PACIFIC JOURNAL OF MATHEMATICS
Vol. 62, No. 2, 1976

PSEUDOFINITE FIELDS, PROCYCLIC FIELDS AND MODEL-COMPLETION

ALLAN ADLER AND CATARINA KIEFE

In this paper, it is shown that the theory of pseudofinite fields is, with respect to a suitable language, the model completion of the theory of procyclic fields. Also, procyclic fields are characterized as the class of relatively algebraically closed subfields of pseudofinite fields.

The first two sections of this paper contain some basic definitions and results necessary for an understanding of the main theorems. These are stated at the end of §1. As is well-known, a model completion of a theory is not determined by the models of the theory alone, but also by the language in which the theory is formulated. This makes the choice of a model-completion rather arbitrary. The advantage of the particular language adopted here for the theory of procyclic fields is that not only does one obtain a model-completion of the theory (Theorem I) but one can recover the models of the theory as the class of all substructures of the models of the model-completion for which the defining axioms of the extended language hold (Theorem 2). This is proved using the results of Ax **[1, 2]** and Jarden **[3]**. It is worth remarking that in this language, the theory of pseudofinite fields has elimination of quantifiers [Kiefe, **4**]. Also, the authors wish to acknowledge that the key idea in the proof of Theorem 2 was inspired by A. Robinson **[6]**.

1. Let τ be a similarity type, L_τ the first-order language of type τ. Given two theories Σ_1 and Σ_2 in L_τ, we recall that Σ_2 is called the *model-completion* of Σ_1 if the following three conditions hold:

(i) any model of Σ_2 is a model of Σ_1.

(ii) any model of Σ_1 can be embedded (as a substructure) into a model of Σ_2.

(iii) if $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are models of Σ_2 having $\mathfrak{C}$ as a common substructure, and if $\mathfrak{C}$ is a model of Σ_1, then $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are elementarily equivalent in the language of $\mathfrak{C}$, i.e., in $L_{\delta,\mathfrak{C}}$ we have $\langle \mathfrak{A}_1, \{c\}_{c\in|\mathfrak{C}|}\rangle \equiv \langle \mathfrak{A}_2, \{c\}_{c\in|\mathfrak{C}|}\rangle$.

It is well-known that model-completion, when it exists, is unique. However, there is no reason to expect model-completion to be "independent of the language", i.e., "preserved under extensions by definitions". In fact, this is not the case for the theories dealt with in this paper.

2. Let K be a field: $\tilde{K}$ will denote the algebraic closure of K, $G(\tilde{K}/K)$ the Galois group of $\tilde{K}$ over K. We recall the following definition:

DEFINITION 1. A field K is called *procyclic* if it is perfect and has at most one extension of each finite degree.

Ordinary field language will be denoted L_τ and consists of the first-order language with equality, two constant symbols (0 and 1) and three funtion symbols $(+, \cdot, -)$. It is easy to check that procyclic fields form an EC_Δ-class with respect to this language; the theory of procyclic fields, i.e., the set of sentences of L_τ satisfied by all procyclic fields will be denoted Σ_1.

DEFINITION 2. A field K is called *pseudofinite* if it is an infinite model of the theory of finite fields, i.e., if K is infinite and every sentence of L_τ which holds in every finite field also holds in K.

Although not crucial to this paper, it is interesting to bear in mind that a purely algebraic description of the class of pseudofinite fields exists: a field F is pseudofinite iff F is perfect, has exactly one extension of each finite degree and every nonempty absolutely irreducible variety over F has an F-rational point (cf. **[2]**).

We will denote by Σ_2 the theory of pseudofinite fields, i.e., the set of sentences in L_τ which hold for every pseudofinite field. Pseudofinite fields again form an EC_Δ-class and in **[2]**, J. Ax gives a recursive axiomatization of Σ_2.

It is now trivial to check that every pseudofinite field is procyclic (since every finite field is). On the other hand, Condition (iii) of the definition of model-completion fails, since Σ_2 is not model-complete (e.g., [**2**, p. 256]). Let us then introduce for every positive integer n an $n+1$-ary predicate symbol ψ_n; $L_{\tau'}$ now denotes the first-order language obtained by adjoining the predicate sysmbols $\{\psi_n\}_{n\in\omega}$ to $L_{\tau'}$. We now consider the following extensions by definitions of Σ_1 and Σ_2:

$$\Sigma_i' = \Sigma_i \cup \{\psi_n(x_0, \cdots, x_n) \leftrightarrow \exists\, y(x_n y^n + \cdots + x_0 = 0) \mid n \in \omega\} \quad (i = 1, 2).$$

The new axioms will be called the defining axioms for the extended language (cf. Introduction).

Thus if $F \models \Sigma_i'$ $(i = 1, 2)$ and $a_0, \cdots, a_n \in F$, $\psi_n(a_0, \cdots, a_n)$ holds in F iff the polynomial $a_0 + a_1 y + \cdots + a_n y^n \in F[y]$ has a root in F.

Observe that all we have done is to require "submodel" to mean "relatively algebraically closed submodel" [**4**, p. 34, Lemma 17]. Similarly, a substructure of a model of Σ_2' is relatively algebraically closed iff it satisfies the defining axioms for the extended language.

We now claim the main result:

THEOREM 1. *Σ_2' is the model-completion of Σ_1.*

In order to prove it, we have to check the three conditions of the model-completion definition:

(i) is trivial, as mentioned before.

(ii) in [**4**, p. 34, Theorem 3] it is shown that Σ_2' admits elimination of quantifiers; hence, by [7, p. 63, Theorem 13.11], Σ_2' is substructure-complete, a condition stronger than the one we want to establish.

(ii) in the present case, we can rephrase this condition as the following:

THEOREM 2. *Every procyclic field is isomorphic to a relatively algebraically closed subfield of a pseudofinite field.*

So, to establish Theorem 1, all we need is to prove Theorem 2.

3. Proof of Theorem 2. Let K be a procyclic field; let p denote the characteristic of K ($p = 0$ or p prime). Let $\mathbf{F}_p$ denote the prime field of K ($\mathbf{F}_0$ just denotes the rational numbers). We break up the proof into four cases:

Case 1. K is a field of absolute numbers, i.e., K is algebraic over $\mathbf{F}_p$.

Case 2. K has finite nonzero transcendence degree over $\mathbf{F}_p$.

Case 3. K has countably infinite transcendence degree over $\mathbf{F}_p$.

Case 4. K has uncountable transcendence degree over $\mathbf{F}_p$ (equivalently, K is uncountable).

The hard case turns out to be Case 2. In fact:

Case 1 has been dealt with by Ax [**2**, p. 262, Theorem 7], when he characterized the fields of absolute numbers of pseudofinite fields as exactly the procyclic absolute numbers fields.

Case 3 can be reduced to Case 2 in the following way: Let $\{t_n\}_{n\in\omega}$ be a transcendence basis for K over $\mathbf{F}_p$. For each n, let K_n be the relative algebraic closure of $\mathbf{F}_p(t_0, t_1, \cdots, t_n)$ in K. Any relatively algebraically closed subfield of a procyclic field is procyclic, hence every K_n is procyclic. By Case 2, for each n, let F_n be pseudofinite field and

$$\varphi_n : K_n \to F_n$$

a homomorphism mapping K_n onto a relatively algebraically closed

subfield of F_n. Let $F = \Pi_{n\in\omega} F_n/D$ be a nonprincipal ultraproduct of the F_n's and

$$\varphi: K \to F$$

the map of K: induced by the φ_n's (an element of K belongs to all but a finite number of the K_n's). F is pseudofinite and it is easy to see that $\varphi(K)$ is relatively algebraically closed in F.

Case 4 is reduced to the previous cases as follows: by Skolem-Lowenheim, let L be a countable field elementarily equivalent to K. Then, it follows by a result of Shelah **[8]**, that K and L have isomorphic ultrapowers; so, in particular, K is isomorphic to a relatively algebraically closed subfield of some ultrapower L^I/D of L. Now, by the previous cases, L is isomorphic to a relatively algebraically closed subfield of a pseudofinite field F; hence L^I/D is isomorphic to a relatively algebraically closed subfield of the pseudofinite field F^I/D.

So the proof of Theorem 2 has been reduced to the following

LEMMA. *Let $\mathbf{F}_p$ denote a prime field of characteristic p ($p \geqq 0$). Let K be a procyclic algebraic extension of the field $\mathbf{F}_p(t_1, \cdots, t_n)$ of rational functions ($n \geqq 1$). Then K is isomorphic to a relatively algebraically closed subfield of a pseudofinite field.*

To prove this lemma, we shall use the following result due to Moshe Jarden [**3**, p. 27, Theorem 3.5]:

"If E is Hilbertian, and $\tilde{E}$ its algebraic closure, then for almost all $\sigma \in G(\tilde{E}/E)$ the fixed field of σ is pseudofinite."

Two remarks are in order:

(1) Hilbertian fields are described in Lang [**5**, Chapter VIII]; in particular, all the fields $\mathbf{F}_p(t_1, \cdots, t_n)$ considered here are Hilbertian (it is crucial that we may assume $n \geqq 1$ if $p > 0$).

(2) $G(\tilde{E}/E)$ becomes a compact group under the Krull topology, so we can define Haar measure on it; the "almost all" of the Jarden result refers to this measure. Naturally, a subset of $G(\tilde{E}/E)$ of Measure 1 is dense in $G(\tilde{E}/E)$.

Proof of Lemma. Let $E = \mathbf{F}_p(t_1, \cdots, t_n)$, $n \geqq 1$, $\mathbf{F}_p$ as above. For $\sigma \in G(\tilde{E}/E)$, let F_σ denote the fixed field of σ in $\tilde{E} = \tilde{K}$. Then, by the Jarden result and the above remarks, the set

$$H = \{\sigma \in G(\tilde{E}/E) \mid F_\sigma \text{ is pseudofinite}\}$$

is dense in $G(\tilde{E}/E)$. Since K is procyclic, there is an automorphism τ of $\tilde{K}$ whose fixed field is K (i.e., $K = F_\tau$); naturally, $\tau \in G(\tilde{E}/E)$. Since H is dense in $G(\tilde{E}/E)$, let $\{\sigma_n\}_{n\in\omega}$ be a sequence of automorphisms such

that $\sigma_n \to \tau$ and for all n F_{σ_n} is pseudofinite. Let D be a nonprincipal ultrafilter on ω, and let $\mathcal{F} = \prod F_{\sigma_n}/D$. We have a natural embedding

$$\nu: E \to \mathcal{F}.$$

Let L denote the relative algebraic closure of $\nu(E)$ in $\mathcal{F}$: we will prove that $K \cong L$. For this, it suffices to prove that a polynomial $f \in E[x]$ has a root in K iff f^ν has a root in L [**1**, p. 172, Lemma 5]: given $f \in E[x]$, let

$$G_f = \{\sigma \in G(\tilde{E}/E) \mid F_\sigma \quad \text{contains a root of } f\}.$$

Claim. Under the Krull topology, G_f is a clopen subset of $G(\tilde{E}/E)$.

Indeed: say F is the splitting field of f over E: $G(\tilde{E}/F)$ is a basic open neighborhood of the identity in $G(\tilde{E}/E)$; now, if $\sigma \in G_f$, $\sigma G(\tilde{E}/F) \subseteq G_f$, so G_f is open. And if $\sigma \notin G_f$, $\sigma G(\tilde{E}/F) \cap G_f = \varnothing$, so G_f is closed. So claim is established.

But now: f has a root in $K \Rightarrow G_f$ is a neighborhood of $\tau \Rightarrow$ all but finitely many $\sigma_n \in G_f$ (since $\sigma_n \to \tau$) $\Rightarrow f$ has a root in all but finitely many $F_{\sigma_n} \Rightarrow f$ has a root in $\mathcal{F} \Rightarrow f^\nu$ has a root in L^n (since such a root is a fortiori algebraic over $\nu(E)$).

Also, since G_f is clopen, so is $G(\tilde{E}/E) - G_f$. Hence: f does not have a root in $K \Rightarrow G(\tilde{E}/E) - G_f$ is a neighborhood of $\tau \Rightarrow$ all but finitely many $\sigma_n \in G(\tilde{E}/E) - G_f \Rightarrow f$ does not have a root in all but finitely many $F_{\sigma_n} \Rightarrow f$ does not have a root in L.

REFERENCES

1. James Ax, *Solving diophantine problems modulo every prime*, Ann. of Math., **85** (1967), 161–183.
2. ———, *The elementary theory of finite fields*, Ann. of Math., **88** (1968), 239–271.
3. S. Shelah, *Every two elementarily equivalent models have isomorphic ultrapowers*, Israel J. Math.
4. Moshe Jarden, *Elementary statements over large algebraic fields*, doctoral thesis, The Hebrew University of Jerusalem (1969).
5. Catarina Kiefe, *On the rationality of a zeta-function of a set definable over a finite field*, doctoral thesis, S.U.N.Y. Stony Brook (1973).
6. Serge Lang, *Diophantine geometry*, Interscience Tracts No. 11 (1962).
7. G. Sacks, Saturated model theory, Benjamin (1972).
8. A. Robinson, Nonstandard Arithmetic, Bull. Amer. Math. Soc., **73** (1967), 818–843.

Received January 1, 1975. The second author was partially supported by NSF Grant No. GP-37492X1.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
AND
UNIVERSITY OF CALIFORNIA, BERKELEY