THE FRATTINI SUBGROUP OF THE ABSOLUTE GALOIS GROUP OF A LOCAL FIELD

by

Moshe Jarden[1)], Tel Aviv University

and

Jürgen Ritter, Universität Augsburg

Abstract

Let K be a local field, T the maximal tamely ramified extension of K, F the fixed field in K_s of the Frattini subgroup of $G(K)$, and J the compositum of all minimal Galois extensions of K containing T. The main result of the paper is that $F = J$. If K is a global field and K_{solv} is the maximal prosolvable extension of K, then the Frattini group of $\mathcal{G}(K_{\mathrm{solv}}/K)$ is trivial.

[1)] Partially supported by a grant from the G.I.F., the German–Israeli Foundation for Scientific Research and Development.

Introduction

The **Frattini group** of a profinite group H is the intersection of all maximal open subgroups of H. It is a characteristic subgroup of H which we denote by $\Phi(H)$. The significance of $\Phi(H)$ arises from its second characterization: "If S is a subset of H which together with $\Phi(H)$ generates H, then S generates H by itself". Thus if N is a closed normal subgroup of H which is contained in $\Phi(H)$, a subset S of H generates H precisely when its image in H/N generates H/N. Also, if U is an arbitrary closed normal subgroup of H, then $\Phi(U) \leq \Phi(H)$ [FJ, Lemma 20.4(c)].

In particular, let K be a local field, i.e., K is a finite extension of $\mathbb{Q}_p$ or of $\mathbb{F}_p((t))$. Let T be the maximal tamely ramified extension of K. Denote the absolute Galois group of K (resp., T) by $G(K)$ (resp., $P = G(T)$). Then P is a closed normal pro-p subgroup of $G(K)$ and therefore $\Phi(P) \leq \Phi(G(K)))$. Moreover, $P/\Phi(P)$ is the maximal p-elementary abelian quotient of P [FJ, Lemma 20.36]. In particular, the commutator subgroup $[P, P]$ is contained in $\Phi(P)$ and therefore in $\Phi(G(K))$. Hence, $G(K)$ has as many generators as $G(K)/[P, P]$.

Jannsen [J, Section 3] has implicitly used this observation to determine the number of generators of $G(K)$. Indeed, if $\mathrm{char}(K) = 0$, then, by results of Iwasawa [I] (which are represented in a sharper form by Jannsen [J]) and by local class field theory, $G(K)/[P, P]$ has $[K{:}\mathbb{Q}_p] + 3$ generators. So, $G(K)$ is also generated by $[K{:}\mathbb{Q}_p] + 3$ elements. If $\mathrm{char}(K) = p$, then the rank of $G(K)/[P, P]$ and therefore also of $G(K)$ is infinite.

Denote the fixed field of $\Phi(G(K))$ in the separable closure K_s of K by F. We call it the **Frattini field** of K. By the preceding paragraph F is contained in the fixed field of $\Phi(P)$. The latter field is the compositum of all Galois extensions of T of degree p. We denote it by $T_{\mathrm{ab}}^{(p)}$.

The goal of this note is to identify F with another distinguished subfield of $T_{\mathrm{ab}}^{(p)}$. To this end we say that a field N is a **minimal Galois extension of K containing** T if N is a Galois extension of K which properly contains T such that no proper intermediate field between T and N is Galois over K; we let J be the compositum of all such N.

THEOREM A: $F = J$.

The field J has an interesting module theoretic interpretation. Let $G = \mathcal{G}(T/K)$ and consider the profinite group ring $\mathbb{F}_p[[G]] = \varprojlim \mathbb{F}_p[\mathcal{G}(L/K)]$, where L ranges over all finite tamely ramified extensions of K. As $V = \mathcal{G}(T_{\mathrm{ab}}^{(p)}/T)$ is a p-elementary abelian closed normal subgroup of $\mathcal{G}(T_{\mathrm{ab}}^{(p)}/K)$, the group ring $\mathbb{F}_p[[G]]$ acts on V. The **Jacobson radical** $\mathcal{J}$ of the $\mathbb{F}_p[[G]]$-module V is, by definition, the intersection of all maximal submodules of V (cf. [H, p. 462]). The fixed field of $\mathcal{J}$ in $T_{\mathrm{ab}}^{(p)}$ is J. We call J the **Jacobson field** of K.

The proof of Theorem A makes extensive use of the prosolvability of $G(K)$ and of the local nature of K. Global prosolvable Galois groups, on the other hand, do not seem to have interesting Frattini groups. Thus, for the maximal solvable extension $\mathbb{Q}_{\mathrm{solv}}$ of $\mathbb{Q}$ we prove:

THEOREM B: *The Frattini group of* $\mathcal{G}(\mathbb{Q}_{\mathrm{solv}}/\mathbb{Q})$ *is trivial.*

ACKNOWLEDGEMENT: This work was done during a visit of the first author in Augsburg University in winter 1990. He would like to thank the Albert Leimer Foundation for its support and the Institute for Mathematics of the University for its kind hospitality.

1. Identification of the Frattini field of K with its Jacobson field.

We retain the following notation of the introduction and fix them for the whole section:

K is a finite extension of $\mathbb{Q}_p$ or of $\mathbb{F}_p((t))$ with residue field $\mathbb{F}_q$,

T is the maximal tamely ramified extension of K,

F is the Frattini field of K, and

J is the Jacobson field of K,

Also, for a field L we denote the maximal p-elementary abelian extension of L by $L_{\mathrm{ab}}^{(p)}$. If L is a finite separable extension of K, we write $U_{1,L}$ for the group of 1-units of L. The field theoretic interpretation of the definition of the Frattini group identifies F with the compositum of all minimal separable extensions M of K. Our first result puts sharp restrictions on the Galois closure of such M.

The nontrivial case occurs where M/K is non-Galois. In this case, F contains, together with M, the compositum N of all K-conjugates of M. Thus N is the Galois closure of M/K.

Note that if L and N are Galois extensions of K such that N/L is abelian, then each extension of an element $\sigma \in \mathcal{G}(L/K)$ to N acts on $\mathcal{G}(N/L)$ by conjugation. This action is independent of the extension and therefore makes $\mathcal{G}(N/L)$ a $\mathcal{G}(L/K)$-module.

PROPOSITION 1.1: *Let M be a minimal separable non-Galois extension of K. Denote the Galois closure of M/K by N. Then either $[M{:}K] = l$ is prime, $l \neq p$, and N/K is tamely ramified, or $[M{:}K] = p^i$ and the maximal tamely ramified extension L of K in N satisfies:*

(a) *$M \cap L = K$, $ML = N$, M/K is totally ramified,*

(b) *N/L is a p-elementary abelian extension which is totally ramified,*

(c) *$G = \mathcal{G}(L/K)$ acts faithfully on $V = \mathcal{G}(N/L)$,*

(d) *V is an irreducible $\mathbb{F}_p[G]$-module,*

(e) *if M' is a minimal separable extension of K with the same Galois closure N, then M' is K-conjugate to M, and*

(f) *$\mathcal{G}(T/L)$ acts trivially on $\mathcal{G}(NT/T)$.*

Proof: Let x_1 be a primitive element for M/K and let $x_1, \ldots, x_m$ be its conjugates over

K. The action of $H = \mathcal{G}(N/K)$ on $\{x_1, \ldots, x_m\}$ represents it as a transitive permutation group of degree m. The stabilizer of x_1, i.e. $\mathcal{G}(N/M)$, is a maximal subgroup. Hence H is primitive [H, p. 147, Satz 1.4]. As H is solvable, we may therefore exploit Galois' theorem [H, p. 159, Satz 3.2]. In field theoretic terms this theorem is concerned with a maximal Galois extension L of K which is properly contained in N. For this field the theorem states that

(1a) $V = \mathcal{G}(N/L)$ is an elementary abelian group,

(1b) $L \cap M = K$, $LM = N$, in particular $\mathcal{G}(N/M) \cong \mathcal{G}(L/K)$ and $|V| = [M : K]$ is an l-power for some prime l,

(1c) V is its own centralizer in H,

(1d) L is the only maximal Galois extension of K which is properly contained in N, and

(1e) $\mathcal{G}(N/M)$ contains no normal nontrivial subgroup of l-power order.

(1f) If another minimal separable extension M' of K has the same Galois closure N as M, then M' is K-isomorphic to M.

As M is a minimal non-Galois extension of K, it is totally ramified. If $l \neq p$, then M/K is tamely ramified. Hence $M = K(a^{1/l^r})$ for some $a \in K$ and a positive integer r [L2, p. 52]. The minimality of M implies that $[M{:}K] = l$. Each of the conjugates of M over K is tamely ramified over K. Hence their compositum N is also tamely ramified over K.

So, we consider the case where $l = p$. By (1b), condition (1e) holds also for $\mathcal{G}(L/K)$. Consider therefore the maximal tamely ramified extension L_1 of K in L. As $\mathcal{G}(L/L_1)$ is a normal p-subgroup of $\mathcal{G}(L/K)$, it must be trivial. So, L is a tamely ramified extension of K. Since $[M{:}K]$ is a p-power, N/L is a totally and wildly ramified extension. It follows that L is the maximal tamely ramified extension of K contained in N.

The group $G = \mathcal{G}(L/K)$ acts on V through $\mathcal{G}(N/M)$ by conjugation. Condition (1c) means that this action is faithful. The minimality of V as a normal subgroup of H (Condition (1d)) means that V contains no proper nontrivial $\mathbb{F}_p[G]$-submodule. This means that V is an irreducible $\mathbb{F}_p[G]$-module.

Finally observe that $\mathcal{G}(NT/L) = \mathcal{G}(NT/T) \times \mathcal{G}(NT/N)$. Hence $\mathcal{G}(T/L)$ acts trivially on $\mathcal{G}(NT/T)$. ∎

Proposition 1.1 supplies a new proof to the assertion, which has already been mentioned in the introduction, that $F \subseteq T_{\mathrm{ab}}^{(p)}$. The next corollary is already an improvement of this.

COROLLARY 1.2: $F \subseteq J$.

Proof: Let M be a minimal separable extension of K. If M/K is Galois, then, since $\mathcal{G}(M/K)$ is solvable, it is isomorphic to $\mathbb{Z}/l\mathbb{Z}$ for some prime l. Hence, $M \subseteq J$. If M/K is non-Galois, then, by Proposition 1.1, either $M \subseteq T$, or M is linearly disjoint from T over K. In the latter case, Proposition 1.1, implies that the Galois closure N of M/K is a minimal Galois extension of K containing L, and N is linearly disjoint from T over L. Hence, NT is a minimal Galois extension of K containing T. So, $NT \subseteq J$. Conclude that $F \subseteq J$. ∎

To get a lower bound for F consider positive integers e, f which satisfy

$$q^f \cong 1 \bmod e. \tag{1}$$

Denote the unique unramified extension of K of degree f by U_f. Let π be a prime element of K, and let $T_{e,f} = U_f(\sqrt[e]{\pi}) = U_f \cdot K(\sqrt[e]{\pi})$. Then $T_{e,f}$ is a **split** tamely ramified Galois extension of K. The Galois group $G = \mathcal{G}(T_{e,f}/K)$ is generated by two elements σ, τ with the following relations [Ha, Section 16, p. 252 with $r = 0$ or I p. 458 for the number field case].

$$\sigma^f = 1, \quad \tau^e = 1, \quad \sigma\tau\sigma^{-1} = \tau^q. \tag{2}$$

We say that $T_{e,f}$ is **faithful** if in addition to (1)

$$q^j \ncong 1 \bmod e \qquad \text{for each } 1 \le j < f. \tag{3}$$

The reason for this name becomes clear in the following lemma:

LEMMA 1.3: *Let $T_{e,f}$ be a split tamely ramified faithful Galois extension of K. Then there exists an irreducible $\mathbb{F}_p[G]$-module V on which G acts faithfully.*

Proof: Let $\zeta = \zeta_e$ be a primitive root of 1 of order e in $\widetilde{\mathbb{F}}_p$. Consider the field $U = \mathbb{F}_{q^f}$ as a vector space over $\mathbb{F}_q$. By (1), $\zeta \in U$. So, G acts on U by the following rule:

$$\sigma(x) = x^q, \quad \tau(x) = \zeta x, \tag{4}$$

(Check that relations (2) are satisfied.)

Thus U is an $\mathbb{F}_q[G]$-module. We prove that U is irreducible by proving that the $\mathbb{F}_q[G]$-module generated by each nonzero $u \in U$ is equal to U.

Indeed, let $[\mathbb{F}_q(\zeta):\mathbb{F}_q] = j$. Then $\zeta^{q^j} = \zeta$. Hence $q^j \cong 1 \bmod e$, and, by (3), $j = f$. So, $U = \mathbb{F}_q(\zeta)$. Now consider the trace function Tr from U to $\mathbb{F}_q$. As $U/\mathbb{F}_q$ is separable, the function $x \mapsto \mathrm{Tr}(xu)$ from U to $\mathbb{F}_q$ is nonzero [L1, p. 211]. Therefore, since the powers of ζ generate U as a vector space over $\mathbb{F}_q$, there exists k such that $c = \mathrm{Tr}(\zeta^k u) \neq 0$. But $\mathrm{Tr}(\zeta^k u) = \sum_{i=0}^{f-1} \sigma^i\tau^k(u)$ belongs to $\mathbb{F}_q[G](u)$. Hence, $1 = c^{-1}c$ belongs to $\mathbb{F}_q[G](u)$ and therefore $\mathbb{F}_q[G](u) = \mathbb{F}_q[G]$, as asserted.

Next we observe that G acts faithfully on U. Indeed, suppose that $\tau^i\sigma^j$, with $0 \leq i < e$ and $0 \leq j < f$, acts trivially on U. In particular $\zeta^i = \tau^i\sigma^j(1) = 1$. Hence, $i = 0$ and therefore $\tau^i = 1$. So, $u = \sigma^j u$ for every $u \in U$. Conclude that $\sigma^j = 1$, as claimed.

Finally, we may consider U also as an $\mathbb{F}_p[G]$-module. As such it is isomorphic to the direct sum $V \oplus \cdots \oplus V$ for some irreducible $\mathbb{F}_p[G]$-module V [HB, p. 18, Thm. 1.16(d)]. Obviously, G acts faithfully on V. So, V is the $\mathbb{F}_p[G]$-module we are looking for. ∎

LEMMA 1.4: *Each split tamely ramified faithful Galois extension $T_{e,f}$ of K is contained in F.*

Proof: Factor the multiplicative group $T_{e,f}^\times$ of $T_{e,f}$ as $T_{e,f}^\times = \langle \sqrt[e]{\pi} \rangle \times W \times U_1$, where W is the finite group of all roots of unity whose order is relatively prime to p, and U_1 is the group of 1-units of $T_{e,f}$. For each $\rho \in G$ there exists i such that $\rho(\sqrt[e]{\pi}) =$

$\zeta_e^i \sqrt[e]{\pi}$. Obviously, W and U_1 are G-invariant. Hence, the factor group U_1/U_1^p is a direct summand of the $\mathbb{F}_p[G]$-module $T_{e,f}^\times/(T_{e,f}^\times)^p$.

Iwasawa proves for $\mathrm{char}(K) = 0$ that $\mathbb{F}_p[G]$ is a direct $\mathbb{F}_p[G]$-summand of U_1/U_1^p (This is implicit in [I, Thm. 1]. It is reproved by Pieper [P, Axiom 2 on p. 176 and Hilfatz 13 on p. 199]). For $\mathrm{char}(K) = p$, Koch [K, Satz 1] proves that $U_1 \cong \mathbb{Z}_p[G]^{\mathbb{N}}$, as $\mathbb{Z}_p[G]$-modules. So, the assertion holds also in this case. In particular, $\mathbb{F}_p[G]$ is an $\mathbb{F}_p[G]$-quotient of $T_{e,f}^\times/(T_{e,f}^\times)^p$. By Lemma 1.3, $\mathbb{F}_p[G]$ has an irreducible module V on which G faithfully acts. Choose a nonzero $v \in V$ and extend the map $1 \mapsto v$ to a homomorphism $\mathbb{F}_p[G] \to V$ of $\mathbb{F}_p[G]$-modules. As V is irreducible, this map is surjective.

On the other hand, $\mathcal{G}(T_{e,f,\mathrm{ab}}^{(p)}/T_{e,f})$ is a p-elementary abelian group on which G acts. The reciprocity map of local class field theory induces an isomorphism of $T_{e,f}^\times/(T_{e,f}^\times)^p$ onto $\mathcal{G}(T_{e,f,\mathrm{ab}}^{(p)}/T_{e,f})$ as $\mathbb{F}_p[G]$-modules [CF, p. 142]. Hence, by the preceding paragraph V is an $\mathbb{F}_p[G]$-quotient of $\mathcal{G}(T_{e,f,\mathrm{ab}}^{(p)}/T_{e,f})$.

In Galois theoretic terms this means that there is a finite Galois extension N of K containing $T_{e,f}$ such that $\mathcal{G}(N/T_{e,f}) \cong V$, and V is its own centralizer in $\mathcal{G}(N/K)$. As $\mathcal{G}(N/K)$ is solvable, a field theoretic interpretation of [H, p. 160, Satz 3.3] gives a minimal extension M of K whose Galois closure is N. Conclude that N and therefore also $T_{e,f}$ are contained in F. ∎

LEMMA 1.5: *Each tamely ramified extension L of K is contained in the compositum of two faithful split tamely ramified extensions of K.*

Proof: Let $T_{e,f}$ be a split tamely ramified extension of K that contains L. Consider the sequence $D_n = (q^n - 1)/(q - 1)$, $n = 1, 2, 3, \ldots$. Like the Fibonacci sequence, D_n is a second order recurring sequence. Carmichael [C, Thm. XXIII] proves that for each $n > 12$, D_n has a **primitive factor** e_1. That is $e_1 \neq 1$, e_1 divides D_n, but is relatively prime to D_m for each $m < n$. Also, each prime factor l of $q - 1$ divides $D_{n(l)}$ for some positive integer $n(l)$. Hence, if f_1 is a multiple of f which is larger than 12 and than $n(l)$ for each l that divides $q - 1$, then D_{f_1} has a primitive divisor e_1 which will satisfy $q^{f_1} \cong 1 \bmod e_1$ but $q^j \ncong 1 \bmod e_1$, for $1 \leq j < f_1$. Thus T_{e_1,f_1} is faithful and split.

Now, let $f_2 = \mathrm{ord}_e q$. Then $q^{f_2} \cong 1 \bmod e$ and $q^j \ncong 1 \bmod e$ for each $1 \leq j < f_2$.

Hence T_{e,f_2} is also faithful and split. Conclude the proof by observing that $T_{e,f} \subseteq T_{e_1,f_1}T_{e,f_2}$. ∎

Combine Lemmas 1.4 and 1.5:

COROLLARY 1.6: $T \subseteq F$.

LEMMA 1.7: *Let N be a minimal Galois extension of K containing T. Then N/T is a finite p-elementary abelian extension and $N \subseteq F$.*

Proof: Choose $x \in N - T$ and let N_0 be the Galois closure of $K(x)/K$. Then TN_0 is contained in N and normal over K. So, the minimality of N implies that $TN_0 = N$. In particular N/T is finite. As an extension of T, N is totally and wildly ramified. Thus $V = \mathcal{G}(N/T)$ is a p-group, which because of the minimality, must be elementary abelian.

Embed V in a p-Sylow group P of $\mathcal{G}(N/K)$. Observe that P/V is a p-Sylow group of $G = \mathcal{G}(T/K)$. The latter is isomorphic to $\mathbb{Z}_p$. As $\mathbb{Z}_p$ is projective, the short exact sequence $1 \to V \to P \to \mathbb{Z}_p \to 0$ splits. In other words, V has a complement in P. As $\gcd(|V|, (\mathcal{G}(N/K):P)) = 1$, a theorem of Gaschütz [FJ, Lemma 20.46] states that V has a complement in $\mathcal{G}(N/K)$.

Alternatively, follow Jannsen [J, Satz 3.1] to observe that $\mathrm{cd}_p G = 1$. As V is a p-group, this implies that the short exact sequence $1 \to V \to \mathcal{G}(N/K) \to G \to 1$ splits [R, p. 211].

Thus, K has an extension M such that $T \cap M = K$ and $TM = N$. As T/K is Galois, M is linearly disjoint from T over K. Let M_0 be a minimal extension of K which is contained in M. By Proposition 1.1, there exists a tamely ramified extension L_0 of K such that $\widehat{M_0} = L_0M_0$ is the Galois closure of M_0/K. As $T\widehat{M_0} \subseteq N$ is Galois over K, the minimality of N implies that $T\widehat{M_0} = N$. Hence $[M_0 : K] = [N : T] = [M : K]$ and therefore $M = M_0$ is a minimal extension of K. Thus $M \subseteq F$. Conclude from Corollary 1.6 that $N = TM \subseteq F$, as desired. ∎

Combine Corollary 1.2 with Lemma 1.7 to obtain our main result:

THEOREM 1.8: $F = J$.

REMARK 1.9: *The field F is properly contained in $T_{\mathrm{ab}}^{(p)}$.* Let L be an unramified extension of K of degree p^m, for $m \geq 2$. Then $G = \mathcal{G}(L/K)$ is a cyclic group of order p^m. We have already mentioned in the proof of Lemma 1.4 that $\mathbb{F}_p[G]$ is an $\mathbb{F}_p[G]$-quotient of $L^\times/(L^\times)^p$. So, by the local reciprocity law, L has an extension N which is Galois over K such that $\mathcal{G}(N/L)$ is isomorphic to $\mathbb{F}_p[G]$ as $\mathbb{F}_p[G]$-modules. As G is a p-group, the Jacobson radical of $\mathbb{F}_p[G]$ is a vector space of dimension $p^m - 1$ over $\mathbb{F}_p$ [H, p. 484]. In particular it is nontrivial. It follows that N is not contained in J and therefore, by Theorem 1.8, also not in F. On the other hand, $N \subseteq T_{\mathrm{ab}}^{(p)}$. Hence $F \neq T_{\mathrm{ab}}^{(p)}$, as claimed. ∎

REMARK 1.10: *The structure of $\mathcal{G}(F/T)$ as a $\mathcal{G}(T/K)$-module.* For each large integer f, Carmichael's theorem mentioned in the proof of Lemma 1.5 and Lemma 1.3 gives a minimal Galois extension $N_{e,f}$ of K containing $T_{e,f}$ such that $N_{e,f}/T_{e,f}$ is a totally ramified extension of degree q^f. Then $TN_{e,f}$ is a minimal Galois extension of K containing T and $[TN_{e,f} : T] = q^f$. As each $TN_{e,f}$ is contained in $J = F$, we have $[F : T] = \infty$.

We may now construct a sequence $N_1, N_2, N_3, \ldots$ of minimal Galois extensions of K containing T which is linearly disjoint over T such that $F = N_1N_2N_3\cdots$. Indeed, choose a sequence $x_1, x_2, x_3, \ldots$ of generators for F/T. Suppose that $N_1, \ldots, N_k$ have already been defined. Let $n(k)$ be the least integer such that $x_{n(k)} \notin N_1 \cdots N_k$. By definition of J, there exists a minimal Galois extension N_{k+1} of K containing T which contains $x_{n(k)}$. The minimality of N_{k+1} implies that $N_1 \cdots N_k \cap N_{k+1} = T$. So, $N_1, \ldots, N_{k+1}$ are linearly disjoint over T. Conclude by induction that the sequence $N_1, N_2, N_3, \ldots$ satisfies the above requirements.

Note, that this sequence presents the $\mathcal{G}(T/K)$-module $\mathcal{G}(F/T)$ as a direct sum: $\mathcal{G}(F/T) \cong \bigoplus_{i=1}^{\infty} \mathcal{G}(N_i/T)$.

For each i, the proof of Lemma 1.7 provides a minimal separable extension M_i of K which is totally and wildly ramified such that $TM_i = N_i$. As each M_i is linearly disjoint from T over K and as $N_1, N_2, N_3, \ldots$ are linearly disjoint over T, the sequence $M_1, M_2, M_3, \ldots$ is linearly disjoint over K. ∎

REMARK 1.11: *The Fitting group of a profinite group.* The product of two closed normal pronilpotent subgroups M and N of a profinite group G is pronilpotent. Indeed, for each p, the p-Sylow subgroups M_p and N_p of M and N, respectively, are normal and therefore so is the p-Sylow subgroup M_pN_p of MN. It follows that G has a unique closed normal pronilpotnet subgroup $\mathrm{F}(G)$, called the **Fitting** group of G, which contains all closed normal pronilpotent subgroups of G. As $\Phi(G)$ is pronilpotent [FJ, Lemma 20.2], it is contained in the Fitting group of G.

Pop [P, Satz 1.4] proves that for the case that K is a finite extension of $\mathbb{Q}_p$ that if H is a closed normal subgroup of $G(K)$, then $H \cap G(T)$ is nontrivial. As $G(T)$ is a pro-p-group, this implies that $\mathrm{F}(G(K))$ is a pro-p-group that contains $G(T)$. Let L' be the fixed field of $\mathrm{F}(G(K))$. Then L' is contained in T and contains the fixed field L of the p-Sylow group of $\mathcal{G}(T/K)$ in T. As the maximal unramified p-extension U of K has Galois group isomorphic to $\mathbb{Z}_p$, and since p does not divide the order of $\mathcal{G}(T/U)$, the extension T/L is unramified and $\mathcal{G}(T/L) \cong \mathbb{Z}_p$. So, for the residue fields, we get $G(\overline{L}) = \mathcal{G}(\overline{T}/\overline{L}) \cong \mathcal{G}(T/L) \cong \mathbb{Z}_p$.

Let now π be a prime element of K. For each integer m prime to p the polynomial $X^m - \pi$ is, by Eisenstein criterion, irreducible over K. Hence $X^m - \pi$ has a root in L, and therefore also in L'. Since L' is normal over K, all roots of $X^m - \pi$ belong to L'. Hence, the mth root of unity ζ_m belongs to L'. It follows that $\zeta_m \in \overline{L'}$, and therefore $\overline{L'} = \widetilde{F}_p$. Conclude that $L' = T$ and that therefore $G(T)$ is the Fitting group of $G(K)$. This gives an alternative proof for Corollary 1.6. ∎

2. The Frattini group of global Galois groups.

In contrast to the local case the Frattini group of $G(K)$ for a global field K is trivial. The same holds even if we replace $G(K)$ by its maximal solvable quotient. In view of Remark 1.11, we show that this is already true for the Fitting group. As our arguments are based on Hilbert Irreducibility theorem, which global fields satisfy, we state and prove the results of this section for arbitrary Hilbertian fields.

LEMMA 2.1: *Let N be a Galois extension of a Hilbertian field K with Galois group G. If the order of $\mathrm{F}(G)$ is divisible by at least two distinct primes, then N is Hilbertian.*

Proof: Let F be the fixed field in N of $\mathrm{F}(G)$. Then F is a Galois extension of K. Choose a prime divisor p of $[N{:}F]$. Denote the maximal p-extension of F in N by F_p. Let F_p' be the compositum of all Galois extensions of F whose orders are relatively prime to p. Since $\mathcal{G}(N/F)$ is pronilpotent, both fields F_p and F_p' are Galois over K and they are proper extensions of F. Also, $F_p \cap F_p' = F$ and $F_p F_p' = N$.

If F_p is a finite extension of F, then N is a finite proper extension of F_p'. By a theorem of Weissauer [FJ, Cor. 12.15], N is Hilbertian.

If $[F_p{:}F] = \infty$ choose a finite extension F' of F which is contained in F_p. By Weissauer's theorem, F' is Hilbertian. Also, $\mathcal{G}(N/F') \cong \mathcal{G}(F_p/F') \times \mathcal{G}(F'F_p'/F_p')$ is a pronilpotent group whose order is divisible by two distinct primes. By a theorem of Kuyk ([Ku, an immediate corollary of Thm. 1] or [U, Thm. 3]), N is Hilbertian. ∎

THEOREM 2.2: *Let K be a Hilbertian field. Then the Fitting and the Frattini groups of both $G(K)$ and $\mathcal{G}(K_{\mathrm{solv}}/K)$ are trivial.*

Proof: Theorem 15.10 of [FJ] states that if N is a Galois extension of K and N is not separably closed, then $G(N)$ is not prosolvable. Since $\mathrm{F}(G(K))$ is pronilpotent and normal, this implies that $\mathrm{F}(G(K)) = 1$.

Now consider the fixed field F of $\mathrm{F}(\mathcal{G}(K_{\mathrm{solv}}/K))$ in K_{solv}. Assume that $F \neq K_{\mathrm{solv}}$. If $[K_{\mathrm{solv}} : F] < \infty$, then, by Weissauer's theorem, K_{solv} were Hilbertrian. This would imply that K_{solv} has a quadratic extension, which is impossible. Hence $[K_{\mathrm{solv}} : F] = \infty$.

So, choose a finite extension F' of F contained in K_{solv}. Again, F' is Hilbertian. Hence, F' has a quadratic extension and a cubic Galois extension [FJ, Thm. 24.48].

Both extensions are contained in K_{solv}. Hence, the order of $[K_{\mathrm{solv}} : F]$ is divisible by 2 and 3. By Lemma 2.1, K_{solv} is Hilbertian. Conclude from this contradiction that $\mathrm{F}(\mathcal{G}(K_{\mathrm{solv}}/K)) = 1$. ∎

EXAMPLE 2.3: *The maximal p-extension.* Let K be a Hilbertian field. Then K has a Galois extension L such that $\mathcal{G}(L/K) \cong \mathbb{Z}/p\mathbb{Z}$ [FJ, Thm. 24.48]. Hence, by [FJ, Prop. 24.47], K has a Galois extension N such that $\mathcal{G}(N/K) \cong \mathbb{Z}/p\mathbb{Z} \operatorname{wr} \mathbb{Z}/p\mathbb{Z}$. The latter group is a nonabelian p-group. It follows that $K_{\mathrm{ab}}^{(p)} \neq K^{(p)}$. Hence, $\Phi(\mathcal{G}(K^{(p)}/K)) = \mathcal{G}(K^{(p)}/K_{\mathrm{ab}}^{(p)})$ is nontrivial. ∎

References

[C] R.D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$,* Annals of Mathematics **15** (1913–1914), 30–70.

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

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

[H] B. Huppert, *Endliche Gruppen I,* Springer, Berlin, 1967.

[Ha] H. Hasse, *Number Theory,* Grundlehren der mathematischen Wissenschaften **229**, Springer, Berlin, 1980.

[HB] B. Huppert and N. Blackburn, *Finite Groups II,* Springer, Berlin, 1982.

[I] K. Iwasawa, *On Galois groups of local fields,* Transactions of the AMS **80** (1965), 448–469.

[J] U. Jannsen, *Über Galoisgruppen lokaler Körper,* Inventiones mathematicae **70** (1982), 53–69.

[K] H. Koch, *Über die Galoische Gruppe der algebraischen Abschließung eines Potenzreihenkörpers mit enlichem Konstantenkörper*, Math. Nachrichten **35** (1967), 323–327.

[Ku] W. Kuyk, *Extensions de corps hilbertiens,* Journal of algebra **14** (1970), 112–124.

[L1] S. Lang, *Algebra,* Addison-Wesley, Reading, 1965.

[L2] S. Lang, *Algebraic Number Theory,* Addison–Wesley, Reading, 1970.

[P] H. Pieper, *Die Einheitengruppe eines zahm-verzweigten galoisschen lokalen Körpers als Galois-Modul,* Mathematische Nachrichten **54** (1972), 173–210.

[Po] F. Pop, *Galoissche Kennzeichnung p-adisch abgeschlossener Körper,* Journal für die reine und angewandte Mathematik **392** (1988), 145–175.

[R] L. Ribes, *Introduction to Profinite Groups and Galois Cohomology,* Queen's papers in pure and applied Mathematics **24**, Queen's University, Kingston, 1970.

[S] J.-P. Serre, *Local Fields,* Springer, New York, 1979.

[U] K. Uchida, *Separably Hilbertian fields,* Kodai Mathematical Journal **3** (1980), 83–95.

Addresses of the authors:

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

Jürgen Ritter
Institut für Mathematik
Universität Augsburg
W-8900 Augsburg
GERMANY