by the Keisler-Robinson Theorem

(3) $$(F_1', F_1) \equiv (F_2', F_2).$$

On the other hand we have, by (2), that $(F_1', F_1) \models \Lambda$ and $(F_2', F_2) \models \Lambda$, which is in contradiction to (3).

For decision procedures in field theory it is important to give a computable version of theorem 1. In order to do this we denote by Π that set of sentences of $\mathscr{L}(P)$ which expresses the fact that K is a field, K' is an algebraically closed extension of K and that $[K' : K] = \infty$. The last of these three statements is equivalent by the Artin-Schreier theorem to the statement $[K' : K] \geqq 3$ (c. f. Lang [6], p. 223) and this is elementarily expressed, for example, by the following sentence:

$$\exists X_1 \exists X_2 \exists X_3 \forall Y_1 \forall Y_2 \forall Y_3 \left[\bigwedge_{i=1}^{3} P(Y_i) \wedge \sum_{i=1}^{3} Y_i X_i = 0 \rightarrow \sum_{i=1}^{3} Y_i = 0 \right].$$

Theorem 2. *There exists a recursive procedure which enables us to find in a finite number of steps, for a given sentence Λ of $L(P)$, a sentence Θ of $\mathscr{L}$ such that (*) holds.*

Proof. Theorem 1 asserts that there exists a Θ which satisfies (*). Let $R(\Theta)$ be the sentence of $\mathscr{L}(P)$ which is obtained from Θ by restricting the range of all the variables of Θ to P (c. f. Keisler [5], p. 79 for a precise definition).

Then

$$K \models \Theta \Leftrightarrow (K', K) \models R(\Theta).$$

Hence, by (*), $\Pi \models R(\Theta) \leftrightarrow \Lambda$, i.e. $R(\Theta) \leftrightarrow \Lambda$ is true in every model of Π. Hence, by the Gödel completeness theorem $\Pi \vdash R(\Theta) \leftrightarrow \Lambda$, i.e. $R(\Theta) \leftrightarrow \Lambda$ is formally provable from Π.

We now order all the proofs of $\mathscr{L}(P)$ from Π in a sequence (e.g. by Cantor's diagonal method) and examine them one by one. After a finite number of steps we shall hit a proof of a sentence of the form $R(\Theta) \leftrightarrow \Lambda$, where Θ' is a sentence of $\mathscr{C}$. Θ' will satisfy (*).

We can now combine previous results with theorems 1 and 2 to get some immediate corollaries.

Denote by $P(\mathbb{Q})$ the set of all prime numbers, with its associated Dirichlet density δ. Furthermore, let $\mathscr{G}(\tilde{\mathbb{Q}}/\mathbb{Q})$ be the Galois group of $\tilde{\mathbb{Q}}$ over $\mathbb{Q}$, with its normalized Haar measure μ with respect to Krull topology. The fixed field of an element $\sigma \in \mathscr{G}(\tilde{\mathbb{Q}}/\mathbb{Q})$ is denoted by $\tilde{\mathbb{Q}}(\sigma)$. For a sentence Λ of $\mathscr{L}(P)$ we denote

$$C(\Lambda) = \{p \in P(\mathbb{Q}) \mid (F_p', F_p) \models \Lambda\},$$

$$D(\Lambda) = \{\sigma \in \mathscr{G}(\tilde{\mathbb{Q}}/\mathbb{Q}) \mid (\tilde{\mathbb{Q}}(\sigma)', \tilde{\mathbb{Q}}(\sigma)) \models \Lambda\}$$

then we have the following theorem.

Theorem 3. (a) *$C(\Lambda)$ has a Dirichlet density $\delta(C(\Lambda))$. If $C(\Lambda)$ is an infinite set, then $\delta(C(\Lambda))$ is a positive rational number.*

(b) *The set $D(\Lambda)$ is measurable and we have $\delta(C(\Lambda)) = \mu(D(\Lambda))$.*

(c) *The theory of all sentences Λ of $\mathscr{L}(P)$ which are true in all the pairs (F', F) where F is a finite field and F' is an algebraically closed extension of F (similarly, in all the pairs (F_p', F_p), in almost all the pairs (F_p', F_p), etc.) is decidable.*

Proof. (a) and (b) follow from Theorem 3.17 of [3] and Theorem 1; (c) follows from Ax ([1], p. 264) and Theorem 2.

Remarks. 1) P. Roquette noted (in a private discussion with the author) that Theorem 1 can also be interpreted topologically. Indeed we define two topologies T_1 and T_2 on I, the bases of which are the sets $A(\Theta)$ and $B(\Lambda)$, where Θ and Λ are sentences of $\mathscr{L}$ and $\mathscr{L}(P)$ respectively. Both T_1 and T_2 are Hausdorff and compact and their open-closed sets are exactly the $A(\Theta)$ and $B(\Lambda)$ respectively. For each Θ of $\mathscr{L}$ we have $A(\Theta) = B(R(\Theta))$, hence the two topologies coincide. In particular, if Λ is a sentence of $\mathscr{L}(P)$, then $B(\Lambda)$ is also open and closed in T_1, i.e. there exists a sentence Θ of $\mathscr{L}$ such that $B(\Lambda) = A(\Theta)$, as Theorem 1 claims.

2) The procedure which is established in Theorem 2 for finding for a given Λ of $\mathscr{L}(P)$ a Θ of $\mathscr{L}$ such that $B(\Lambda) = A(\Theta)$, is recursive but not primitive recursive.

Thus we are not able to give in advance an upper bound for the number of steps which are necessary in order to find Θ. Can one give a primitive recursive procedure for this problem ?

References

[1] J. Ax, The elementary theory of finite fields. Ann. of Math. 88, 239–271 (1968).
[2] J. L. Bell and A. B. Slomson, Models and ultraproducts. Amsterdam 1969.
[3] M. Jarden, Elementary statements over large algebraic fields. Trans. Amer. Math. Soc. **164**, 67–91 (1972).
[4] M. Jarden, Algebraic extension of finite co-rank of hilbertian fields. Israel J. Math. **18**, 279–307 (1974).
[5] H. J. Keisler, Complete theories of algebraically closed fields with distinguished subfields. Michigan Math. J. **11**, 71–81 (1964).
[6] S. Lang, Algebra. Reading 1967.

Eingegangen am 4. 6. 1975

Anschrift des Autors:

Moshe Jarden
Department of Mathematical Sciences
Tel Aviv University
Tel-Aviv, Israel