JOURNAL OF ALGEBRA **143**, 470–486 (1991)

Properties of Fields

K. DECK AND D. K. HARRISON

Department of Mathematics, University of Oregon, Eugene, Oregon 97403

Communicated by Kent R. Fuller

Received August 15, 1989

INTRODUCTION

We study the category of fields and places. We show the rational numbers are the initial object in this category, and

(1) every morphism can be factored (uniquely up to multiplication by a unit—that is, an isomorphism) as a product of a surjective morphism and a ring homomorphism;

(2) every ring homomorphism can be factored (uniquely up to multiplication by a unit) as a ring homomorphism and an integrally closed morphism;

(3) every object has an essential ring homomorphism into an injective object and this is unique up to isomorphism.

We do some field theory in such a category. We leave the theory of local fields (i.e., Henselizations), and the theory of ordered fields (i.e., automorphisms of order two of injective objects), to a sequel, and restrict attention to studying the transcendence degree. We get a result which is new and can be stated in the more usual language; the group of automorphisms of an algebraically closed field has a certain structure and the perfect subfields correspond bijectively with certain subgroups (isomorphic subfields correspond to conjugate subgroups). In a short last section, we give a purely group theoretic realization of the category of subfields of algebraically closed fields of transcendence degree zero and their places.

1. FIELDS AND PLACES

Let **Plc** be the category whose objects are fields and whose morphisms are places. Recall that a place from a field F to E is a triple $(D_\varphi, \varphi, I_\varphi)$,

0021-8693/91 $3.00

where D_φ is a valuation ring, φ is a ring homomorphism from D_φ onto I_φ, and I_φ is a subfield of E. We write $\mathscr{M}(F, E)$ for the set of all ring homomorphisms from F to E, and $\mathscr{E}(F, E)$ for the set of all surjective places from F to E, for F and E fields.

THEOREM 1.1. **Plc** *has an initial object.*

Proof. The initial object is $\mathbf{Q}$. If $F \in \mathbf{Ob}(\mathbf{Plc})$, and $\mathbf{char}\, F = 0$, then $\mathbf{Q} \subseteq F$ and the unique place is the inclusion morphism.

If $\mathbf{char}\, F = p \neq 0$, then there is a unique place from $\mathbf{Q}$ to F with valuation ring $\mathbf{Z}_{(p)}$.

DEFINITION 1.2. By a **category with factorization** we mean a category $\mathscr{C}$ and for each pair of objects (A, B) subsets $\mathscr{E}(A, B)$ and $\mathscr{M}(A, B)$ of $\mathbf{Mor}(A, B)$ such that:

(1) $e_1 \in \mathscr{E}(A, B)$, $e_2 \in \mathscr{E}(B, C) \Rightarrow e_2 \circ e_1 \in \mathscr{E}(A, C)$;

(2) $m_1 \in \mathscr{M}(A, B)$, $m_2 \in \mathscr{M}(B, C) \Rightarrow m_2 \circ m_1 \in \mathscr{M}(A, C)$;

(3) $\forall f \in \mathscr{C}(A, B), f \in \mathscr{E}(A, B) \cap \mathscr{M}(A, B) \Leftrightarrow f$ is an isomorphism;

(4) $\forall f \in \mathscr{M}(A, B)$, $\exists f_e \in \mathscr{E}$, and $f_m \in \mathscr{M}$ *with* $f = f_m \circ f_e$;

(5) $f = m \circ e$, $e \in \mathscr{E}$, $m \in \mathscr{M} \Rightarrow \exists$ unique isomorphism t with $e = t \circ f_e$, $m = f_m \circ t^{-1}$;

(6) $e \in \mathscr{E}, f \circ e = g \circ e \Rightarrow f = g$;

(7) $m \in \mathscr{M}$, $m \circ f = m \circ g \Rightarrow f = g$.

THEOREM 1.3. **Plc** *with* $\mathscr{M}$ *and* $\mathscr{E}$ *is a category with factorization.*

Proof. We leave (1)–(4) and (6) as exercises.

(5) Let $(D_\varphi, \varphi, I_\varphi)$ be a place from F to E with $\varphi = \varphi_m \circ \varphi_e$, $\varphi_m \in \mathscr{M}$, $\varphi_e \in \mathscr{E}$. Write I for $\varphi(D_\varphi)$. Let $i: I \hookrightarrow E$; define $\eta: F \to I$ by $\alpha \mapsto \varphi(\alpha)$. Then $\varphi = i \circ \eta$, η is surjective, and i is monic. For $\alpha \in D_\varphi$, $\varphi_m(\varphi_e(\alpha)) = \varphi(\alpha) = \eta(\alpha) \in I$. *Let* C be the codomain of φ_e. φ_e is surjective so $\varphi_e(D_\varphi) = C$. Since φ_m is a ring homomorphism, $\varphi_m(C) \subseteq I$. If $\beta \in I$, then $\exists \alpha \in F$ with $\eta(\alpha) = \beta$. So $\varphi(\alpha) = \beta \Rightarrow \varphi_m(\varphi_e(\alpha)) = \beta \Rightarrow I \subseteq \varphi_m(C)$. Hence $I = \varphi_m(C)$.

Define $h: C \to I$ by $c \mapsto \varphi_m(c)$. h is an isomorphism, $h(\varphi_e(\alpha)) = \eta(\alpha)$. Hence $h \circ \varphi_e = \eta$. For $c \in C$, $i \circ h(c) = i(\varphi_m(c)) = \varphi_m(c) \Rightarrow i \circ h = \varphi_m$. If $\varphi = m \circ e$ for $m \in \mathscr{M}$ and $e \in \mathscr{E}$, there exists an isomorphism $t: C' \to I$, where C' is the codomain of e and $t \circ e = \eta$, $i \circ t = m$. Thus $h \circ \varphi_e = t \circ e = \eta \Rightarrow t^{-1} \circ h \circ \varphi_e = e$ and $\varphi_m \circ h^{-1} = m \circ t^{-1} \Rightarrow \varphi_m \circ h^{-1} \circ t = m$. Let $\psi = t^{-1} \circ h$. Then $\psi \circ \varphi_e = e$, $\varphi_m \circ \psi^{-1} = m$. Suppose γ is another such isomorphism. So $\gamma \circ \varphi_e = e$, $\varphi_m \circ \gamma^{-1} = m$. But then $\gamma \circ \varphi_e = \psi \circ \varphi_e \Rightarrow \gamma = \psi$ since φ_e is surjective.

(7) Define $\tilde{F} = F \cup \{\infty\}$. Let $m: \tilde{F} \to \tilde{E}$ be a ring homomorphism. Let $K \in \mathbf{Ob(Plc)}$, $\varphi, \psi \in \mathbf{Mor}(K, F)$. Suppose $m \circ \varphi = m \circ \psi$. So for all $\beta \in K$, $m(\varphi(\beta)) = m(\psi(\beta))$. m is $1-1$ since $\ker m$ is an ideal of F, but $1 \notin \ker m = 0$. Hence, $\varphi(\beta) = \psi(\beta)$ $\forall \beta \in K$, which implies $\varphi = \psi$. Thus, m is monic.

Definition 1.4. Let $\mathscr{C}$ be a category with factorization, with $A, B \in \mathbf{Ob}(\mathscr{C})$. $i \in \mathscr{M}(A, B)$ is $\mathscr{M}$-essential if $j \in \mathbf{Mor}(B, C)$ with $j \circ i \in \mathscr{M} \Rightarrow j \in \mathscr{M}$.

Theorem 1.5. *Let $\varphi \in \mathbf{Mor}(F, E)$; φ is $\mathscr{M}$-essential $\Leftrightarrow \varphi \in \mathscr{M}$ with E algebraic over $\varphi(F)$.*

Proof. [$\Leftarrow$] Since φ is a ring homomorphism, φ is monic. Let $\theta \in \mathbf{Mor}(E, K)$ with $\theta \circ \varphi \in \mathscr{M}$. Let D be the domain of θ. Then $\varphi(F) \cap D = \varphi(F)$ and $\varphi(F) \cap D \backslash U(D) = 0$. We show $D = E$. Let $\beta \in E$, and just suppose that $\beta \notin D$; $\exists \alpha_1 \cdots \alpha_{n-1} \in F$ such that

$$\beta^n + \alpha_{n-1}\beta^{n-1} + \cdots + \alpha_1\beta \in D.$$

Choose n to be minimal. By factoring, $\beta(\beta^{n-1} + \alpha_{n-1}\beta^{n-2} + \cdots + \alpha_1) \in D$ and $\beta \notin D \Rightarrow \beta^{-1} \in D$. So $\beta^{n-1} + \alpha_{n-1}\beta^{n-2} + \cdots + \alpha_1 \in D$. This contradiction gives $\beta \in D$ $\forall \beta \in E$, which implies $E = D$. Hence θ is a ring homomorphism which implies $\theta \in \mathscr{M}$. Thus φ is essential.

[$\Rightarrow$] Assume φ is essential. Just suppose $\exists$ transcendental $x \in E \backslash F$. Then $\exists$ a valuation ring D of $F(x)$ such that $D \neq F(x)$. By the extension theorem for places, there exists a valuation ring V of E with $F(x) \cap (V \backslash U(V)) = F(x) \backslash U(D)$ and with $D \subseteq V$. Hence $V \neq E$ so the composition map $F \to K \to V \backslash M(V)$ is not a ring homomorphism.

Definition 1.6. Let $\mathscr{C}$ be a category with factorization, A, $\bar{A}$, X, $Y \in \mathbf{Ob}(\mathscr{C})$. An injective envelope of A is a pair $(i, \bar{A})$ where $\bar{A}$ is an object, $i \in \mathscr{M}(A, \bar{A})$, i is $\mathscr{M}$-essential, and $m \in \mathscr{M}(X, Y)$ and $f \in \mathbf{Mor}(X, \bar{A})$ implies there exists $g \in \mathbf{Mor}(Y, \bar{A})$ such that $g \circ m = f$.

Theorem 1.7. *For F any object of* **Plc**, *an injective envelope $(i, \bar{F})$ exists.*

Proof. Let $\bar{F}$ be the algebraic closure of F. Let $i: F \to \bar{F}$ be the inclusion place. Since $\bar{F}/i(F)$ is algebraic, and i is a ring homomorphism, i is $\mathscr{M}$-essential.

Theorem 1.8. *Let $i: F \to \bar{F}$ be an essential $\mathscr{M}$-morphism with $\bar{F}$ injective. Let $\sigma \in \mathbf{Mor}(\bar{F}, \bar{F})$ with $\sigma \circ i = i$. Then σ is an isomorphism.*

Proof. Let $\sigma: \bar{F} \to \bar{F}$ be a place such that $\sigma \circ i = i$. Since i is $\mathcal{M}$-essential, $\sigma \circ i \in \mathcal{M}$, so $\sigma \in \mathcal{M}$. Let $\alpha \in F$. The splitting field N of the irreducible polynomial of α over F is of finite dimension over F, and $\sigma(N) \subseteq N$ since N is a normal extension. $\sigma|_N$ is $1-1$ since σ is a ring homomorphism. But $\sigma|_N: N \to N$ is linear and $1-1$ so onto. Hence $\exists \beta \in N$ such that $\sigma(\beta) = \alpha$. Thus σ is an isomorphism.

THEOREM 1.9. *Let $i: F \to \bar{F}$ be as above. Let $j: F \to E$ be $\mathcal{M}$-essential with E injective. Then there exists an isomorphism $t: \bar{F} \to E$ with $t \circ i = j$.*

Proof. First note that by Definition 1.2(7), $i \in \mathcal{M}$ implies that i is monic. Since E is injective, $\exists t: \bar{F} \to E$ such that $t \circ i = j$. t is monic since j is monic and i is essential. Since $\bar{A}$ is injective and j is monic, $\exists s: E \to \bar{F}$ such that $s \circ j = i$. s is monic since i is monic and j is essential. We have $s \circ t \circ i = s \circ j = i \Rightarrow s \circ t \circ i = i \Rightarrow s \circ t$ is an isomorphism by Theorem 1.8. So s is onto, and t is injective. Applying Theorem 1.8 to j, one gets that $t \circ s$ is an isomorphism. Hence t is onto, which implies t is an isomorphism.

DEFINITION 1.10. Let $\mathscr{C}$ be a category with factorization with $A, B \in \mathbf{Ob}(\mathscr{C})$. A morphism $f: A \to B$ is **$\mathcal{M}$-extremal** if $f = m \circ g$ with $m \in \mathcal{M}$ implies m is an isomorphism.

CLAIM 1.11. *In* **Plc** *a morphism $\varphi: F \to E$ is $\mathcal{M}$-extremal $\Leftrightarrow$ φ is surjective.*

Proof. [$\Rightarrow$] Define $\eta: F \twoheadrightarrow \operatorname{Im} \varphi$, $i: \operatorname{Im} \varphi \hookrightarrow E$ as above. $f = i \circ \eta$ and $i \in \mathcal{M}$ so i is and isomorphism, and $\operatorname{Im} \varphi = E$ which implies φ is surjective.

[$\Leftarrow$] Suppose φ is surjective, and $\varphi = m \circ \psi$ with $m \in \mathcal{M}$, where $\psi: F \to K$; $m: K \to E$. φ is surjective so $\forall \beta \in E\ \exists \alpha \in F$ such that $\varphi(\alpha) = \beta$. Hence, $m(\psi(\alpha)) = \beta$ implies $\forall \beta \in E$, $\exists \psi(\alpha) \in K$ such that $m(\psi(\alpha)) = \beta$. Thus m is onto. Define $n: E \to K$ by $\beta \mapsto \psi(\alpha)$ where $m(\psi(\alpha)) = \beta$. Then $n(m(\psi(\alpha))) = n(\beta) = \psi(\alpha)$ and $m(n(\beta)) = m(\psi(\alpha)) = \beta$. Hence $m \circ n = 1$ and $n \circ m = 1$. Thus m is an isomorphism and φ is $\mathcal{M}$-extremal.

DEFINITION 1.12. Let $\mathscr{C}$ be a category with factorization with $A, B \in \mathbf{Ob}(\mathscr{C})$. A morphism $f: A \to B$ is **integrally closed** if $f \in \mathcal{M}$ and if $f = g \circ m$ with m $\mathcal{M}$-essential implies m is an isomorphism.

THEOREM 1.13. *Any ring homomorphism φ in* **Plc** *can be factored*

$$\varphi = \varphi_{ic} \circ \varphi_s,$$

where φ_s is $\mathcal{M}$-essential and φ_{ic} is integrally closed. If $\varphi = \psi \circ t$ with t essential and ψ integrally closed, then there exists a unique isomorphism γ with $t = \gamma \circ \varphi_s$ and $\psi \circ \gamma = \varphi_{ic}$.

Proof. Let $\varphi: F \to E$, I the integral closure of F in E and factor φ through I by $\varphi = \varphi_{ic} \circ \varphi_s$. Since I is algebraic over F and φ_s is a ring homomorphism, φ_s is $\mathscr{M}$-essential, hence $\varphi_{ic} \in \mathscr{M}$. Suppose φ_{ic} factors through K by $\varphi_{ic} = \psi \circ m$, and suppose m is $\mathscr{M}$-essential. By Theorem 1.5, K is algebraic over $m(I)$. Hence K is algebraic over I, but I is the algebraic closure of F in E so $K \cong I$. Thus φ_{ic} is indeed integrally closed.

Suppose $\varphi_{ic} \circ \varphi_s = \psi_{ic} \circ \psi_s$. Integral closures are unique up to isomorphism so there exists an isomorphism $r: I \to J$ such that $r^{-1} \circ \psi = \varphi_s$ and $\psi_{ic} \circ r = \varphi_{ic}$.

DEFINITION 1.14. The **adjusted characteristic** of a field F, denoted **adj. char** F, is $p =$ **char** F if $p \neq 0$, and 1 if **char** $F = 0$.

THEOREM 1.15. *A ring homomorphism $\varphi: F \to E$ is epic in* **Mor**$(F, E) \Leftrightarrow \varphi$ *is a ring homomorphism and $\forall \alpha \in E$, $\exists n \geqslant 0$ with $\alpha^{p^n} = \varphi(\beta)$, $\beta \in F$, and $p =$* **adj. char**(F).

Proof. $[\Leftarrow]$ Suppose $\sigma, \tau \in$ **Mor**(F, E) with $\sigma \circ \varphi = \tau \circ \varphi$. Let $\alpha \in E$. $\alpha^{p^n} = \varphi(\beta)$ for some $\beta \in F$. Hence $\sigma(\varphi(\beta)) = \tau(\varphi(\beta)) \Rightarrow \sigma(\alpha^{p^n}) = \tau(\alpha^{p^n}) \Rightarrow (\sigma(\alpha))^{p^n} = (\tau(\alpha))^{p^n} \Rightarrow (\sigma(\alpha) - \tau(\alpha))^{p^n} = 0 \Rightarrow \sigma(\alpha) = \tau(\alpha)$, since F is an integral domain. Hence $\sigma = \tau$, so φ is epic.

$[\Rightarrow]$ Just suppose $\exists \beta \in E$ and there does not exist an n with $\beta^{p^n} = \varphi(\alpha)$ for any $\alpha \in F$. Let $\bar{E}$ be the algebraic closure of E. Let L be the image of φ.

Case 1. β is algebraic over L. We have $\beta^{p^n} \notin L$, $\forall n \geqslant 0$. By the perfectness of fields of characteristic zero, and by p. 283, Lemma 6.3 of [5], $\exists m$ such that β^{p^m} is separable over L. Let N be the splitting field of the irreducible polynomial that β^{p^m} satisfies over L. N is normal separable over L, and $\beta^{p^m} \in N$. Since $\beta^{p^m} \notin L$, $\exists \sigma \in$ **Aut**$_L(N)$ with $\sigma(\beta^{p^m}) \neq \beta^{p^m}$. σ extends to $\tau \in$ **Aut**$_L \bar{L}$ (by p. 317, Theorem 1.12 of [5]). Then $\tau(\varphi(\gamma)) = 1(\varphi(\gamma))$ $\forall \gamma \in \varphi^{-1}(L)$. Hence $\tau \circ \varphi = 1 \circ \varphi$. But $\tau \neq 1$. This contradiction proves the first case.

Case 2. β is transcendental over L and $\beta^2 \neq \beta$. $\exists \sigma \in$ **Rng**$(L(\beta), (L(\beta^2))$ with $\sigma(\beta) = \beta^2$, and $\sigma: L(\beta) \cong L(\beta^2)$. Extend σ to $\tau \in$ **Aut**$_L(\overline{L(\beta)})$. $\tau(\varphi(\alpha)) = 1(\varphi(\alpha))$ $\forall \alpha \in \varphi^{-1}(L)$. Hence $\tau \circ \varphi = 1 \circ \varphi$ and $\tau \neq 1$. With this contradiction the theorem is proved.

THEOREM 1.16. *If φ is an epic morphism in* **Plc**, *and φ is also in $\mathscr{M}$, then φ is essential.*

Proof. Let $\varphi \in \mathscr{M}$ and φ epic in **Plc**. By Theorem 1.15,

$$\{\alpha \in E \mid \exists n \in \mathbf{N}, \alpha^{p^n} = \varphi(\beta), \beta \in F\} = E.$$

So $E/\text{Im}\ \varphi$ is algebraic, which implies φ is $\mathscr{M}$-essential.

DEFINITION 1.17. Let $\mathscr{C}$ be a category with factorization, f is **separable** if f is $\mathscr{M}$-essential and if $f = t \circ s$ with $t \in \mathscr{M}$ and t an epic morphism $\Rightarrow t$ is an isomorphism.

THEOREM 1.18. *Let φ be an $\mathscr{M}$-essential morphism from F to E. Then there exists a ring homomorphism b which is epic and a separable morphism s with $\varphi = b \circ s$. Moreover, if $b' \in \mathscr{M}$ with b' epic and s' is a separable morphism, such that $\varphi = b' \circ s'$, then $\exists$ a unique isomorphism σ such that $b' = b \circ \sigma$, $s' = \sigma^{-1} \circ s$.*

Proof. Let F^s be the set of elements in E which are separable over F. Factor φ through F^s by $\varphi = b \circ s$. Since F^s/F is algebraic, and s is a ring homomorphism, s in $\mathscr{M}$-essential. Suppose s factors through K for $K \in \mathbf{Ob(Plc)}$, by $s = t \circ r$, and suppose t is a ring homomorphism which is epic. By Theorem 1.15, $F^s = \{\alpha \in F^s \mid \exists n \in \mathbf{N} \text{ with } \alpha^{p^n} = t(c) \text{ for } c \in K\}$. But $F^s = (F^s)^{p^n}$ $\forall n$ implies t is onto. Since s is the inclusion map, t must be an isomorphism. Hence s is separable. Since $E/\varphi(F)$ is algebraic, $E/b(F^s)$ is algebraic, hence for any $\beta \in E$, there exists n such that β^{p^n} is separable over $b(F^s)$. Hence $\exists \alpha \in F^s$ with $\beta^{p^n} = b(\alpha)$. By Theorem 1.15, b is epic. Since $\varphi = b \circ s \in \mathscr{M}$ with s essential, $b \in \mathscr{M}$. Uniqueness follows since the elements of E separable over F form a subfield of E.

2. AN EXTENDED GALOIS CORRESPONDENCE

DEFINITION 2.1. For Γ a profinite group, consider a triple $(G, \varphi, \mathscr{S})$, where G is a group, φ is a surjective group homomorphism from G onto Γ, and $\mathscr{S}$ is a set of subgroups of $\ker \varphi$. For such, call a subgroup H of G **basic** if

$$H = \varphi^{-1}(N) \cap J_1 \cap \cdots \cap J_n,$$

where $0 \leqslant n$, $J_1, ..., J_n \in \mathscr{S}$, and N is an open subgroup of Γ. Call a subset V of G **open** if it is a union of sets of the form σH, $\sigma \in G$, H basic.

DEFINITION 2.2. A set $\mathscr{B}$ of subsets of $\mathscr{S}$ is **independent** if for $n \geqslant 1$ and all distinct elements $J_1, ..., J_n$ of $\mathscr{B}$ the index $[\bigcap_{j \neq i} J_j : J_1 \cap \cdots \cap J_n] = \infty$ for all $i = 1, ..., n$.

DEFINITION 2.3. A triple $(G, \varphi, \mathscr{S})$ is a **Γ-system** if:

(1) $\bigcap_{J \in \mathscr{S}} J \cap \ker \varphi = \{1\}$;

(2) $J \in \mathscr{S}$ implies $\{kJk^{-1} \mid k \in \ker \varphi\} = \mathscr{S}$;

(3) $J \in \mathscr{S}$, $\sigma \in G$ implies $\sigma J \sigma^{-1} \in \mathscr{S}$;

One checks that if $(G, \varphi, \mathscr{S})$ is a Γ-system then G is a Hausdorff, 0-dimensional, topological group and φ is continuous.

DEFINITION 2.4. For $(G, \varphi, \mathscr{S})$ a Γ-system, call a subgroup T of G **tight** if

$$T = \varphi^{-1}(M) \cap \left(\bigcap J \right),$$

where the J are intersected over some subset $\mathscr{H}$ of $\mathscr{S}$ and M is a closed subgroup of Γ.

THEOREM 2.5. *Let F be an algebraically closed field. Write F_0 for the set of elements of F which are algebraic over the prime subfield P of F. Let Γ be the Galois group of F_0 over P, let $G = \mathbf{Aut}(F)$, let $\varphi\colon G \to \Gamma$ be given by restriction, and let*

$$\mathscr{S} = \{ \mathbf{Aut}_{P_0(\alpha)}(F) \mid \alpha \in F, \alpha \notin F_0 \}.$$

Then a Γ-system results, and the map $L \mapsto \mathbf{Aut}_L(F)$ is an order-inverting bijection from the set of all perfect subfields of F onto the set of all tight subgroups of G. This bijection takes composites to intersections. If L_i corresponds to T_i, $i = 1, 2$, then L_1 is isomorphic to L_2 if and only if T_1 is conjugate to T_2. Also L_1 includes F_0 if and only if T_1 is included in ker φ. *Also $L_1 \subseteq L_2$, if and only if $T_2 \subseteq T_1$; if $L_1 \subseteq L_2$ then $\mathbf{dim}_{L_1} L_2 = [T_1 : T_2]$.*

Proof. One checks the three properties of a Γ-system.
We will need three lemmas.

LEMMA 2.6. *For any perfect subfield L of F with $H = \mathbf{Aut}_L F$ then $F^H = L$.*

Proof. Let $a \in F \backslash L$ and $a \in F^H$.

Case 1. a algebraic over L, $\bar{L} = F$. $H = \mathbf{Aut}_L F = \mathbf{Aut}_L \bar{L}$. Let b be any other root of the irreducible polynomial of a over L. Then $\exists h \in \mathbf{Aut}_L \bar{L} = H$ such that $h(a) = b$. But this contradicts $a \in F^H$.

Case 2. a algebraic over L, $\bar{L} \neq F$. Let A be the transcendence base of L over P such that $A \subseteq X$, where X is the transcendence base of F. Let $B = X \backslash A$. Since a is algebraic over L, $\exists \sigma \in \mathbf{Aut}_L \bar{L}$ such that $\sigma(a) = b$, for b another root of the irreducible polynomial of a over L. Extend σ to $\hat{\sigma}\colon \bar{L}(B) \to \bar{L}(B)$ by $\hat{\sigma}(d) = d$, $\forall d \in B$, $\hat{\sigma}(l) = \sigma(l)$, $\forall l \in L$ [5, p. 312]. $\overline{L(B)} = F$ so extend $\hat{\sigma}$ to $\tau\colon F \to F$. Then $\tau \in \mathbf{Aut}_L F = H$. But $\tau(a) = b$ which contradicts $a \in F^H$.

Case 3. a is transcendental over L. Let $b=a+1$. Let S (respectively T), be a transcendence base which contains a (respectively b). Define a map γ: $\bar{L}(a)\to\bar{L}(b)$ such that $\gamma|_{\bar{L}}=1$ and $a\mapsto b$. Extend γ to $\hat{\gamma}$: $\bar{L}(S)\to\bar{L}(T)$, and then extend to φ: $F\to F$. $\varphi\in \mathbf{Aut}_L F=H$. But $\varphi(a)=b$, which contradicts $a\in F^H$. Thus, $F^H\subseteq L\Rightarrow F^H=L$.

LEMMA 2.7. *For any perfect subfield of F, $H=\mathbf{Aut}_L F$ is tight.*

Proof. $\mathbf{Aut}_L F=\bigcap_{l\in L}\mathbf{Aut}_{P(l)} F$. Let $T=\{t\in L\mid t$ is transcendental over $P\}$.

$$A=\{a\in L\mid a \text{ is algebraic over } P\}.$$

We have $L=P(T)(A)$. Let t_0 be a particular element of T. For any $t\in T$ there is a map $\tilde{\sigma}_t$: $P(t_0)\to P(t)$ by $t_0\mapsto t$ and $\tilde{\sigma}_t$ can be extended to $\sigma_t\in\mathbf{Aut}_P F$ as before. $\mathbf{Aut}_{P(t)} F=\mathbf{Aut}_{P(\sigma_t(t_0))} F=\sigma_t^{-1}(\mathbf{Aut}_{P(t_0)} F)\,\sigma_t$. Hence,

$$\mathbf{Aut}_P F=\bigcap_{t\in T}\sigma_t^{-1}(\mathbf{Aut}_{P(t_0)} F)\,\sigma_t;$$

which is tight. For each $a\in A$,

$$\sigma\in\mathbf{Aut}_{P(a)} F\Leftrightarrow\sigma(a)=a\Leftrightarrow\sigma(a)=\varphi^{-1}(1(a))\Leftrightarrow\sigma\in\varphi^{-1}(\mathbf{Aut}_{P(a)} F_0).$$

So $\mathbf{Aut}_{P(a)} F=\varphi^{-1}(\mathbf{Aut}_{P(a)} F_0)$ and $\mathbf{Aut}_{P(A)} F=\bigcap_{a\in A}\varphi^{-1}(\mathbf{Aut}_{P(a)} F_0)$ which is tight. Thus

$$\mathbf{Aut}_L F=\bigcap_{l\in L}\mathbf{Aut}_{P(l)} F=\bigcap_{t\in T}\sigma_t^{-1}(\mathbf{Aut}_{P(t_0)} F)\,\sigma_t\cap\bigcap_{a\in A}\varphi^{-1}(\mathbf{Aut}_{P(a)} F_0).$$

LEMMA 2.8. *If H is a tight subgroup of G, then there exists a perfect subfield L such that $P\subseteq L\subseteq F$ and $H=\mathbf{Aut}_L F$.*

Proof. Case 1. $H=\varphi^{-1}(M)$, M is a closed subgroup of Γ. By infinite Galois theory, $M=\mathbf{Aut}_L F_0$, with L perfect. So

$$\begin{aligned}H&=\{\varphi^{-1}(\mathbf{Aut}_L F_0)\}=\{\sigma\in G\,|\sigma|_{F_0}(l)=l,\ l\in L\}\\&=\{\sigma\in G\mid\sigma(l)=l\ \forall l\in L\}\end{aligned}$$

as $L\leqslant F_0$. Hence, $\sigma\in H\Rightarrow\sigma\in\varphi^{-1}(M)\Rightarrow\varphi(\sigma)\in M\Rightarrow\varphi(\sigma)l=l$, $\forall l\in L$. Hence $\sigma\in\mathbf{Aut}_L F$. For $\sigma\in\mathbf{Aut}_L F$, $\varphi(\sigma)\in\mathbf{Aut}_L F_0\Rightarrow\varphi(\sigma)\in M\Rightarrow\sigma\in\varphi^{-1}(M)=H$. Thus $H=\mathbf{Aut}_L F$.

Case 2. $H=\mathbf{Aut}_{P(t)} F$, $t \in F \backslash F_0$. Let p be the **adj. char** F. Let L be the perfect closure of $P(t)$. That is,

$$L=\{\alpha \mid \alpha^{p^n} \in P(t)\}=\{\alpha \mid \sigma(\alpha)=\alpha, \sigma \in H\}.$$

Case 3. $H=\varphi^{-1}(M) \cap (\bigcap_{J \in \mathscr{H} \subseteq \mathscr{S}} J)$. Each $J \in \mathscr{H}$ corresponds to a field L_J by Case 2. By Case 1, $\phi^{-1}(M)$ corresponds to a field L_M. Then $H=\bigcap_{J \in \mathscr{H} \cup M} \mathbf{Aut}_{L_J} F$. Let $L=\bigcap E$ where $\bigcup L_i \subseteq E \leqslant F$. Then $\sigma \in H \Leftrightarrow \sigma$ fixes $\bigcap_{J \in \mathscr{H} \cup M} \Leftrightarrow L \subseteq F^{\{\sigma\}} \Leftrightarrow \sigma \in \mathbf{Aut}_L F$. With these lemmas, the theorem is proved.

DEFINITION 2.9. A subset $\mathscr{B}$ of $\mathscr{S}$ is a **basis** if the elements of $\mathscr{B}$ are independent and $\forall J \in \mathscr{S}$, $\exists J_1, \ldots, J_n \in \mathscr{B}$ with $[J_1 \cap \cdots \cap J_n: J \cap J_1 \cap \cdots \cap J_n] < \infty$.

THEOREM 2.10. *Every independent subset of $\mathscr{S}$ can be expanded to a basis. Every spanning subset of $\mathscr{S}$ can be contracted to a basis. Any two bases have the same cardinality.*

Proof. We use the fact that for tight subgroups T_1, T_2 and corresponding fields L_1, L_2, $\mathbf{dim}_{L_2} L_1=[T_1 : T_2]$ and check that Theorems 64.1, 2, 3 from [6] apply. Let $\mathscr{M}$ be an independent set. We show that $\mathscr{M}$ can be extended to a basis. Let

$$\mathscr{F}=\{\mathscr{N} \mid \mathscr{M} \subseteq \mathscr{N}, \mathscr{N} \text{ independent}\}.$$

One checks that $\mathscr{F}$ is a partially ordered set. Given a chain $\mathscr{A}$, the upper bound of $\mathscr{A}$ is $\bigcup_{\mathscr{N} \subseteq \mathscr{A}} \mathscr{N}$. Apply Corollary 33.1 of [6] to show that $\bigcup_{\mathscr{N} \subseteq \mathscr{A}} \mathscr{N}$ is independent. Thus, every chain of $\mathscr{F}$ has an upperbound, and by Zorn's Lemma, $\mathscr{F}$ has a maximal element. Let $\mathscr{P}$ be the maximal element and apply Corollary 33.2 of [6] to show that $\mathscr{P}$ spans $\mathscr{S}$. Thus, $\mathscr{P}$ is a spanning set for $\mathscr{S}$, and the independent set $\mathscr{M}$ can be expanded to the basis $\mathscr{P}$.

We now show that any spanning set can be contracted to a basis. Suppose $\mathscr{N}$ is a spanning set. Let $\mathscr{F}=\{\mathscr{O} \mid \mathscr{O} \subseteq \mathscr{N}$ and $\mathscr{O}$ is a spanning set$\}$. One checks that $\mathscr{F}$ is partially ordered. Let $\mathscr{B}$ be a chain of $\mathscr{F}$. Check that $\mathscr{B}$ has a lower bound of $\bigcap_{\mathscr{O} \in \mathscr{B}} \mathscr{O}$ by applying Corollaries 33.3 and 33.4 of [6]. Thus, every chain of $\mathscr{F}$ has a lower bound, so by Zorn's Lemma, $\mathscr{F}$ has a minimal element, $\mathscr{Q}$. Apply Theorem 64.3 of [6] to show that $\mathscr{Q}$ is linearly independent. Thus $\mathscr{N}$ contracts to a basis $\mathscr{Q}$. We refer to p. 315 of [5] to show that any two sets have the same transcendence degree.

DEFINITION 2.11. The transcendence degree of a Γ-system $(G, \phi, \mathscr{S})$ is the cardinality of the basis of $\mathscr{S}$. One checks this is equal to the transcendence degree of the algebraically closed field.

THEOREM 2.12. *Let $\psi: E \to F$ be a ring homomorphism between fields (i.e., $\psi \in \mathcal{M}(E, F)$) with F algebraically closed. The following are equivalent.*

(1) $\mathbf{Aut}_E F$ *is compact;*

(2) $\forall \alpha \in F$ *the orbit* $\mathbf{Aut}_E F(\alpha)$ *is finite;*

(3) *the extension F/E is algebraic.*

Proof. (1) $\Rightarrow$ (2). Let $H = \mathbf{Aut}_E F$. In the Krull topology, $V_1(\{\alpha\})$ is open. The set of left cosets $H/V_1(\{\alpha\})$ maps bijectively onto the orbit $H(\alpha)$ by $\sigma V_1(\{\alpha\}) \mapsto \sigma(\alpha)$.

$$H = \dot{\bigcup_{\sigma}} \sigma V_1(\{\alpha\}).$$

H is compact, hence there exists a finite number of σ such that $H = \dot{\bigcup}_\sigma \sigma V_1(\{a\})$.

(2) $\Rightarrow$ (3). Just suppose F/E is a transcendental extension. Suppose E is infinite. $\exists x \in F \backslash E$ transcendental, and $x + \alpha$ transcendental for all $\alpha \in F$. For each α, $\exists \sigma: E(x) \to E(x + \alpha)$ defined by $x \to x + \alpha$ and $\sigma|_E = 1$. Extend σ to $\tau \in \mathbf{Aut}\, F$. Since E is infinite, the orbit of x is infinite. Now suppose that E is finite. Then $\bar{E}$ is infinite. Since F is transcendental over $\bar{E}$ and F is algebraically closed, $\bar{E}$ is a proper subset of F. Now use the above argument to prove the theorem.

(3) $\Rightarrow$ (1). Consider E^*, the perfect closure of E. F/E^* is a Galois extension. By infinite Galois theory, $\mathbf{Aut}_{E^*} F$ is compact. But $\mathbf{Aut}_{E^*} F = \mathbf{Aut}_E F$, hence the theorem is proved.

THEOREM 2.13. *Let $(G, \varphi, \mathcal{S})$ be a Γ-system associated to an algebraically closed field F. For $J \in \mathcal{S}$, J is compact $\Leftrightarrow$ the transcendence degree of $\mathcal{S}$ is* 1 *or* 0.

Proof. [$\Leftarrow$] If the transcendence degree is 0, then $\mathcal{S}$ is empty. If the transcendence degree is 1, and J corresponds to the subextension L of F, then F/L is an algebraic extension, so by Theorem 2.12, $J = \mathbf{Aut}_L F$ is compact.

[$\Rightarrow$] Let H be any open subgroup of G. $J \cap H$ is open since both J and H are open. Hence $[J: J \cap H]$ has finite index since J is compact. Thus, J, and H are dependent, and J spans $\mathcal{S}$. Thus, the transcendence degree is 1.

THEOREM 2.14. *Let $(G, \varphi, \mathcal{S})$ be a Γ-system associated to an algebraically closed field F. G is locally compact if and only if the transcendence degree of $\mathcal{S}$ is finite.*

Proof. We use the fact that G is locally compact and 0-dimensional if and only if G has an open profinite subgroup. (See [4, pp. 12, 62] for one direction. The other is an easy check.)

Let $G = \mathbf{Aut}\, F$. For T a trancendence basis of F over P, $G = \mathbf{Aut}_P\, \overline{F_0(T)}$. Let

$$H = \mathbf{Aut}_P\, \overline{F_0(T)},$$

where F_0 is the perfect closure of P. H is compact since $\overline{F_0(T)} \backslash P(T)$ is an algebraic extension. Also, $H = \bigcap_{t \in T} V_1(t)$. This is a finite intersection, so H is open. Thus G has a compact open subgroup, hence G is locally compact.

Suppose G is locally compact. G contains a subgroup H which is open and compact. $\forall \sigma \in H$, choose a finite subset A_σ of F such that $V_\sigma(A_\sigma) \subseteq H$. Then $H = \bigcup_{\sigma \in H} V_\sigma(A_\sigma)$. Since each $V_\sigma(A_\sigma)$ is open and H is compact, there exists a finite subset I such that $H = \bigcup_I V_{\sigma_i}(A_{\sigma_i})$. Since H is a group at least one $V_{\sigma_i}(A_{\sigma_i})$ contains the identity. For this i, $V_{\sigma_i}(A_{\sigma_i}) = V_1(A_{\sigma_i})$. $V_1(A_{\sigma_i})$ is a tight subgroup of G. Hence $V_1(A_{\sigma_i})$ corresponds to a perfect subfield L of F. $L = F_0(A_{\sigma_i})$ or $(F_0(A_{\sigma_i}))^*$ (where * denotes the perfect closure). Since the transcendence degree of $(F_0(A_{\sigma_i}))^*$ equals the transcendence degree of $F_0(A_{\sigma_i})$ and $F_0(A_{\sigma_i})$ has finite transcendence degree over P, L has finite transcendence degree over P. But $F^H \subseteq F^{V_1(A_{\sigma_i})}$. Hence F^H has finite transcendence degree. But $\mathbf{Aut}_{F^H} F = H$ by Lemma 1.9 of [3], and H is compact, so F/F^H is algebraic. Therefore F is an algebraic extension of a finitely generated field extension, hence F has finite transcendence degree.

3. Absolute Galois Groups

Definition 3.1. A **coplace** from a profinite group H to a profinite group G is a closed subgroup Δ of $H \times G$ such that for all $h \in H$ there exists a $g \in G$ with $(h, g) \in \Delta$.

Theorem 3.2. *If $\Delta \colon H \to G$, $\Theta \colon G \to K$ are coplaces then*

$$\Theta \circ \Delta := \{(h, k) \in H \times K \mid \exists g \in G \text{ with } (h, g) \in \Delta,\ (g, k) \in \Theta\}$$

is a coplace from H to K.

Proof. Let $h \in H$. Since Δ is a coplace, $\exists g \in G$ such that $(h, g) \in \Delta$. Since Θ is a coplace, $\exists k \in K$ such that $(g, k) \in \Theta$. Thus, $(h, k) \in \Theta \circ \Delta$. One checks $\Theta \circ \Delta$ is closed under inverses, multiplication, associativity, and that $\Theta \circ \Delta$ is a closed subgroup of $H \times K$.

THEOREM 3.3. *For* $g \in G$, $\Delta_g := \{(\sigma, g\sigma g^{-1}) \in G \times G \mid \sigma \in G\}$ *is a coplace from G to G.*

Proof. $\forall \sigma \in G$, $g\sigma g^{-1} \in G \Rightarrow (\sigma, g\sigma g^{-1}) \in \Delta_g$. One checks Δ_g is closed under inverses, multiplication, and that Δ_g is a closed subgroup of $G \times G$.

DEFINITION 3.4. Coplaces $\Delta: H \to G$, $\Theta: H \to G$ will be called conjugate if $\Delta = \Delta_g \circ \Theta$ for some $g \in G$.

THEOREM 3.5. *If* $(g, e) \in \Theta$, *then* $\Delta_e \circ \Theta = \Theta \circ \Delta_g$.

Proof. $(a, b) \in \Delta_e \circ \Theta \Rightarrow \exists t \in G$ such that $(a, t) \in \Theta$, $(t, b) \in \Delta_e$. Hence $b = ete^{-1} = e\Theta(a)\, e^{-1}$. $(a, b) \in \Theta \circ \Delta_g \Rightarrow \exists t \in G$ such that $(a, t) \in \Delta_g$, $(t, b) \in \Theta$. Hence $t = gag^{-1}$, $b = \Theta(t) = \Theta(gag^{-1})$. But $b = e\Theta(a)\, e^{-1} = \Theta(g)\, \Theta(a)\, \Theta(g^{-1}) = \Theta(gag^{-1}) \Rightarrow \Delta_e \circ \Theta = \Theta \circ \Delta_g$.

DEFINITION AND THEOREM 3.6. *For* $\Delta: H \to G$, *and* $\Theta: G \to K$, *let*

$$[\Delta] = \{\Delta_g \circ \Delta \mid g \in G\}$$

and let $[\Theta] \circ [\Delta] = [\Theta \circ \Delta]$. *This is well-defined and a category results.*

Proof. Let $\Delta_{k_1} \circ \Theta \circ \Delta_{g_1} \circ \Delta$, $\Delta_{k_2} \circ \Theta \circ \Delta_{g_2} \circ \Delta \in [\Theta \circ \Delta]$, where $k_1, k_2 \in K$, $g_1, g_2 \in G$. We show that there exists an $m \in K$ such that

$$\Delta_m \circ \Delta_{k_2} \circ \Theta \circ \Delta_{g_2} \circ \Delta = \Delta_{k_1} \circ \Theta \circ \Delta_{g_1} \circ \Delta.$$

By Theorem 3.5, $\Delta_{k_1} \circ \Theta \circ \Delta_{g_1} \circ \Delta = \Delta_{k_1} \circ \Delta_{l_1} \circ \Theta \circ \Delta$, where $(g_1, l_1) \in \Theta$. Also, $\Delta_{k_2} \circ \Theta \circ \Delta_{g_2} \circ \Delta = \Delta_{k_2} \circ \Delta_{l_2} \circ \Theta \circ \Delta$, where $(g_2, l_2) \in \Theta$.

$$\Delta_{k_1} \circ \Delta_{l_1} \circ \Delta_{l_2^{-1}} \circ \Delta_{k_2^{-1}} \circ \Delta_{k_2} \circ \Delta_{l_2} \circ \Theta \circ \Delta = \Delta_{k_1} \circ \Delta_{l_1} \circ \Theta \circ \Delta.$$

Equivalently, $\Delta_{k_1 l_1 (k_2 l_2)^{-1}} \circ \Delta_{k_2} \circ \Delta_{l_2} \circ \Theta \circ \Delta = \Delta_{k_1} \circ \Delta_{l_1} \circ \Theta \circ \Delta$. We have $k_1 l_1 (k_2 l_2)^{-1} \in K$, so call this m. Applying Theorem 3.5 again, we have

$$\Delta_m \circ \Delta_{k_2} \circ \Theta \circ \Delta_{g_2} \circ \Delta = \Delta_{k_1} \circ \Theta \circ \Delta_{g_1} \circ \Delta.$$

One checks associativity, and that the identity map 1 is a coplace. With these, a category results.

THEOREM 3.7. *For each object* A, *let* $i_A: A \to \bar{A}$ *be essential with* $\bar{A}$ *injective, and define*

$$\mathbf{Gal}(A) = \{\sigma \in \mathbf{Aut}(\bar{A}) \mid \sigma \circ i_A = i_A\}.$$

For any morphism $f: A \to B$, *since* $\bar{A}$ *is injective, we can choose an* $\bar{f}: \bar{A} \to \bar{B}$ *such that* $\bar{f} \circ i_A = i_B \circ f$. *For each* $\tau \in \mathbf{Gal}(B)$, $\exists \sigma \in \mathbf{Gal}(A)$ *with* $\bar{f} \circ \sigma = \tau \circ \bar{f}$.

Define

$$\mathbf{G}(f) := \{(\tau, \sigma) \in \mathbf{Gal}(B) \times \mathbf{Gal}(A) \mid \bar{f} \circ \sigma = \tau \circ \bar{f}\}.$$

Up to conjugacy (as in 3.4), *this is well-defined contravariant functor from* **Mor** *to the category of profinite groups and conjugacy classes of coplaces.*

Proof. We first show that $\mathbf{G}(f) = \Delta$ is a coplace. By Proposition 7, p. 428 of [2], $\forall \tau \in \mathbf{Gal}(B)$, $\exists \sigma \in \mathbf{Gal}(A)$ with $\bar{f} \circ \sigma = \tau \circ \bar{f}$, $\forall \tau \in \mathbf{Gal}(B)$. Thus, $(\tau, \sigma) \in \Delta$. One checks that Δ is a closed subgroup of $\mathbf{Gal}(B) \times \mathbf{Gal}(A)$. Thus, $\Delta = \mathbf{G}(f) \in \mathbf{hom}(\mathbf{Gal}(B), \mathbf{Gal}(A))$.

Suppose $f: A \to B$, $g: B \to C$ induce $\bar{f}: \bar{A} \to \bar{B}$, $\bar{g}: \bar{B} \to \bar{C}$, and

$$(\tau, \sigma) \in [\mathbf{G}(f)] = \Delta, \qquad (\gamma, \tau) \in [\mathbf{G}(g)] = \Theta.$$

We have $\bar{f} \circ \sigma = b\tau b^{-1} \circ \bar{f}$, and $\bar{g} \circ \tau = c\gamma c^{-1} \circ \bar{g}$, for $b \in \mathbf{Gal}(B)$, and $c \in \mathbf{Gal}(C)$. By Theorem 3.5, $\bar{f} \circ a\sigma a^{-1} = \tau \circ \bar{f}$ for $(b, a) \in \Delta \Rightarrow \bar{g} \circ \bar{f} \circ a\sigma a^{-1} = \bar{g} \circ \tau \circ \bar{f} = c\gamma c^{-1} \circ \bar{g} \circ \bar{f}$. So $(c\gamma c^{-1}, a\sigma a^{-1}) \in \Theta \circ \Delta$, which implies $(\gamma, \sigma) \in [\Theta \circ \Delta]$.

Suppose $(\gamma, \sigma) \in [\Theta \circ \Delta]$. We have $\bar{g} \circ \bar{f} \circ \sigma = c\gamma c^{-1} \circ \bar{g} \circ \bar{f}$, for $c \in \mathbf{Gal}(C)$. Since Θ is a coplace, $\exists \beta \in \mathbf{Gal}(B)$ such that $c\gamma c^{-1} \circ \bar{g} = \bar{g} \circ b\beta b^{-1}$. So $c\gamma c^{-1} \circ \bar{g} \circ \bar{f} = \bar{g} \circ b\beta b^{-1} \circ \bar{f}$. Since Δ is a coplace, $\exists \delta \in \mathbf{Gal}(A)$ such that $b\beta b^{-1} \circ \bar{f} = \bar{f} \circ a\delta a^{-1} \Rightarrow \bar{g} \circ b\beta b^{-1} \circ \bar{f} = \bar{g} \circ \bar{f} \circ a\delta a^{-1} \Rightarrow \bar{g} \circ \bar{f} \circ \alpha = \bar{g} \circ \bar{f} \circ a\delta a^{-1}$. By Lemma A, p. 383 of [1], there exists an automorphism τ of B such that $\tau(\sigma) = a\delta a^{-1}$. If τ is given by conjugation by an element r of $\mathbf{Gal}(B)$, we have $r\sigma r^{-1} = a\delta a^{-1}$. So $\sigma = ra\,\delta(ra)^{-1}$. Hence, $(\beta, \sigma) \in [\Delta]$, $(\gamma, \beta) \in [\Theta]$. Thus $\mathbf{G}(-)$ preserves composition. One checks that 1 is the identity coplace to complete the proof that $\mathbf{G}(-)$ is a contravariant functor.

THEOREM 3.8. *With notation as above,*

(1) *If f is $\mathcal{M}$-essential then $\mathbf{G}(f) = \Delta$ is an injective group homomorphism.*

(2) *If $f \in \mathcal{M}$ then Δ is a surjective homomorphism.*

(3) *If $f \in \mathcal{E}$ then the set $\{a \in \mathbf{Gal}(A) \mid (a, 1) \in \Delta\} = \{1\}$.*

Proof. (1) $[\Rightarrow]$ One checks that f *$\mathcal{M}$-essential* implies that $\bar{f}$ is $\mathcal{M}$-essential. Since $\bar{f}$ is $\mathcal{M}$-essential, $\bar{B}/\bar{f}(\bar{A})$ is an algebraic extension. But $\bar{f}(\bar{A})$ is algebraically closed, hence $\bar{B} = \bar{f}(\bar{A})$. Thus, $\bar{B} \cong \bar{A}$ and $\bar{f}$ is an isomorphism. In particular, $\bar{f}$ is epic. Suppose $(\sigma, 1) \in \Delta$. Then $\sigma \circ \bar{f} = \bar{f} \circ 1 \Rightarrow \sigma \circ \bar{f} = 1 \circ \bar{f} \Rightarrow \sigma = 1$. Next show that $f \in \mathcal{M}$ implies Δ is a group homomorphism. Suppose $(1, \sigma) \in \Delta$. Since $f \in \mathcal{M}$, f is monic. Then $\bar{f} \circ \sigma = 1 \circ \bar{f} = \bar{f} \circ 1 \Rightarrow \sigma = 1$, as $\bar{f}$ is monic. Also, for any $\sigma \in \mathbf{Gal}(B)$, $\exists \tau \in \mathbf{Gal}(A)$, with $\sigma \circ \bar{f} = \bar{f} \circ \tau$ (by [2, Proposition 7]).

To prove (2), it suffices to show that Δ is surjective. Let $\gamma \in \mathbf{Gal}(\mathbf{A})$. Since $\bar{B}$ is injective and $f \in \mathscr{M} \Rightarrow f$ monic $\Rightarrow \bar{f}$ monic, $\exists\omega: \bar{B} \to \bar{B}$ such that $\omega \circ \bar{f} = \bar{f} \circ \gamma \Rightarrow (\omega, \gamma) \in \Delta$.

To prove (3), we first show that if f is extremal then $\bar{f}$ is extremal. Suppose $\bar{f} = j \circ g$ with $j \in \mathscr{M}$. If D is the valuation ring for $\bar{f}$, and M is its unique maximal ideal, $D/M \cong \kappa$. Suppose κ is not algebraically closed. There exists a monic irreducible non-linear polynomial, $h \in \kappa[x]$. Choose representatives of the coefficients of h in D so that

$$t = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

satisfies $t + M\kappa[x] = h$. There exists $b \in \bar{A}$ such that $t(b) = 0$. b is integral over D, so $b \in D$. Hence $b + M$ is a zero of h; but this is a contradiction. Since κ is algebraically closed, κ is injective, hence $j(\kappa)$ is injective and $j(\kappa) = \bar{B}$. Thus, j is an isomorphism and $\bar{f}$ is extremal. By Claim 1.11, $\bar{f}$ is surjective.

Now suppose $(a, 1) \in \Delta$. Then $\bar{f} \circ 1 = a \circ \bar{f} \Rightarrow 1 \circ \bar{f} = a \circ \bar{f} \Rightarrow 1 = a$.

4. Embedded Algebraic Fields

We say a field F is **algebraic** if F is algebraic over its prime subfield. By an **embedded field** we mean a triple $(F, i_F, \bar{F})$ where $\bar{F}$ is an algebraically closed algebraic field, F is an algebraic field, and i_F is a ring homomorphism from F to $\bar{F}$. By a morphism $(F, i_F, \bar{F}) \to (K, i_K, \bar{K})$ we mean a pair $(\varphi, \bar{\varphi})$, where $\bar{\varphi}$ is a place from F to K, φ is a place from $\bar{F}$ to $\bar{K}$, and $\bar{\varphi} \circ i_F = i_k \circ \varphi$. We write $\mathscr{F}$ for the resulting category. We sometimes write F for the triple $(F, i_F, \bar{F})$.

Proposition 4.1. *For any embedded algebraic field F there exists $\mu_F: \bar{\mathbf{Q}} \to \bar{F}$ such that $i_F \circ \alpha = \mu_F \circ \beta$ where $\alpha: \mathbf{Q} \to F$, $\beta: \mathbf{Q} \to \bar{\mathbf{Q}}$.*

Proof. Since $\bar{F}$ is algebraically closed, it is injective. Since β is monic, there exists $\mu_F: \bar{\mathbf{Q}} \to \bar{F}$ such that $i_F \circ \alpha = \mu_F \circ \beta$.

Proposition 4.2. *For each morphism $\varphi: F \to K$ there exists $g \in G = \mathbf{Aut}\ \bar{\mathbf{Q}}$ with $\mu_K = \bar{\varphi} \circ \mu_F \circ g$.*

Proof. $i_F \circ \alpha = \mu_F \circ \beta$, $i_K \circ \gamma = \mu_K \circ \beta$ where $\alpha: \mathbf{Q} \to F$, $\beta: \mathbf{Q} \to \bar{\mathbf{Q}}$, $\gamma: \mathbf{Q} \to K$. Since $\mathbf{Q}$ is initial, $\varphi \circ \alpha = \gamma$. Write $a = \bar{\varphi} \circ \mu_F$, $b = \mu_K$. Then $a \circ \beta = b \circ \beta$. For V the valuation ring of a and W the valuation ring of b, there exists $\sigma \in G$ with $\sigma(W) = V$ (Lemma A of [1]). Hence $a \circ \sigma^{-1}$ and b have the same valuation ring. There exists $\tau \in \mathbf{Aut}\ \bar{K}$, $\tau \circ a \circ \sigma^{-1} = b$ since $a \circ \sigma^{-1}$ and b are equivalent. By Proposition 7, p. 428 of [2], there exists $\omega \in G$ with $\tau \circ a = a \circ \omega$. Hence there exists $g \in G$ with $a \circ g = b$. One checks that g is well-defined with respect to i_F.

DEFINITION 4.3. $A_F = \{\sigma \in G \mid \exists \tau \in \mathbf{Aut}\, \bar{F}$ with $\mu_F \circ \sigma = \tau \circ \mu_F\}$. $S_F = \{\sigma \in G \mid \mu_F \circ \sigma = \mu_F\}$. $H_F = \{\sigma \in G \mid \exists \tau \in \mathbf{Aut}\, \bar{F}$ with $\mu_F \circ \sigma = \tau \circ \mu_F$ and $\tau \circ i_F = i_F\}$.

PROPOSITION 4.4. *If* $\mu_K = \bar{\varphi} \circ \mu_F \circ g_1 = \bar{\varphi} \circ \mu_F \circ g_2$, *then* $g_1 S_K = g_2 S_K$ *where* $S_F = \{\sigma \in G \mid \mu_F \circ \sigma = \mu_F\}$, $S_K = \{\sigma \in G \mid \mu_K \circ \sigma = \mu_K\}$.

Proof. $\mu_K = \bar{\varphi} \circ \mu_F \circ g_1 = \bar{\varphi} \circ \mu_F \circ g_2 \Rightarrow \mu_K \circ g_1^{-1} = \bar{\varphi} \circ \mu_F = \bar{\varphi} \circ \mu_F \circ g_2 \circ g_1^{-1}$ $\Rightarrow \mu_K \circ g_1^{-1} = \mu_K \circ g_1^{-1} \circ g_2 \circ g_1^{-1} \Rightarrow \mu_K = \mu_K \circ g_1^{-1} \circ g_2 \circ g_1^{-1} \circ g_1 \Rightarrow$ $\mu_K \circ g_1^{-1} \circ g_2 = \mu_K$. *Hence* $g_1^{-1} \circ g_2 \in S_K$. *Thus* $g_1 S_K = g_2 S_K$.

DEFINITION 4.5. Let $\mathscr{P}$ be all pairs (S, A) where A is a closed subgroup of a profinite group G, and S is a closed normal subgroup of A. For (S, A), $(T, B) \in \mathscr{P}$ write $(S, A) \leqslant (T, B)$ if $T \leqslant S$ and $A \leqslant B$. For $g \in G$, $g(S, A)\, g^{-1} = (gSg^{-1}, gAg^{-1}) \in \mathscr{P}$. Let P be the set of all (S_F, A_F) such that F is an object in $\mathscr{F}$. A **P-object** is a triple (S, H, A) where $(S, A) \in P$ and H is a closed subgroup of A which includes S. Let $X = (S, H, A)$, $Y = (T, L, B)$ be P-objects. We write

$$\mathscr{C}(X, Y) = \{gS \mid \text{either } g(S, A)\, g^{-1} < (T, B), \text{ or}$$
$$g(S, A)\, g^{-1} = (T, B) \text{ and } gHg^{-1} \leqslant L\},$$

with $g \in \mathbf{Aut}\, \bar{\mathbf{Q}}$. Let $Z = (U, M, C)$ be a P-object, and let $g_2 T \in \mathscr{C}(Y, Z)$. Define $g_2 T \circ gS = g_2 gS$. One checks $\mathscr{C}$ is a well-defined category. For F an embedded algebraic field define $\Psi(F) = (S_F, H_F, A_F)$. For $(\varphi, \bar{\varphi})$ a morphism from F to K choose g as in Proposition 4.2 and define $\Psi(\varphi, \bar{\varphi}) = gS_K$. Ψ is well-defined by Proposition 4.4.

THEOREM 4.6. *Ψ is a contravariant equivalence of categories.*

Proof. One checks that Ψ preserves the identity and composition. We check that Ψ is dense, faithful, and full. Ψ is dense by the fundamental theorem of Galois theory.

Full. Given gS: $(S, H, A) \to (T, L, B)$ with $g(S, A)\, g^{-1} = (T, B)$. Let $H = H_K$ and $L = H_F$. $gHg^{-1} \leqslant L \Rightarrow gH_K g^{-1} \leqslant H_F \Rightarrow H_{g(K)} \leqslant H_F \Rightarrow$ $g(K) \geqslant F$. Let $\bar{\varphi} = g^{-1}|_{\bar{F}}$. If $(S, H, A) < (T, L, B)$ then $(T, B) = (1, G)$ and μ_F is an isomorphism. Let $\bar{\varphi} = \mu_K \circ g^{-1} \circ \mu_F^{-1}$.

Faithful. Suppose $g_1 S_K = g_2 S_K$, $g_1 = a \circ g_2 \circ b$ where $\mu_F \circ a = \mu_F$, $\mu_K \circ b = \mu_K$, and $a, b \in \mathbf{Aut}\, \mathbf{Q}$. We have $\mu_K = \bar{\varphi}_1 \circ \mu_F \circ g_1$, and

$\mu_K = \bar{\varphi}_2 \circ \mu_F \circ g_2$. Hence $\mu_K = \bar{\varphi}_1 \circ \mu_F \circ a \circ g_2 \circ b \Rightarrow \mu_K \circ b^{-1} = \bar{\varphi}_1 \circ \mu_F \circ a \circ g_2$ $\Rightarrow \mu_K = \bar{\varphi}_1 \circ \mu_F \circ a \circ g_2$. Thus $\bar{\varphi}_1 \circ \mu_F \circ g_2 = \bar{\varphi}_2 \circ \mu_F \circ g_2$. Since both μ_F and g_2 are epic, $\mu_f \circ g_2$ is epic. Thus $\bar{\varphi}_1 = \bar{\varphi}_2$.

Comment. In Theorem 4.6 we have not claimed that factorization is preserved; however, in the case where the characteristics of the fields are the same, factorization is preserved. The following lemmas are to this effect.

LEMMA 4.7. *Either* **char** $F =$ **char** K *and* $\bar{\varphi}$ *is an isomorphism with* $\bar{\varphi}$ *mapping* F *into* K, *or* **char** $F \neq$ **char** K *and* μ_F *is an isomorphism with* $\bar{\varphi}$ *mapping* $\tilde{F}$ *into* $\tilde{K}$.

Proof. If **char** $F =$ **char** K then $\bar{F} \cong \bar{K}$. For V the valuation ring of $\bar{\varphi}$ and M the maximal ideal of $\bar{\varphi}$, V/M is algebraically closed, hence $V/M \cong \bar{K}$. But then $V/M = \bar{F}$ which implies $V = \bar{F}$ and $M = 0$. Thus $\bar{\varphi}$ is an isomorphism. The fact that $\bar{\varphi}$ maps F into K follows from $\bar{\varphi} \circ i_F = i_K \circ \varphi$.

If **char** $K \neq$ **char** K then **char** $F = 0$, $\bar{F} \cong \bar{\mathbf{Q}}$ and $\mu_F : \bar{\mathbf{Q}} \to \bar{F}$ by the above argument. Thus μ_F is an isomorphism.

LEMMA 4.8. $S_F \leqslant g S_K g^{-1}$.

Proof. Let $\sigma \in S_F$.

$$\mu_K \circ g^{-1} \circ \sigma \circ g = \bar{\varphi} \circ \mu_F \circ g \circ g^{-1} \circ \sigma \circ g$$
$$= \bar{\varphi} \circ \mu_F \circ \sigma \circ g = \bar{\varphi} \circ \mu_F \circ g = \mu_K.$$

Hence $g^{-1} \circ \sigma \circ g \in S_K$. Thus $S_F \leqslant g S_K g^{-1}$.

LEMMA 4.9. $A_K \leqslant g^{-1} A_F g$.

Proof. *Case* 1. **char** $F =$ **char** K. Let $\sigma \in A_K$. $\exists \tau \in$ **Aut** $\bar{K}$ such that $\mu_K \circ \sigma = \tau \circ \mu_K$. Since $\bar{\varphi} \circ \mu_F \circ g = \mu_K$, $\bar{\varphi} \circ \mu_F \circ g \circ \sigma = \tau \circ \bar{\varphi} \circ \mu_F \circ g$. Composing with $\bar{\varphi}^{-1}$ on the left and g^{-1} on the right, one has $\mu_F \circ g \circ \sigma \circ g^{-1} = \bar{\varphi}^{-1} \circ \tau \circ \bar{\varphi} \circ \mu_F$. Since $\bar{\varphi}^{-1} \circ \tau \circ \bar{\varphi} \in$ **Aut** $\bar{F}$, $g \circ \sigma \circ g^{-1} \in A_F$. Thus $A_K \leqslant g^{-1} A_F g$.

Case 2. **char** $F \neq$ **char** K. **char** $F = 0 \Rightarrow \mu_F$ is an isomorphism. Hence $A_F = G$. Thus $A_K \leqslant g^{-1} A_F g = G$.

LEMMA 4.10. *For* **char** $F =$ **char** K, $g H_K g^{-1} \leqslant H_F$.

Proof. Let $\sigma \in H_K$. $\exists \tau \in$ **Aut** $\bar{K}$ with $\mu_K \circ \sigma = \tau \circ \mu_K$ and $\tau \circ i_K = i_K$.

$$\bar{\varphi} \circ \mu_F \circ g \circ \sigma = \tau \circ \bar{\varphi} \circ \mu_F \circ g \Rightarrow \mu_F \circ g \circ \sigma \circ g^{-1} = \bar{\varphi}^{-1} \circ \tau \circ \bar{\varphi} \circ \mu_F.$$

Also, $\bar{\varphi}^{-1} \circ \tau \circ \bar{\varphi} \circ i_F = i_F$ since $\bar{\varphi}(F) \leqslant K$ and $\tau \circ i_K = i_K$.

LEMMA 4.11. *For* **char** $F=$ **char** K, $H_F \leqslant gA_K g^{-1}$.

Proof. Let $\sigma \in H_F$. $\exists \tau \in \mathbf{Aut}\, \bar{F}$ with $\mu_F \circ \sigma = \tau \circ \mu_F$ and $\tau \circ i_F = i_F$. $\mu_K \circ g^{-1} \circ \sigma \circ g = \bar{\varphi} \circ \mu_F \circ g \circ g^{-1} \circ \sigma \circ g = \bar{\varphi} \circ \mu_F \circ \sigma \circ g = \bar{\varphi} \circ \tau \circ \mu_F \circ g = \bar{\varphi} \circ \tau \circ \bar{\varphi}^{-1} \circ \bar{\varphi} \circ \mu_F \circ g = \bar{\varphi} \circ \tau \circ \bar{\varphi}^{-1} \circ \mu_K$. Also, $\bar{\varphi} \circ \tau \circ \bar{\varphi}^{-1} \in \mathbf{Aut}\, \bar{K}$. Hence $g^{-1} \sigma g \in A_K$. Thus $H_F \leqslant gA_K g^{-1}$.

REFERENCES

1. S. BEALE AND D. K. HARRISON, Prime-like subobjects of a profinite group, *Comm. Algebra* **17**, No. 2 (1989), 377–392.
2. N. BOURBAKI, "Commutative Algebra," Addison–Wesley, Reading, MA, 1972.
3. M. FRIED AND M. JARDEN, "Field Arithmetic," Springer-Verlag, New York, 1986.
4. E. HEWITT AND K. ROSS, "Abstract Harmonic Analysis," Springer-Verlag, New York, 1979.
5. T. HUNGERFORD, "Algebra," Holt, Rinehart & Winston, New York, 1974.
6. B. L. VAN DER WAERDEN, "Modern Algebra," New York, 1964.