THE ALGEBRAIC NATURE OF THE ELEMENTARY THEORY OF PRC FIELDS

Moshe Jarden

A field K is **PAC** if every nonempty absolutely irreducible variety V defined over K has a K rational point. Similarly K is **PRC** if each such V has a K-rational point provided it has a simple $\overline{K}$-rational point for every real closure $\overline{K}$ of K.

The elementary theory of algebraic PAC fields determines the elementary theory of all PAC fields. Thus a sentence θ is true in each PAC field of characteristic 0 if it is true in each PAC field which is algebraic over $\mathbb{Q}$ [FJ, Corollary 20.25].

The goal of the present note is to use the methods that lead to this result and the prove the analogous one for PRC fields and for maximal PRC fields. We also prove that the absolute Galois group of a maximal PRC field is a free product of groups of order 2 in the category of pro-2 groups. Conversely each such group is isomorphic to the absolute Galois group of a maximal PRC field.

1. The elementary equivalence theorem for PRC fields.

Let K be a field. An integral domain R that contains K is **regular** (resp. **totally real**) over K if the quotient field of R is regular over K (resp. totally real, i.e., every ordering of K extends to the quotient field).

LEMMA 1: *Let K be an $\aleph_1$-saturated PRC field. Let $R = K[x_1, x_2, \ldots]$ be an integral domain, countably generated, regular and totally real over K. Then there exists a homomorphism $\varphi\colon R \to K$.*

Proof: Let F be the quotient field of R. Denote the ideal of all polynomials in $K[X_1, \ldots, X_n]$ that vanish at $(x_1, \ldots, x_n)$ by I_n. Let $f_{n,1}, \ldots, f_{n,r(n)}$ be a system of genarators for I_n. Then $I_1 \subseteq I_2 \subseteq I_3 \ldots$. Since $K[X_1, \ldots, X_n]/I_n \cong_K K[x_1, \ldots, x_n]$ and $F_n = K(x_1, \ldots, x_n)$ is regular over K, $V(I_n)$ is a variety defined over K. Moreover F_n/K is a totally real extension. Hence, $V(I_n)$ has a simple $\overline{K}$-rational point for each real closure $\overline{K}$ of K [La, p. 282]. Hence there exist elements $a_1, \ldots, a_n \in K$ such that

$$\bigwedge_{i=1}^{n} \bigwedge_{j=1}^{r(i)} f_{ij}(a_1, \ldots, a_i) = 0. \tag{1}$$

By the saturation property of K, there exists a sequence $b_1, b_2, b_3, \ldots$ of elements of K such that $f_{nj}(b_1, \ldots, b_n) = 0$ for each n and j. The map $x_i \mapsto b_i$, $i = 1, 2, 3, \ldots$ extends to a K-homomorphism of R into K. ∎

The embedding lemma for PAC fields ([JK] or [FJ, Lemma 18.2]) and its proof have been generalized to other "pseudo closed" fields in [J1, Lemma 3.1] and by Pop [Po, 5.5]. Cherlin, v.d. Dries and Macintyre's [CDM] modification of the proof of the embedding lemma for PAC fields has been generalized by Ershov [E, Lemma 7] to PRC fields. We repeat the proof of the lemma for PRC fields for the sake of completeness. It is the induction step in the proof of the elementary equivalence theorem for PRC fields, Proposition 3.

Denote the absolute Galois group of a field E by $G(E)$. Denote the set of involutions of a group G by $\mathrm{Inv}(G)$.

LEMMA 2: *Let E and F be field extensions of a common field L. Suppose that E is countable and that F is* PRC *and $\aleph_1$-saturated. Suppose further that there exists a homomorphism φ: $G(F) \to G(E)$ such that $\mathrm{Res}_{\tilde{L}}\varphi(\sigma) = \mathrm{Res}_{\tilde{L}}\sigma$ for each $\sigma \in G(F)$. Then there exists an $\widetilde{L}$-embedding Φ: $\widetilde{E} \to \widetilde{F}$ such that*

$$\Phi(\varphi(\sigma)x) = \sigma\Phi(x), \text{ for each } x \in \widetilde{E} \text{ and each } \sigma \in G(F). \tag{1}$$

Proof: Assume without loss that $\widetilde{E}$ is free and therefore linearly disjoint from $\widetilde{F}$ over $\widetilde{L}$. Then each $\sigma \in G(F)$ uniquely extends to an elment $\widetilde{\sigma} \in \mathcal{G}(\widetilde{E}\widetilde{F}/EF)$ such that

$$\widetilde{\sigma}x = \begin{cases} \sigma x & \text{if } x \in \widetilde{F} \\ \varphi(\sigma)x & \text{if } x \in \widetilde{E}. \end{cases}$$

The map $\sigma \mapsto \widetilde{\sigma}$ is an embedding of $G(F)$ into $\mathcal{G}(\widetilde{E}\widetilde{F}/EF)$ whose inverse is the restriction map. Denote the fixed field of the image of $G(F)$ in $\widetilde{E}\widetilde{F}$ by D. Then res: $\mathcal{G}(\widetilde{E}\widetilde{F}/D) \to G(F)$ is an isomorphism. That is, $D \cap \widetilde{F} = F$ and $D\widetilde{F} = \widetilde{E}\widetilde{F}$.

We show that D is a totally real extension of F. Indeed, let P be an ordering of F. Take an involution ζ of $G(F)$ that induces P on F. Let $\varepsilon = \varphi(\zeta)$. Denote the fixed field of ε (resp. ζ) in $\widetilde{E}$ (resp. $\widetilde{F}$) by $\overline{E}$ (resp. $\overline{F}$). As $\mathrm{Res}_{\tilde{L}}(\varepsilon) = \mathrm{Res}_{\tilde{L}}(\zeta)$ is an involution both fields are real closed. Hence $\overline{EF}(\sqrt{-1}) = \widetilde{E}\widetilde{F}$. Since $\widetilde{\zeta}$ fixes both $\overline{E}$ and $\overline{F}$ it belongs to $\mathcal{G}(\widetilde{E}\widetilde{F}/\overline{EF})$. Since $\widetilde{\zeta}$ is an involution it generates $\mathcal{G}(\widetilde{E}\widetilde{F}/\overline{EF})$. So, $\overline{EF}$ contains D. Since $\overline{E} \cap \widetilde{L} = \overline{F} \cap \widetilde{L}$ a lemma of v.d. Dries [D, p. 75], amalgamates the orderings of $\overline{E}$ and $\overline{F}$ to an ordering of $\overline{EF}$. The restriction of this ordering to D extends P.

Now observe that $\widetilde{E}\widetilde{F}$ is an algebraic extension of D. Hence $\widetilde{E} \subseteq \widetilde{E}\widetilde{F} = D[\widetilde{F}] = \widetilde{F}[D]$. Write each $x \in \widetilde{E}$ as

$$x = \sum f_j d_j, \text{ with } f_j \in \widetilde{F} \text{ and } d_j \in D. \tag{2}$$

As $\widetilde{E}$ is countable, the set D_0 of all d_j appearing in the expressions (2) (one expression for each $x \in \widetilde{E}$) is countable. The integral domain $F[D_0]$ is a regular, totally real, and countably generated extension of F. By Lemma 1, there exists an F-homomorphism $\Psi\colon F[D_0] \to F$. Use the linear disjointness of $F[D_0]$ from $\widetilde{F}$ over F to extend Ψ to an $\widetilde{F}$-homomorphism $\widetilde{\Psi}\colon \widetilde{F}[D_0] \to \widetilde{F}$. It satisfies

$$\widetilde{\Psi}(\widetilde{\sigma} z) = \sigma \widetilde{\Psi}(z), \quad \text{for every } \sigma \in G(F) \tag{3}$$

and for each z that belongs either to $\widetilde{F}$ or to D_0. Therefore (3) is true for each $x \in \widetilde{F}[D_0]$. By definition $\widetilde{E} \subseteq \widetilde{F}[D_0]$. Hence (3) is true for each $x \in \widetilde{E}$.

Let $\Phi = \mathrm{Res}_{\tilde{E}} \widetilde{\Psi}$. Then Φ is an $\widetilde{L}$-embedding of $\widetilde{E}$ into $\widetilde{F}$ that satisfies (1). ∎

Denote the first order language of rings (resp., with a constant symbol for each element of a field L) by $\mathcal{L}(\mathrm{ring})$ (resp. $\mathcal{L}(\mathrm{ring}, L)$).

PROPOSITION 3: *Let E and F be* PRC *fields that contain a common field L. Suppose that there exists an isomorphism $\varphi\colon G(F) \to G(E)$ such that $\mathrm{Res}_{\tilde{L}}\varphi(\sigma) = \mathrm{Res}_{\tilde{L}}\sigma$ for each $\sigma \in G(F)$. Then E is elementarily equivalent to F over L.*

Proof: In each sentence of $\mathcal{L}(\mathrm{ring}, L)$ there appear only finitely many elements of L. We may therefore suppose that L is a countable field. Further, replace E and F by ultrapowers ${}^*E = E^{\mathbb{N}}/\mathcal{D}$ and ${}^*F = F^{\mathbb{N}}/\mathcal{D}$. By [FJ, Lemma 18.4], $\varphi^{\mathbb{N}}/\mathcal{D}$ induces an isomorphism ${}^*\varphi\colon G({}^*F) \to G({}^*E)$ such that $\mathrm{Res}_{\tilde{L}}\varphi(\sigma) = \mathrm{Res}_{\tilde{L}}\sigma$ for each $\sigma \in G({}^*F)$. By [P1, Thm. 4.1] both ${}^*E$ and ${}^*F$ are PRC. By [FJ, Lemma 6.14], they are $\aleph_1$-saturated. So, without loss assume that E and F are PRC and $\aleph_1$-saturated.

Use the Skolem-Löwenheim theorem [FJ, Proposition 6.4] to construct a countable elementary subfield E_1 of E that contains L. Let $\overline{\varphi}$ be the map $\varphi \circ \mathrm{Res}\colon G(F) \to G(E_1)$. By Lemma 2, there exists an $\widetilde{L}$-embedding $\Phi_1\colon \widetilde{E}_1 \to \widetilde{F}$ such that $\Phi_1(\overline{\varphi}(\sigma)x) = \sigma\Phi_1(x)$ for each $x \in \widetilde{E}_1$ and $\sigma \in G(F)$. Let $E_1' = \Phi_1(E_1)$. If $x \in E_1$ and $\sigma \in G(F)$, then $\overline{\varphi}(\sigma) \in G(E_1)$. Hence $\sigma\Phi_1(x) = \Phi_1(\overline{\varphi}(\sigma)x) = \Phi_1(x)$. It follows that $E_1' \subseteq F$.

Let $\varphi_1\colon G(E_1') \to G(E_1)$ be the isomorphism induced by Φ_1. It satisfies

$$\Phi_1(\varphi_1(\overline{\sigma})x) = \overline{\sigma}\Phi_1(x)$$

for each $\overline{\sigma} \in G(E_1')$ and $x \in \widetilde{E}_1$. In particular, for $\sigma \in G(F)$, $\overline{\sigma} = \mathrm{Res}_{\widetilde{E_1'}}\sigma$ and $x \in \widetilde{E}_1$ we have $\Phi_1(\varphi(\sigma)x) = \sigma\Phi_1(x) = \Phi_1(\varphi_1(\overline{\sigma})x)$. Hence $\mathrm{Res}_{\tilde{E}_1}\varphi(\sigma) = \varphi_1(\overline{\sigma})$.

Use the Skolem-Löwenheim theorem once more to construct a countable elementary subfield F_1 of F that contains E_1'. Exchange the roles of E and F, use the preceding paragraph and identify $\widetilde{E}_1$ and $\widetilde{E_1'}$ via Φ_1. Then apply Lemma 2 to extend $\Phi_1^{-1}\colon \widetilde{E_1'} \to \widetilde{E}_1$ to an embedding $\Psi_1\colon \widetilde{F}_1 \to \widetilde{E}$ such that $\Psi_1(\varphi^{-1}(\tau)y) = \tau\Psi_1(y)$ for each $y \in \widetilde{F}_1$ and $\tau \in G(E)$.

Continue in this manner by induction to construct two towers of fields $L \subseteq E_1 \subseteq F_1' \subseteq E_2 \subseteq F_2' \subseteq \cdots \subseteq E$ and $L \subseteq E_1' \subseteq F_1 \subseteq E_2' \subseteq F_2 \subseteq \cdots \subseteq F$, and to construct for each i isomorhisms $\Phi_i\colon \widetilde{E}_i \to \widetilde{E_i'}$ and $\Psi_i\colon \widetilde{F}_i \to \widetilde{F_i'}$ such that $\Phi_i(E_i) = E_i'$, $\Psi_i(F_i) = \widetilde{F}_i'$, E_i is a countable elementary subfield of E and F_i is a countable elementary subfield of F. Moreover Ψ_i extends Φ_i^{-1} and Φ_{i+1} extend Ψ_i^{-1}, $i = 1, 2, 3, \ldots$. Let $E_\omega = \bigcup_{i=1}^\infty E_i$ and $F_\omega = \bigcup_{i=1}^\infty F_i$. Then E_ω (resp., F_ω) is an elementary subfield of E (resp., F) [FJ, Lemma 6.3(b)]. Also, $E_\omega \cong_L F_\omega$. Conclude that E is elementarily equivalent to F over L. ∎

Corollary 4: *Let $K \subseteq L$ be* PRC *fields. If* Res: $G(L) \to G(K)$ *is an isomorpism, then K is an elementary subfield of L.*

2. The elementary theory of algebraic PRC fields.

The main ingredient of the proof of the algebraic nature of the elementary theory of PRC fields is the following existence theorem for algebraic PRC fields with a given absolute Galois group. This is Theorem 5.1 of [HJ3].

PROPOSITION 5: *Let K be a countable formally real Hilbertian field and let K' be a finite Galois extension of K. If G is a real projective group of rank $\le \aleph_0$ and $\pi\colon G \to \mathcal{G}(K'/K)$ is an epimorphism such that $\pi(\mathrm{Inv}(G)) \subseteq \mathrm{Res}_{K'}(\mathrm{Inv}(G(K)))$, then there exists a* PRC *algebraic extension E of K and an isomorphism $\gamma\colon G(E) \to G$ such that $\mathrm{Res}_{\tilde{E}/K'} = \pi \circ \gamma$.*

The following result generalizes [FJ, Prop. 20.23].

PROPOSITION 6: *Let K be a countable Hilbertian field. Let F be a countable* PRC *extension of K. Then F is K-elementarily equivalent to an ultraproduct $\prod_{n=1}^{\infty} E_n/\mathcal{D}$ of* PRC *fields, with E_n algebraic over K and $G(E_n) \cong G(F)$, $n = 1, 2, 3, \ldots$.*

Proof: If F is not formally real, then it is PAC. In this case the proposition reduces to Proposition 20.23 of [FJ]. So, assume that F is formally real.

Let $L_1 \subseteq L_2 \subseteq L_3 \cdots$ be an ascending sequence of finite Galois extensions of K whose union is $\widetilde{K}$. For each n the intersection $K_n = L_n \cap F$ is a countable formally real Hilbertian field. By Theorem 10.1 of [HJ1], $G(F)$ is a real projective group. Since F is countable, $\mathrm{rank}(G(F)) \le \aleph_0$. Apply Proposition 5 with L_n/K_n replacing K'/K and $G(F)$ replacing G to find a PRC field E_n and an isomorphism φ_n which makes the following diagram commutative:

$$\begin{tikzcd} & G(E_n) \arrow[dl, "\varphi_n"'] \arrow[d, "\mathrm{Res}"] \\ G(F) \arrow[r, "\mathrm{Res}"'] & \mathcal{G}(L_n/K_n) \end{tikzcd}$$

Let $\mathcal{D}$ be a nonprincipal ultraproduct of $\mathbb{N}$ and let ${}^*E = \prod E_n/\mathcal{D}$ and ${}^*F = F^{\mathbb{N}}/\mathcal{D}$. By [FJ, Lemma 18.4] there exists an isomorpism φ that makes the following diagram commutative:

$$\begin{tikzcd} & G(^*E) \arrow[dl, "\varphi"'] \arrow[d, "\mathrm{Res}"] \\ G(^*F) \arrow[r, "\mathrm{Res}"'] & G(K) \end{tikzcd}$$

Since $^*E$ and $^*F$ are PRC fields [P1, Thm. 4.1], Proposition 3 asserts that $^*E \equiv_K {}^*F$. Conclude that $^*E \equiv_K F$. ∎

Proposition 7: *Let K be a countable Hilbertian field. Let $\mathcal{P}$ be a family of profinite groups with this property: If E and F are two elementary equivalent* PRC *fields and if $G(F) \in \mathcal{P}$, then $G(E) \in \mathcal{P}$. Then a sentence θ of $\mathcal{L}(\mathrm{ring}, K)$ is true in all* PRC *fields F with $K \subseteq F$ and $G(F) \in \mathcal{P}$ if and only if θ is true in all* PRC *fields E algebraic over K, with $G(E) \in \mathcal{P}$.*

Proof: Let F be a PRC field containing K such that $G(F) \in \mathcal{P}$. By the Skolem-Löwenheim theorem, F has a contable elementary subfield F_0 that contains K. By Proposition 6, $F_0 \equiv_K \prod E_i/\mathcal{D}$ with E_i a perfect PRC field, algebraic over K, and $G(E_i) \cong G(F_0)$, for each $i \in I$. By assumption $G(E_i) \in \mathcal{P}$. Hence θ is true in E_i for each i, and therefore θ is true in F. ∎

Apply Proposition 7 to the family of all profinite groups.

Theorem 8: *A sentence θ of $\mathcal{L}(\mathrm{ring})$ is true in each* PRC *field of characteristic 0 if and only if θ is true in each* PRC *field which is algebraic over $\mathbb{Q}$.*

3. The elementary theory of maximal PRC fields.

A field extension L/K is **totally real** if each ordering of K extends to L. A field K is **maximal real** if it has no proper algebraic totally real extensions [P2, p. 482]. Call a profinite group G **minimal real** if for each proper closed subgroup H of G there exists an involution ε of G which is conjugate to no involution of H.

LEMMA 9: *A* PRC *field K is maximal real if and only if $G(K)$ is minimal real.*

Proof: Suppose first that K is maximal real. Let L be a proper algebraic extension of K. Then K has an ordering P which does not extend to L. Let ε be an involution of $G(K)$ which induces P on K. Then ε is conjugate to no involution of $G(L)$. Conclude that $G(K)$ is minimal real. The other direction of the lemma follows similarly. ∎

THEOREM 10: *A sentence θ of $\mathcal{L}(\mathrm{ring})$ is true in each maximal* PRC *field of characteristic 0 if and only if θ is true in each maximal* PRC *field which is algebraic over $\mathbb{Q}$.*

Proof: The class of maximal PRC fields has been axiomatized in $\mathcal{L}(\mathrm{ring})$ by Prestel [P2, Lemma 1] (Note that axioms (ii) and (iii) of [P2] which express the maximality axiom and the PRC axiom are actually expressed in $\mathcal{L}(\mathrm{ring})$ and not in the extended language of preordered fields, as follows from [P1, Thm. 4.1].)

If E and F are elementarily equivalent PRC fields and $G(E)$ is minimal real, then E is maximal real (Lemma 10). Hence F is also maximal real and therefore $G(F)$ is minimal real. Our theorem is therefore a special case of Proposition 7. ∎

4. The absolute Galois group of a maximal PRC field.

The absolute Galois group of a PRC field (resp. an algebraic PRC field) is characterized in [HJ1] (resp. [HJ3]) as a real projective group (resp. of rank $\le \aleph_0$). Here we characterize the absolute Galois group of a maximal PRC field as a real projective group free on a set of involutions in the category of pro-2-groups.

Let G be a profinite group. Recall that a **finite real embedding problem** for G is a pair $(\varphi\colon G \to A, \alpha\colon B \to A)$ of epimorphisms with A and B finite groups such that for each $g \in \mathrm{Inv}(G)$ with $\varphi(g) \ne 1$ there exists $b \in \mathrm{Inv}(B)$ such that $\alpha(b) = \varphi(g)$ [HJ1, p. 468]. The problem is **solvable** if there exists a homomorphism $\gamma\colon G \to B$ such that $\alpha \circ \gamma = \varphi$. The group G is **real projective** if each finite real embedding problem for G is solvable and $\mathrm{Inv}(G)$ is closed in G.

For each Boolean space X there exists a unique (up to an isomoprhism) pro-2 group $\widehat{D}_2(X)$ such that $X \subseteq \mathrm{Inv}(\widehat{D}_2(X))$ and such that the following holds: Each continuous map φ of X into a pro-2 group G such that $\varphi(x)^2 = 1$ for each $x \in X$ uniquely extends to a homomorphism of $\widehat{D}_2(X)$ into G. We call $\widehat{D}_2(X)$ **real 2-free group** with basis X.

The construction and the proof of the properties of $\widehat{D}_2(X)$ is a verbatim repetition of those made in [HJ2] except that we have to work in the category of pro-2 groups instead of working in the category of all profinite groups.

LEMMA 11: *A profinite group G is minimal real if and only if it is a pro-2 group generated by involutions.*

Proof: Suppose first that G is a minimal real profinite group. Let G_2 be a 2-Sylow subgroup of G. Each involution of G is contained in a 2-Sylow subgroup of G and the latter is conjugate to G_2. Hence each involution of G is conjugate to some involution in G_2. Conclude that $G = G_2$ is a pro-2 group.

Let H be the closed subgroup of G generated by $\mathrm{Inv}(G)$. If $H \ne G$, then H is contained in an open normal subgroup N of index 2 (since this is the case for finite 2-groups). Hence $\mathrm{Inv}(G) \subseteq N$. This contradiction to the minimality of G proves that $H = G$.

Conversely, suppose that G is a pro-2 group which is generated by $\mathrm{Inv}(G)$. Let H be a proper closed subgroup of G. Let N be as in the preceding paragraph. Then $\mathrm{Inv}(G) \not\subseteq N$. In particular there exists $g \in \mathrm{Inv}(G)$ which is conjugate to no element of H. Conclude that G is minimal real. ∎

Haran proves in [H2] that each pro-2 real projective group is real 2-free. We need a special case of this theorem. It relies on the following result.

Lemma 12 ([HJ2, Lemma 3.5]): *Let D and G be real projective groups.*

(a) *There exists a closed system of representatives of the conjugacy classes of* $\mathrm{Inv}(G)$.

(b) *Let $\varphi\colon D \to G$ be a continuous epimorphism and let $\widehat{X}$ be a system of representatives of the conjugacy classes of* $\mathrm{Inv}(D)$. *If φ maps $\widehat{X}$ bijectively onto a system of representatives of the conjugacy classes of* $\mathrm{Inv}(G)$, *then there exists a continuous monomorphism $\psi\colon G \to D$ such that* $\varphi \circ \psi = \mathrm{id}$.

Proposition 13: *A profinite group G is minimal real projective if and only if $G = \widehat{D}_2(X)$ for some Boolean space X.*

Proof: Suppose first that $G = \widehat{D}_2(X)$ for some subset X of involutions. Then G is real projective (this is the pro-2 analogue of [HJ2, Corollary 2.2]). By Lemma 11, G is minimal real.

Conversely suppose that G is minimal real projective. Then G is a pro-2 group (Lemma 11). Let X be a closed system of representatives for the G-orbits of $\mathrm{Inv}(G)$ (Lemma 12). The minimality of G implies that X generates G. Let $\widehat{X}$ be a homeomorphic copy of X, with $\hat{x}$ the element of $\widehat{X}$ that corresponds to x. Consider the real free group $D = \widehat{D}_2(\widehat{X})$. The set $\widehat{X}$ is a closed system of representatives for the D-orbits of $\mathrm{Inv}(D)$ [HJ2, Cor. 3.2]. The bijective map $\hat{x} \mapsto x$ extends to an epimorphism $\varphi\colon D \to G$. Let $\psi\colon G \to D$ be a monomorphism as in Lemma 12. In particular $\psi(x)^2 = 1$ and $\psi(x) \neq 1$ for each $x \in X$. Hence $\psi(x) = \hat{y}^d$ for some $y \in X$ and $d \in D$. Hence $x = y^{\varphi(d)}$ and therefore $x = y$. Conclude that $\psi(x) = \hat{x}^d$. If $\psi(X)$ were contained in a proper closed subgroup of D it would be contained in a normal open closed subgroup N of index 2. This would imply that $\widehat{X} \subseteq N$, and therefore that $D \subseteq N$, a contradiction. It follows that $\psi(X)$ generates D. Conclude that ψ is an isomorphism and that $G \cong \widehat{D}_2(X)$. ∎

The absolute Galois group of a maximal PRC field with exactly e orderings is isomorphic to the free product of e copies of $\mathbb{Z}/2\mathbb{Z}$ [J2, Corollary 5.2]. Part (a) of the following theorem generalizes this result to arbitrary maximal PRC fields (see also [He, Thm. 3.2]).

THEOREM 14: (a) *If K is a maximal* PRC *field, then $G(K) = \widehat{D}_2(X)$ for some Boolean space X.*

(b) *For each Boolean space X there exists a maximal PRC field K such that $G(K) \cong \widehat{D}_2(X)$.*

(c) *For each separable Boolean space X there exists a maximal PRC field K, algebraic over $\mathbb{Q}$ such that $G(K) \cong \widehat{D}_2(X)$.*

Proof of (a): The main result of [HJ1], namely Theorem 10.1, asserts that $G(K)$ is real projective. By Lemma 9 and Proposition 13, $G(K) = \widehat{D}_2(X)$, for some Boolean space X.

Proof of (b) and (c): Let X be a Boolean space. Then $G = \widehat{D}_2(X)$ is real projective and real minimal (Proposition 13). By [HJ1, Theorem 10.1], there exists a PRC field K such that $G(K) \cong G$. By Lemma 9, K is maximal real. If in addition X is separable, then $\mathrm{rank}(G) \leq \aleph_0$. The main theorem of [HJ3] asserts that K can be chosen to be algebraic over $\mathbb{Q}$. ∎

5. Two more theories of fields.

Not every theory of fields is determined by its algebraic models.

Remark 15 (Prestel): *The Theory of fields.* Unlike the theorey of PAC fields, the theory of PRC fields and the theory of maximal PRC fields the theory of fields of characteristic 0 is not determined by its algebraic models. Indeed consider the elementary statement "if an element x is the sum of 5 squares, then x is the sum of 4 squares". We prove that this statement is true for each algebraic extension K of $\mathbb{Q}$ and for each $a \in K$ but is false for a certain element of $\mathbb{Q}(t)$.

Let K be an algebraic extension of $\mathbb{Q}$. Let $a \in K$, $a \neq 0$, be a sum of 5 squares in K. Without loss assume that K has a finite degree over $\mathbb{Q}$. Then a is a positive and therefore a square in each real closure of K. Hence the quadratic form

$$f(X_1, X_2, X_3, X_4, X_5) = X_1^2 + X_2^2 + X_3^2 + X_4^2 - aX_5^2$$

has a nontrivial zero in each real closure of K. By the Hasse-Minkowski principle ([L, p. 169]) or [CF, p. 259]) there exists x_1, x_2, x_3, x_4, x_5 in K, not all 0, such that $f(\mathbf{x}) = 0$. If $x_5 \neq 0$, divide the last equality by x_5 to get a representation of a as a sum of 4 squares in K. Otherwise suppose without loss that $x_1 = 1$. Then with $t = (a-1)/2$ we have $(t+1)^2 + (x_2 t)^2 + (x_3 t)^2 + (x_4 t)^2 = a$.

On the other hand 7 is not the sum of 3 squares in $\mathbb{Q}$. Otherwise there exist positive integers x, y, z and u such that $u \neq 0$ and $7u^2 = x^2 + y^2 + z^2$. Without loss assume that 2 does not divide all these integers. Now consider the above equation modulo 8 to derive a contradiction (cf. [Le, p. 133]). A result of the Cassels-Pfister theorem asserts that for t transcendental over $\mathbb{Q}$ the element $7 + t^2$ is not the sum of 4 squares in $\mathbb{Q}(t)$ [L, p. 261].

Likewise, the theory of fields of characteristic p is not determined by its algebraic models. Indeed, for each a and b in a finite field K the Galois group of $x^3 + aX + b$ has order at most 3. In contrast, since for t transcendental over $\mathbb{F}_p$, the field $\mathbb{F}_p(t)$ is Hilbertian and since for u, v algebraically independent over $\mathbb{F}_p(t)$ the Galois group $\mathcal{G}(X^3 + uX + v, \mathbb{F}(t, u, v)$ is isomorphic to S_3 there exist $a, b \in \mathbb{F}_p(t)$ such that the order of $\mathcal{G}(X^3+aX+b, \mathbb{F}(t,u,v))$ is 6. Thus not every sentence true in all algebraic extensions of $\mathbb{F}_p$ is also true in $\mathbb{F}_p(t)$. ∎

References

[CDM] G. Cherlin, L. v.d. Dries, and A. Macintyre, *The elementary theory of regularly closed fields,* a manuscript.

[CF] J.W.S. Cassels and A. Fröhlich, Algebraic Number Theory, Academic Press, London, 1967.

[D] L. v.d. Dries, *Model theory of fields,* Dissertation, Utrecht, 1978.

[E] Ju.L. Ershov, *Two theorems on regularly r-closed fields,* Journal für die reine und angewandte Mathematik 347 (1987), 154–167.

[FJ] M. Fried and M. Jarden, *Field Arithmetic,* Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge **11**, Springer, Heidelberg, 1986.

[H1] D. Haran, *On closed subgroups of free products of profinite groups,* Proceedings of the London Mathematical Society **55** (1987), 266–289.

[H2] D. Haran, *closed subgroups of $G(\mathbb{Q})$ with involutions,* preprint.

[He] B. Heinemann, *On finite intersections of "Henselian valued" fields,* manuscripta mathematica **52** (1985), 37–61.

[HJ1] D. Haran and M. Jarden, *The absolute Galois group of a pseudo real closed field,* Annali Scuola Normale Superiore — Pisa, Serie IV, **XII** (1985), 449–489.

[HJ2] D. Haran and M. Jarden, *Real free groups and the absolute Galois group of $\mathbb{R}(t)$,* Journal of Pure and Applied Algebra **37**, 155–165.

[HJ3] D. Haran and M. Jarden, *The absolute Galois group of a pseudo real closed algebraic field,* Pacific Journal of Mathematics **123** (1986), 55–69.

[HJ4] D. Haran and M. Jarden, *The absolute Galois group of a pseudo p-adically closed field,* Journal für die reine und angewandte Mathematik.

[J1] M. Jarden, *The elementary theory of large e-fold ordered fields,* Acta mathematica **149** (1982), 239–259.

[J2] M. Jarden, *On the model companion of the theory of e-fold ordered fields,* Acta mathematica **150** (1983), 243–253.

[L] T.Y. Lam, *The algebraic theory of quadratic forms,* Mathematics Lecture Note Series, Benjamin, Reading, 1973.

[La] S. Lang, *Algebra,* Addison–Wesley, Reading, 1967.

[Le] W.J. LeVeque, *Topic in Number Theory I,* Addison-Wesely, Reading, 1958.

[P1] A. Prestel, *Pseudo real closed fields,* Set Theory and Model Theory, Lecture Notes **872**, Springer, 1982.

[P2] A. Prestel, *Decidable theories of preordered fields,* Mathematische Annalen **258** (1982), 481–492.

Moshe Jarden
School of Mathematical Sciences
Raymond and Beverly Sackler
Faculty of Exact Sciences
Tel Aviv University
Ramat Aviv, Tel Aviv 69978
Israel