PLISKA
STUDIA MATHEMATICA BULGARICA
ПЛИСКА
БЪЛГАРСКИ МАТЕМАТИЧЕСКИ СТУДИИ

For further information on
Pliska Studia Mathematica Bulgarica
visit the website of the journal http://www.math.bas.bg/~pliska/
or contact: Editorial Office
Pliska Studia Mathematica Bulgarica
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Telephone: (+359-2)9792818, FAX:(+359-2)971-36-49
e-mail: pliska@math.bas.bg

MAXIMAL SUBFIELDS AND ALGEBRAIC PROPERTIES OF FIELDS

IVAN D. CHIPCHAKOV

In this paper U-fields are characterized in temrs of maximal subfields of their algebraic closures in case of a saturated class U of finite groups. A simple link between the maximal perfect subfield of a field and its purely inseparable closure is proved to exist. The q-maximal problem is considered in detail.

Preliminary remarks. In this paper U will always mean a class of finite groups. A field K is said to be an U-field in its normal extension L iff for any subfield of L which is a Galois extension M of K the Galois group $G(M/K)$ is an element of U. A field is said to be an U-field iff it is an U-field in its algebraic closure.

Definition 1. *A class U (of finite groups) is said to be regular iff U is closed with respect to taking subgroups, quotient groups and finite direct products. A regular class U is called saturated iff for any finite group G such that $G/\Phi(G)\in U$, $\Phi(G)$ being the Frattini subgroup of G, it follows that $G\in U$.*

Regular (saturated) classes of finite groups are closed with respect to intersections. A union of a chain of regular (saturated) classes is regular (saturated). Examples of saturated classes are numerous: the class of all finite groups satisfying (β), (β) being any of the following properties: solvable; supersolvable; nilpotent; Π-groups, i. e. any prime multiple of the order of any group belonging to the class of Π-groups is an element of a fixed set of primes Π; if $\prec$ is a fixed linear order of the set of all prime numbers, we shall sign by $(\prec)$ the class of all finite groups such that $G\in(\prec)$ iff $|G|=p_1^{k_1}\ldots p_s^{k_s}$, $p_1\prec p_2\prec\cdots\prec p_s$, $k_l\geqq 0$, $l=1,\ldots,s$, $p_l\in\Pi$, and such that there exists a Hall normal $\{p_1,\ldots,p_r\}$-subgroup of G for all $r=1,\ldots,s$; if T is a class of finite simple groups containing all groups of prime order, then a finite group G satisfies the condition (β, T) iff any simple group isomorphic to a quotient group of some subgroup of G belongs to T. The class of all finite groups satisfying a fixed set of group laws is regular. References on some of the examples listed above may be found in [3].

In this paper a characterization of U-fields is presented in case of a saturated class U. Examples based on different ideas are presented thus giving a positive answer to a question in [2] — see example (iii).

The relations among some field K, its maximal perfect subfield and the minimal perfect subfield of the algebraic closure $\bar{K}$ of K containing K is presented characterizing as a partial case the fields whose finite extensions are always simple thus linking the results in [5] on such fields.

PLISKA Studia mathematica bulgarica. Vol. 8, 1986, p. 158—168.

The q-maximal problem — whether a proper subfield K of a field L is q-maximal in L, i. e the set of subfields of L containing K is linearly ordered with respect to set theory inclusion, iff for some $\xi \in L$, K is a maximal subfield of L disjoint from ξ — is considered in detail. Some general situation provides a positive solution however, although its conditions are proved to be essential they are not necessary to have a positive solution.

Definition 2. *A field K, $\mathrm{ch}\, K=p>0$, is said to be imperfect of degree α ($\mathrm{imp}\, K=\alpha$) iff α is the highest cardinality of a subset T of $K_{p^{-1}}$: $=\{s \in \overline{K}: s^p \in K\}$ such that for any natural number k and any two-by-two different elements $\alpha_1, \ldots, \alpha_k$ of T, $[K(\alpha_1, \ldots, \alpha_k): K]=p^k$.*

In this paper complete proofs of the results announced in [1] are presented — up to [1, Th. 5], the rest of the results in [1] having been proved in [2].

Fields of positive characteristics. In [5, Th. 3] it is proved that any finite extension of a field K is simple iff no extension of K contains two distinct purely inseparable extensions of K of the same degree and besides if $K=k(x)$, x — transcendental over k the property referred to is equivalent to k being perfect. The following result in this paper links the results in [5] referred to.

Theorem 1. *Let K be a field, K_0 — its maximal perfect subfield. Then $\mathrm{imp}\, K \leqq \deg_{K_0} K$, $\deg_{K_0} K$ being the transcendency degree of K over K_0.*

Corollary 1. *Let K be a field. The following conditions are equivalent:*

(i) *Every finite extension of K is simple;*

(ii) $\mathrm{imp}\, K \leqq 1$;

(iii) *K is a q-maximal subfield of some perfect field.*

The equivalence of (i) and (iii) is announced in [1, Th. 3 (v)].

On U-fields. The following two results prove the existence of cyclic fields and U-fields, U — saturated — due to Zorn's lemma as well as to the fact [9, Th. 2] that profinite groups can be interpreted as Galois groups of appropriate field extensions.

Theorem 2. *Let U be a saturated class of finite groups, L — a proper normal extension of a field K. Then K is an U-field in L iff there exists a subset S of L such that K is a maximal subfield of L without S (i. e with respect to disjointness from S) and for any, α-separable over K, $G(K_\alpha \mid K)$ is an element of U, $G(K_\alpha \mid K)$ being the Galois group of the minimal Galois extension K_α of K in L containing α* (see [1, Th. 3 (i)]).

Corollary 2. *Let L be a proper normal extension of a field K.*

(i) *K is supersolvable (nilpotent) in L iff there exists a subset S of L such that K is a maximal subfield of L without S and $[K(\alpha): K]$ is a prime number ($K(\alpha)$ is a normal extension of K in the nilpotent case) for any $\alpha \in S$ (see* [1, Th. 3 (ii)]).

(ii) *K is cyclic in L iff for some subset S of L, K is a maximal subfield of L without S and for any two different elements α, β of S separable over K, $[K(\alpha): K] \neq [K(\beta): K]$ [see* (1, Th. 3 (iii))].

(iii) *For every $n \in N$ there exists at most a single extension of K in L of dimension n, L being either perfect or separable over K, iff for some subset S of L, K is a maximal subfield of L without S and for any $\alpha \in S$, $\beta \in S$: $\alpha \neq \beta$, $[K(\alpha): K] \neq [K(\beta): K]$ (see* [1, Th. 3 (iv)]).

We shall remark that quasi-finite fields defined by Serre are characterized in [8, Ch. XIII, § 2, Ex. 1] in a way analogous to (ii) and (iii) — the specific properties of quasi-finite fields having been taken into consideration as well. In case of an algebraically closed field (AC field) L one can get most of the

results on maximal subfields of an *AC* field disjoint from one or two elements proved in (6) and (4), directly applying Corollary 2.

Corollary 3. *Let L be an AC field,* $\mathrm{ch}\,L=0$.

(i) *For any saturated class of finite solvable groups U, there exists a subfied L_0 of L such that L is algebraic over L_0 and for any finite extension K of L_0 (in L), the elements of U are exactly the finite groups realized as Galois groups of certain finite Galois extensions of K* [1, Th. 4].

(ii) *Any $\{p\}$-field L_1 in L, p—prime, is an algebraic extension of a field L_0 satisfying the conditions in* (i) *regarding the class of all finite p-groups* [1, Th. 5].

Clearly by "digging holes" one can prove the existence of U-fields of any characteristics for any saturated class U. However, this is by no means the only way to be used. The following example is based on the theory of complete fields with respect to a discrete valuation. It gives a positive answer to a question in [2] — whether there exists a nilpotent field and a central associative division algebra over this field of finite dimension which is not a power of a prime number.

Example. (i) Let K be a complete field with respect to a discrete valuation such that the residue field $\widetilde{K}:=\rho/m$ is solvable, ρ being the valuation ring of K, i. e. $\rho:=\{\alpha\in K: |\alpha|\leq 1\}$, while $m:=\{\alpha\in\rho: |\alpha|<1\}$ is its single maximal ideal, $|\ |$ is the valuation of K referred to — see [15, Ch. XII]. If $\widetilde{K}$ is perfect, then K is solvable.

(ii) Let K be an abelian perfect field containing all primitive n-th roots of unity for all n (if $\mathrm{ch}\,K=q>0$ we assume $(n, q)=1$). Then the field $K((x_1, \ldots, x_m))$, $m\in N$, of formal power series of m algebraically independent variables $x_1, \ldots, x_m$ over K is abelian if $\mathrm{ch}\,K=0$. If $\mathrm{ch}\,K=q>0$ then a field K_1 which is a maximal algebraic extension of $K((x_1))$ with respect to the property that any subextension of $K((x_1))$ of finite dimension contained in K_1 is of dimension over $K((x_1))$ which is a power of q, is a perfect abelian field.

(iii) If K is as in (ii) and besides for any prime $p\neq\mathrm{ch}\,K$ there exists an extension of K of dimension p, then there exists a central division algebra of dimension p^2 over $K((x_1))$ in case $\mathrm{ch}\,K=0$ (over K_1 in case $\mathrm{ch}\,K\neq 0$).

Quasi-maximal problem. F. Quigley has proved in [6] that the q-maximal problem has a positive solution if L is an AC field. As for [6, Th. 2] it may be extended in a natural way in terms of the q-maximal problem. Moreover, this extension proves to be in a sense the maximal possible due to the following result.

Theorem 3. (i) *Let L be a proper normal extension of K. If L is perfect or if L is a Galois extension of K, then the q-maximal problem is solved positively.*

(ii) *The field $L=GF(p)(x, y, z, \sqrt[p]{x+yz^p})$, p — prime, x, y, z — algebraically independent over $GF(p)$ is a normal extension of $K=GF(p)(x, y, z^{p^2})$, K is a maximal subfield of L without z^p but is not q-maximal.*

(iii) *Let K be a finite extension of the field of rationals Q. Then there exist sets M_1, M_2 both of continuum cardinality whose elements are two-by-two K-unisomorphic algebraic extensions of K such that for any $F_1\in M_1$ $\times(F_2\in M_2)$ there exists no proper q-maximal subfield of F_1 containing K (K is a q-maximal subfield of F_2).*

Corollary 4. *Let K be an ordered field as in Theorem 3* (iii). *Then M_1, M_2 exist as in Theorem 3,* (iii) *whose elements have the property to be*

ordered fields. F_2 is normal over no of its proper subfields containing K.

The case $K=Q$ provides examples of "many" unisomorphic algebraic extensions F of Q containing no q-maximal subfield but F.

Corollary 5. *Let L be a Galois extension of a field K and let M be an extension of K in L which is an U-field in L. Then M contains a subfield M_0 which is minimal with respect to being an U-field in L containing K (hence any q-maximal subfield of L containing K contains a subfield M_0 which is minimal with respect to being a q-maximal subfield of L containing K).*

Proofs and remarks. Proof of Theorem 1. If K is perfect $\operatorname{imp} K = \deg_{K_0} K = 0$. Let $\operatorname{ch} K = p > 0$, $K \neq K_0$. Due to the maximum condition on K_0 any element of $K \setminus K_0$ is transcendental over K_0. A finite set of elements $t_1, \ldots, t_k$ of the algebraic closure $\bar{K}$ of K is algebraically independent over K_0 iff $t_1^{p^{l_1}}, \ldots, t_k^{p^{l_k}}$ are algebraically independent over K_0 for any fixed non-zero integers $l_1, \ldots, l_k$. As $K_0(\sqrt[p]{t_1}, \ldots, \sqrt[p^k]{t_1}, \ldots)$ is perfect, there exists a transcendency basis B of K over K_0 such that for any $\alpha \in B$, $\sqrt[p]{\alpha} \in K$. So $[K(\sqrt[p]{\alpha_1}, \ldots, \sqrt[p]{\alpha_k}) : K] = p^k$ for any k two-by-two different elements of B, $k \in N$. Theorem 1 is proved.

Proof of Corollary 1. Let every finite extension of K be simple. As $[K(S) : K]$ equals either 1 or p for any $s \in Kp^{-1}$ it follows that $\operatorname{imp} K \leqq 1$. Let $\operatorname{imp} K \leqq 1$. If $\operatorname{imp} K = 0$ then K is perfect, so Corollary 1 (iii) is evident. Let $\operatorname{imp} K = 1$, i. e. for some element α of K the p-th root of α $\sqrt[p]{\alpha} \notin K$. Let $L = K(\sqrt[p]{\alpha}, \ldots, \sqrt[p^k]{\alpha}, \ldots)$. We shall prove that L is perfect and K is a q-maximal subfield of L. Let $L_k := K(\sqrt[p^k]{\alpha})$. For any polynomial $f_k(x) \in L_k[x]$, $(f_k(x))^p = \tilde{f}_k(x^p)$, $\tilde{f}_k(x) \in L_{k-1}[x]$. As L_1 is the only purely inseparable extension of K in $\bar{K}$ of dimension $p = \operatorname{ch} K$, it follows that f_1 is irreducible over L_1 iff $\tilde{f}_1$ is irreducible over K, hence L_2 is the only purely inseparable extension of L_1 in $\bar{K}$ of dimension p. By induction L_k is proved to be the only inseparable extension of $L_{k-1}(L_0 := K)$ in $\bar{K}$ of dimension p for any natural k, hence L is perfect. Our considerations prove also that any simple purely inseparable extension of K in $\bar{K}$ of dimension p^k equals L_k, so K, L_k, $k \in N$, L are all (two-by-two different) subfields of L containing K, i. e K is a q-maximal subfield of L.

The implication (iii) $\rightarrow$ (i) is trivial if K is perfect. Otherwise as K is a q-maximal subfield of a perfect field $\tilde{L}$, $\tilde{L}$ is purely inseparable over K with an analogous lattice of subfields containing K to the respective lattice of subfields of L over K. So if $\xi \in \bar{K}$, $s \in N \cup \{0\}$ is the least number such that ξ^{p^s} is separable over K, $p = \operatorname{ch} K$, then $K(\xi) = K(\xi^{p^s}, \sqrt[p^s]{\alpha})$. Combining this fact with the well-known result that finite separable extensions of K are simple we prove Corollary 1 (α is assumed to belong to $K \setminus K^p$).

Proof of Theorem 2. Assume the opposite, i. e. S exists as in Theorem 2 but K is not an U-field in L (the other implication of Theorem 2 is evident). Let R be a Galois extension of K in L such that $G(R|K)\in U$, $G(R_0|K)\in U$ for any proper subfield R_0 of R which is a Galois extension of K. Due to the maximum condition on S, $G=G(R|K)$ is not simple. If the intersection of all proper normal subgroups of G is trivial there exist proper normal subgroups H_1, H_2 of G such that $H_1\cap H_2=\{1\}$. Due to the fundamental theorem of Galois theory G/H_i are Galois groups of certain Galois extensions of K in R, so $G/H_i\in U$, $i=1, 2$ due to the condition on R, hence $G=G/H_1\cap H_2\in U$, being a subgroup of the direct product $G/H_1\times G/H_2$. Thus it follows that the intersection of all proper normal subgroups of G is a proper normal subgroup M. Due to the condition on S and FTGT (i. e the fundamental theorem of Galois theory) M is a subgroup of all maximal subgroups of G, hence $M\subset\Phi(G)$. As $G/\Phi(G)=(G/M)/(\Phi(M)/M)$, $|G||M|<|G|$, due to FTGT and the fact that U is saturated $G\in U$ — a contradiction proving Theorem 2.

Proof of Corollary 2. Corollary 2 (i) is a direct result of Theorem 2 and the Huppert (Burnside — Wielandt) theorem characterizing the finite supersolvable (nilpotent) groups mainly by properties of their maximal subgroups [14, Ch. 6, § 17, Th. 17.1.4; Ch. 7. § 20, Th. 20.3.1] as well as of FTGT. As for Corollary 2 (iii) it is a direct result of Corollary 2 (ii) as well as of the proof of Corollary 1.

Proof of Corollary 2 (ii). If K is cyclic in L, then $S:=\{\alpha: K(\alpha)$ is a minimal extension of K in L, if $\alpha\in S$, $\beta\in S$, $K(\alpha)=(\beta)$ iff $\alpha=\beta$, any extension of K in L equals $K(g)$ for some $g\in S\}$ satisfies the necessary conditions due to FTGT.

Let S satisfy the necessary conditions. So S is either finite or infinite denumerable. Let f_α be the minimal polynomial of α over K for any $\alpha\in S$, $\widetilde{S}$ be the set of all elements of S separable over K. If $\widetilde{S}=\emptyset$, then (ii) is proved. If $\widetilde{S}\neq\emptyset$, $\alpha\prec\beta$ iff $\deg f_\alpha<\deg f_\beta$. Clearly $\prec$ induces a linear order in $\widetilde{S}$, so $\alpha_1, \ldots, \alpha_n$ are the first n elements of $\widetilde{S}$ regarding $\prec$. Besides, $\widetilde{S}$ may be considered to have the property that for any proper subset S_1 of $\widetilde{S}$, K is not maximal in L without $S_1\cup S\setminus\widetilde{S}$. If α_1 is the minimal element of $\widetilde{S}$ then $K(\alpha_1)$ is normal over K. By induction one may assume that $K(\alpha_i)$ is normal over K, $i=1, \ldots, n$. If $\widetilde{S}=\{\alpha_1, \ldots, \alpha_n\}$ (ii) is proved. Let $S\neq\{\alpha_1, \ldots, \alpha_n\}$ and let α_{n+1} be the minimal element of $S\setminus\{\alpha_1, \ldots, \alpha_n\}$. If $K(\alpha_{n+1})$ is not normal over K, then $K(\beta)\neq K(\alpha_{n+1})$ for some root β of $f_{\alpha_{n+1}}$. As $K(\beta)$ is a separable extension of K in L clearly $\widetilde{S}\cap K(\beta)\neq\emptyset$, hence $K(\alpha_i)\subset K(\beta)$ for some $i\in\{1, \ldots, n\}$. As $K(\alpha_i)$ is normal over K, $\alpha_i\in K(\alpha_{n+1})$, i. e K is a maximal subfield in L without $S\setminus\{\alpha_{n+1}\}$ — a contradiction proving the assertion that $K(\alpha)$ is normal over K for any $\alpha\in\widetilde{S}$. Due to Corollary 2 (i) K is nilpotent in L, so any finite Galois extension M of K in L is a composite of Galois extensions of K in L of dimensions which are powers of prime numbers, i. e a composite of cyclic fields as any finite group with a single maximal subgroup is cyclic [6, p. 563] (in fact we make use of the Burnside — Wielandt theorem referred to that a finite group is nilpotent iff it is isomorphic to a direct product of its Sylow p-subgroups for all prime multiples p of its order; due to the condition on S if $P\in \mathrm{Syl}_p G$, $G:=G(M|K)$ then P is cyclic for any prime multiple p of $|G|$, since P is a quotient group of G, therefore a Galois group of some

finite Galois extension of K in M — we apply FTGT again). For that reason G is cyclic, hence any separable finite extension of K in L is cyclic due to FTGT and the fact that it is a subfield of some finite Galois extension of K in L. Corollary 2 is proved.

Proof of Corollary 3. Corollary 3 (ii) is a direct result of Corollary 2 (i) and the Sylow theorem on profinite groups [7, Ch. I, § 5, Pr. 5.2].

Proof of Corollary 3 (i). As U is a class of finite solvable groups any element of U is a Galois group of some Galois extension over the field of rationals Q due to the Shaffarevich theorem [16] that any finite solvable group may be realized as a Galois group of some finite Galois extension of Q. Let $\tilde{L}$ be the minimal subfield of L containing all finite Galois extensions of Q with a Galois group belonging to U. As U is saturated Q is an U-field in $\tilde{L}$ (Theorem 2). Due to Zorn's lemma there exists a maximal subfield L_0 of L without: $S=\tilde{L}\setminus Q$. As L_0 is a maximal subfield of L without a set of algebraic elements over L_0, L is algebraic over L_0. Due to Theorem 2 L_0 is an U-field such that any element of U may be realized as a Galois group of an appropriate Galois extension of L_0. Let K be a finite extension of L_0 in L. As U is closed with respect to taking subgroups and quotient groups K is an U-field being algebraic over L_0 due to FTGT. If $G\in U$ is not a Galois group of any finite extension (Galois) of K, then $M\cap K\neq L_0$ for any finite Galois extension M of L_0 such that $M\subset L$, $G(M\mid L_0)=G$. As U is regular $\tilde{G}=G_1\times\cdots\times G_n\in U$ for any $n\in N$, $G_i\in U$, $i=1,\ldots,n$. Assuming n big enough $\tilde{G}=G$, $\tilde{G}=\tilde{G}_1\times\cdots\times\tilde{G}_n$ and applying FTGT to a finite Galois extension $\tilde{M}$ of L_0 such that $G(\tilde{M}\mid L_0)=\tilde{G}$ it follows that $[K: L_0]=\infty$ — a contradiction proving Corollary 3.

Proofs of the example. (i) In terms of this item as the residue field $\tilde{K}$ of K is perfect any finite extension L of K contains a maximal non-ramified extension T of K, such that every non-ramified extension of K in L is a subfield of T, besides $[T: K]=[\tilde{L}: \tilde{K}]$ (see [10, Ch. IV, § 1, Ex. 12]). So if L is a finite Galois extension of K, T is a Galois extension of K. Let R be the valuation ring of T with respect to the valuation of L induced by the valuation of K (as for some general facts on valuation theory see [15, Ch. XII]) Let $\mathfrak{M}$ be the maximal ideal of R. For every $\varphi\in G:=G(T\mid K)$, $\varphi(R)\subset R$. $\varphi(\mathfrak{M})\subset\mathfrak{M}$. Assume $\tilde{\varphi}(a+\mathfrak{M}):=\varphi(a)+\mathfrak{M}$, $a\in R$. Clearly $\tilde{\varphi}$ is a well defined, $\tilde{K}$-automorphism of $\tilde{L}$, i. e $\tilde{\varphi}\in\tilde{G}:=G(\tilde{L}/\tilde{K})$. The mapping $\varphi\to\tilde{\varphi}$ is an isomorphism of G on $\tilde{G}$, hence G is solvable. On the other hand, $[L: T]$ equals the ramification index of the extension $L\mid T$, hence $G(L\mid T)$ is solvable [13, Ch. 1, Th. 4]. As the class of solvable groups is well-known to be closed with respect to group extensions, (i. e if $H\lhd G$, H and G/H are solvable, so is G) $G(L\mid K)$ is solvable. Example (i) is correct.

(ii) Any finite extension of $K((x_1))$, $\mathrm{ch}\,K=0$, is a subfield of $K_2((u))$, $u^e=x_1$, e being the ramification index of the extension over $K((X_1))$, K_2 being a finite extension of K (if $\mathrm{ch}\,K=q>0$ the same result holds for any finite extension of $K((x_1))$ of dimension prime-to-q) — see [10, Ch. IV, § 1, Th. 6]. As a primitive e-th root of unity exists in K (if $\mathrm{ch}\,K=0$ or $(e, \mathrm{ch}\,K)=1$) $K((u))$ is a cyclic extension of $K((x_1))$, while $K_2((x_1))=K_2\cdot K((x_1))$, hence $G(K_2((x_1))\mid K((x_1)))$ is abelian as $G(K_2\mid K)$ is abelian. As $K((x_1))=K((u))\cap K_2((x_1))$, $G(K_2((u))\mid K((x_1)))=G(K_2((x_1))\mid K((x_1)))\times G(K((u))\mid K((x_1)))$ (see [11, Ch. V, p 217, Ex. 3]). So if $\mathrm{ch}\,K=0$, $K((x_1))$ is abelian. If $\mathrm{ch}\,K=q>0$ any finite extension of

$K((x_1))$ of dimension prime-to-q is an abelian Galois extension. As K is perfect $K((x_1))$ is solvable. Clearly K_1 is a composite of the minimal perfect subfield K_3 of the algebraic closure $\bar{M}$ of $M: =K((x_1))$ containing M and M_1, M_1 being the invariant subfield of the maximal separable extension M_s of M regarding the action of a Hall $\bar{q}$-subgroup of $G(M_s|M)$, $\bar{q}$ being the set of all prime numbers but q (see Remark 1), i. e $K_1=K_3.M_1$. So K_1 is an abelian perfect field. As for the case $\mathrm{ch}\,K=0$, $K((x_1,\ldots,x_m))$, $m\in N$, is trivially proved to be abelian by induction. Example (ii) is correct.

(iii) Due to [2, Lemma 2] it suffices to prove that if $M=K((x_1))$, p is prime, $p\neq\mathrm{ch}\,K$, $R_p=M(\xi,\eta)$, $\xi^p\eta=\varepsilon\eta\xi$, $\xi^p=a$, $a\in K\setminus K^p$, $\eta^p=x_1$, $K^p:=\{s\in K,$ $s_1^p=s$ for some $s_1\in K\}$, ε is a fixed primitive p-th root of unity (clearly $K\neq K^p$ due to the conditions on K and Galois theory on cyclic extensions [15, Ch. VIII, § 6]), then R_p is a division algebra. As R_p is a central simple artinian M-algebra if R_p is not a division algebra, then it is M-isomorphic to a full matrix algebra M_p of order p due to Wedderburn — Artin's theorem. Skolem — Noether's theorem [12, Th. IV. 4.1] and the well-known fact that any extension of M of dimension p is M-isomorphic to subfield of M_p prove that $M(\xi_1,\eta_1)\cong M_p$, $\xi_1^p=\eta_1^p=a$, $\xi_1\eta_1=\varepsilon\eta_1\xi_1$. The norm condition [12, Ch. V, Ex. 24] indicates that $R_p\cong M_p$ (over M) iff $N_M(\sum_{i=0}^{p-1}\alpha_i\xi_1^i)a=x_1$ for some $(\alpha_0,\ldots,\alpha_{p-1})\in M^p$ (iff $N_M(\sum_{i=0}^{p-1}\beta_i\xi_1^i)a=x_1^{pn+1}$ for some $n\geqq 0$, $\beta_i=\sum_{j=0}^{\infty}\beta_{ij}x_1^j$, $i=0,\ldots,p-1$, $\beta_{k0}=0$ for some $k\in\{0,\ldots,p-1\}$ — hence $N_K(\sum_{i=0}^{p-1}\beta_{i0}\xi_0^i)=0$ — contradiction to the fact that $a\in K\setminus K^p$). So R_p is a central division M-algebra $[R_p: M]=p^2$. The question in (2) referred to is solved positively.

Proof of Theorem 3. (i) is a partial case of Corollary 2. (ii) Any proper extension of K in L contains a subextension L_1 of dimension $p=\mathrm{ch}\,K$ over K. So $L_1=K(\beta)$, $\beta=\sum_{i,j,k=0}c_{ijk}z^{pk}z^i\sqrt[p]{(x+yz^p)^j}$. As $\beta^p\in K$ it is a rational function of x, y, z^{p^2}; c_{ijk}^p are rational functions of x^p, y^p, z^{p^2}. As x, y, z are algebraically independent over $GF(p)$ the condition $\beta^p\in K$ is equivalent to a system of equations. It is easily solved to prove that $\beta=\sum_{k=0}^{p-1}c_{00k}z^{pk}+c_{000}$, hence $z^p\in L_1$ (see [15, Ch. VIII, § 9, Cor. 1). Evidently $K(z)\neq K(\sqrt[p]{x+yz^p})$, L is normal over K, being purely inseparable over K. Theorem 3 (ii) is proved.

The proof of Theorem 3 is realized by several steps.

Proposition 1. *Let $p_1<\cdots<p_k$, $k\in N$, be prime numbers. Then if $n\in N$, $[Q(\sqrt[n]{p_1},\ldots,\sqrt[n]{p_k}): Q]=n^k$* (this result is proved by A. Besicovitch in 1940).

Proposition 2. *Let $f(x)\in Z[x]$, Z be the ring of integer rational numbers and let f be irreducible over the field of rationals Q. Then the set of prime numbers q such that for some $k=k_q\in Z$, $f(k)\equiv 0(\mathrm{mod}\,q)$, $f(k)\not\equiv 0(\mathrm{mod}\,q^2)$ is infinite.*

Proof. As f is irreducible over Q, for some $u, v\in Z[x]$, $hu+\frac{df}{dx}\cdot v=l\in Z$. It is known that $f(k_q)\equiv 0(\mathrm{mod}\,q)$ for an infinite set of primes q and certain $k_q\in Z$. For any prime q big enough $(q, l)=1$. For any such q if $f(k_q)\equiv 0(\mathrm{mod}\,q)$

then $f(k_q+q)\equiv 0(\mathrm{mod}\, q)$, however it is impossible to have $f(k_q)\equiv f(k_q+q)\equiv 0 (\mathrm{mod}\, q^2)$. Proposition 2 is proved.

Lemma 1. *Let K be as in Theorem 3* (iii), *P be an extension of K $[P: K]=2^k$, $k\in N\cup\{0\}$. Then there exist elements p_1, p_2 of P such that:*

(i) $P=K(p_1)=K(p_2)=K(p_1p_2)$, $N(p_i)\overline{\in} Q^2$, $i=1, 2, 3$, *N being the standard norm in P over Q, $p_3: p_1p_2$.*

(ii) *All the roots p_{si}, $i=1, \ldots, 2^k$, in $\overline{Q}$* of the minimal polynomial of $p_s=p_{s1}$, $s=1, 2$, *over K satisfy the condition* $(\widetilde{p}: =K(p_{11}, \ldots p_{12^k}))\widetilde{p}^2 \cap \{p_{1i}, p_{2i}, p_{1i}p_{2j}, p_{1i}p_{1j}p_{2j}, p_{1i}p_{2i}p_{2j}, i=1, \ldots, 2^k, j=1, \ldots, 2^k\}=\varnothing$ *(if F is a field* $F^p: =\{s\in F, s_1^p=s$ *for some* $s_1\in F\}$).

Proof. As $[P: Q]<\infty P$ is a simple extension of Q. Due to Proposition 1 and 2, it is easy to find elements r_1, r_2 (integer over Z) satisfying (i). As $[\widetilde{P}: Q]$ is finite there exists a natural number $M=M(\widetilde{P})$ such that if $m\in N$, $M<q_1<\cdots <q_m$, $q_1, \ldots, q_m$ — prime, then $q_{i_1}\ldots q_{i_s}\overline{\in}\widetilde{P}^2$ for $s\in\{1, \ldots, m\}$ $i_1<\cdots<i_s$ (Proposition 1). Hence if q_1, q_2 are big enough prime numbers such that $q_1\neq q_2$, then $p_1=q_1r_1$, $p_2=q_2r_2$ will satisfy the conditions (i), (ii) of Lemma 1. Lemma 1 is proved.

Lemma 2. *Let K, P, p_1, p_2 satisfy the conditions of Lemma 1. Let $R_s=K(\theta_s)$, $\theta_3=\theta_1\theta_2$, $\theta_s\overline{\in}\overline{Q}$, $\theta_s^2=p_s$, $s=1, 2$. Let $R=P(\theta_1, \theta_2)$. Then the subfields of R containing K are exactly R_1, R_2, R_3, R and the subfields of P containing K.*

Proof. Let $\alpha_s\in R_s\setminus P$, i. e $\alpha_s=a+b\theta_s$, $a\in P$, $b\in P\setminus\{0\}$, $s=1, 2, 3$. Any K-monomorphism of R in $\overline{Q}$ extends some K-monomorphism of P in $\widetilde{P}$. If $K(\alpha_s)$ is a proper subfield of R_s, then for some different indices $i, j\in\{1, \ldots, 2^k\}$ $a_i+b_i\theta_{si}=a_j+b_j\theta_{sj}$ $(\theta_{sj}^2=p_{sj})$, a_r, b_r being the images of a, b under the action of that K-monomorphism of P in $\widetilde{P}$ that transforms p_s into p_{sr}, $r=1, \ldots, 2^k$. As $(x-a_r-b_r\theta_{sr})(x-a_r+b_r\theta_{sr})\in\widetilde{P}[x]$ for all $r=1, \ldots, 2^k$ it follows that (Lemma 1, (ii)) $a_i-b_i\theta_{si}=a_j-b_j\theta_{sj}$, hence $b_i\theta_{si}=b_j\theta_{sj}$, i. e $R_s\neq K(b\theta_s)$. However $\theta_s\overline{\in}P$, $N(p_sb^2)\overline{\in}Q^2$ (the norm in P over Q), so having $[P: K]=2^k$ it follows that $P=K(b^2p_s)$, $R_s=K(b\theta_s)$. This contradiction proves the assertion that the subfields of R_s, $s=1, 2, 3$, are exactly R_s and the subfields of P (here subfields mean subfields containing K). Let $\alpha=a_0+\sum\limits_{s=1}^{3}a_s\theta_s\in R$, $a_0\in P$, $a_s\in P$, $s=1, 2, 3$.

To prove Lemma 2 it suffices to prove that if $\alpha\in R\setminus(R_1\cup R_2\cup R_3)$ then $K(\alpha)=R$. As $\{1, \theta_1, \theta_2, \theta_3=\theta_1\theta_2\}$ is a P-basis of R (Proposition 3) $\alpha\overline{\in}R_1\cup R_2\cup R_3$ iff $a_ia_j\neq 0$ for some different indices, $i, j\in\{1, 2, 3\}$. Assume $K(\alpha)\subsetneq R$. Then for some $j\neq i$, j, $i\in\{1, \ldots, 2^k\}$ (as $\alpha\overline{\in}R_1\cup R_2\cup R_3$), $\theta=a_{0i}+\sum\limits_{s=1}^{3}a_{si}\theta_{si}=a_{0j}+\sum\limits_{s=1}^{3}a_{sj}\delta_{sj}$, $\delta_{3j}: =\delta_{1j}\delta_{2j}$ for some $(\delta_{1j}, \delta_{2j})$ belonging to $\{(\theta_{1j}, \theta_{2j}), (-\theta_{1j}, \theta_{2j})$ $(\theta_{1j}, -\theta_{2j}), (-\theta_{1j}, -\theta_{2j})\}$, a_{sr}, $s=1, 2, 3, 0$ being the images of a_s under the action of the corresponding K-monomorphism of P in $\widetilde{P}\subset\overline{Q}$, $r=1, \ldots, 2^k$, $\theta_{sr}^2=p_{sr}$.

Let $f_r(x)=N_{\widetilde{P}(x)}(x-a_{0r}-\sum\limits_{s=1}^{3}a_{sr}\theta_{sr})\in\widetilde{P}[x]$ (the norm in $\widetilde{P}(x, \theta_{1r}, \theta_{2r})$ over, $\widetilde{P}(x)$), $r=1, \ldots, 2^k$. As f_r has no root in $\widetilde{P}$ (Proposition 3) for any r it follows that f_i and f_j have at least two different common roots.

The proof of Lemma 2 is reduced to case by case discussion. Due to Lemma 1 (ii) it suffices to assume $\widetilde{\theta}=a_{0i}-(\sum_{s=1}^{2} a_{si}\theta_{si})+a_{3i}\theta_{3i}$, θ and $\widetilde{\theta}$ to be the common roots of f_i, f_j and to consider the following cases:

1. $\widetilde{\theta}=a_{0j}-a_{1j}\delta_{1j}+a_{2j}\delta_{2j}-a_{3j}\delta_{3j}$;
2. $\widetilde{\theta}=a_{0j}+a_{1j}\delta_{1j}-a_{2j}\delta_{2j}-a_{3j}\delta_{3j}$;
3. $\widetilde{\theta}=a_{0j}-a_{1j}\delta_{1j}-a_{2j}\delta_{2j}+a_{3j}\delta_{3j}$.

Case 1. As $\theta+\widetilde{\theta}=2(a_{0i}+a_{3i}\theta_{3i})=2(a_{0j}+a_{2j}+a_{2j}\delta_{2j})$ using Lemma 1 and, the fact that $(x-a_{0i}-a_{3i}\theta_{3i})\,(x-a_{0i}+a_{3i}\theta_{3i})\in\widetilde{P}[x]$, $(x-a_{0j}-a_{2j}\delta_{2j})(x-a_{0j}+a_{2j}\,.\,\delta_{2j})\in\widetilde{P}[x]$, we have $a_{0i}-a_{3i}\theta_{3i}=a_{0j}-a_{2j}\delta_{2j}$, hence $a_2=a_3=0$. As $i\neq j$ $a_1=0$, too, so $\alpha\in P$.

Case 2 is considered in the same way as case 1 to prove $\alpha\in P$.

Case 3. As $\theta+\widetilde{\theta}=2(a_{0i}+a_{3i}\theta_{3i})=2(a_{0j}+a_{3j}\delta_{3j})$, $i\neq j$, we have proved that $a_3=0$. Considering $(\theta-\widetilde{\theta})^2$ it follows that $a_1a_2=0$, i. e $\alpha\in R_1\cup R_2$.

The contradiction proves in all cases that if $\alpha\in R_1\cup R_2\cup R_3$ then $K(\alpha)=R$. Lemma 2 is proved.

Propositions 1, 2, 3 and Lemmas 1, 2 make clear that if P, K are as in Lemma 1, then there exist at least two K-unisomorphic extensions of P satisfying the conditions imposed on R in Lemma 2. So let $F_0=K$, F_n be an extension of F_{n-1} in $\bar{Q}$ for every $n\in N$ and let F_{ns}, be as R_s, $s=1, 2, 3$, regarding F_n as R, F_{n-1} as P in Lemma 2. Then $F\colon \cup_{n=0}^{\infty}F_n$, K, F_n, F_{ns}, $s=1, 2, 3$, $n\in N$, are all subfields of F containing K. If $G\colon =\cup_{n=0}^{\infty}G_n$ is constructed like F, and for some $m\in N$ F_m and G_m are not K-isomorphic then F and G are not K-isomorphic as $F_m(G_m)$ is the only extension of K in $F(G)$ of dimension 4^m. As $\bar{Q}$ is infinite denumerable and there exists a mapping of the set all series $\{\alpha_i\}_0^{\infty}$, $\alpha_i\in\{0, 1\}$, $i\in N$, in the set of all subfields of $\bar{Q}$ containing K such that the images of any two different series are K-unisomorphic fields, the existence of M_1 as in Theorem 3 (iii) is proved. As for M_2 it suffices to consider $\widetilde{F}_0=K$, $\widetilde{F}_n$ being over $\widetilde{F}_{n-1}$ like R_1 over P in Lemma 2 for every $n\in N$, to notice that the only subfields of $\widetilde{F}\colon =\cup_{n=0}^{\infty}\widetilde{F}_n$ containing K are K, $\widetilde{F}$, $\widetilde{F}_n$, $n\in N$, and to apply the method of proving the existence of M_1. Theorem 3 (iii) is proved.

Proof of Corollary 4. It suffices to notice that if K is an ordered field, for any $n\in N$, $\widetilde{F}_n\supset\widetilde{F}_{n-1}$ can be constructed such that for some $\theta_n\in\widetilde{F}_n$: $K(\theta_n)=\widetilde{F}_n$ there exists a root $\widetilde{\theta}_n\neq\theta_n$ of the minimal polynomial of θ_n over $\widetilde{F}_{n-1}$ belonging to $\widetilde{F}_n$, $\theta_n\,\widetilde{\theta}_n<0$ regarding some order of $\widetilde{F}_n$ extending the fixed order of $\widetilde{F}_{n-1}$, F_n being as in the proof of Theorem 3. All this is possible moreover $\widetilde{F}_n$ is not unique over a fixed field $\widetilde{F}_{n-1}$ up to a K-isomorphism — see the proof of Theorem 3 (iii). Corollary 4 is proved.

Proof of Corollary 5. If $M\supset K$ is an U-field in L, L — a Galois extension of K, then the set of subfields of M containing K satisfies the Zorn lemma conditions with respect to $\prec$($A\prec B$ iff $A\supset B$), as any irreducible polynomial over $S\colon =\bigcap_{\alpha\in I}S_\alpha$, $S_\beta\supset S_g$, β, $g\in I$, $\beta<g$, S_α — subfield of L for all $\alpha\in I$, is irreducible over $S_{\tilde{\alpha}}$ for some $\tilde{\alpha}\in I$. If M is subfield of L containing K then M is q-maximal in L iff it is cyclic in L, Corollary 5 is proved due to Zorn's emma.

Remark. Clearly $\operatorname{imp} L \leqq \operatorname{imp} K (\operatorname{imp} L = \operatorname{imp} K)$ if L is an algebraic (a finite) extension of a field K. Also if $K \subset L$, L — algebraic over K, K being an U-field then L is an U-field when U is closed with respect to taking subgroups and quotient groups. Another way of constructing U-fields is based on the fact that if P is an extension of a field K, P is an U-field, then the maximal algebraic extension of K in P is an U-field. Thus example (ii) makes clear that for any cardinal $\alpha \geqq 1$ there exists an abelian field K, $\deg_F K = \alpha$, F — the simple subfield of K, such that K is not cyclic (if $\alpha = 0$ this is impossible due to a result of Geyer [7, Ch. V, § 9, Th. 9.1]).

Remark. It has become clear that while a proper q-maximal subfield of a field L is maximal in L without a single element, the reverse is not generally true. A q-maximal problem can be formulated for other algebraic systems as well. We shall notice that in terms of modules over a commutative integral domain R, any ideal of R being principal, any maximal submodule of an R-module M without one element is q-maximal in M, while the reverse is true iff M_0 is q-maximal in M such that M/M_0 is an Artinian R-module, i. e the reverse is not generally true.

Proposition 3. *Let K be a field, $p \neq \operatorname{ch} K$, p — prime, $k \in N$, $p_1, \ldots p_k$ be such that if $(i_1, \ldots, i_k, p) = 1$ then $p_1^{i_1} \ldots p_k^{i_k} \in K/K^p$. Let ξ_j belong to some extension of K, $\xi_j^p = p_j$, $j = 1, \ldots, k$. Then $[K(\xi_1, \ldots, \xi_k) : K] = p^k$.*

Proof. It is clearly reduced to the case when a primitive p-th root o unity exists in K as $[K(\xi_1^{i_1} \ldots \xi_k^{i_k}) : K] = p$ if $(i_1, \ldots, i_k, p) = 1$ due to [15, Ch VIII, § 9, Th. 16], so if $k = 1$ Proposition 3 is true. As [2, Prop. 5] proves that $\xi_2, p_2, \ldots, \xi_k, p_k$ satisfy the conditions of Proposition 3 over $K(\xi_1)$ the proof of Proposition 3 is accomplished by induction.

Remark 1. Let U be a regular class of finite groups. If a topological group is isomorphic to a projective limit of elements of U, then it is said to be a pro-U-group. If L is a Galois extension of K, K is an U-field in L iff $G(L \mid K)$ is a pro-U-group due to the Krull Galois theory. Besides for any purely inseparable extension K_0 of K in $\bar{L}$, the composite $L \cdot K_0$ is a Galois extension of K_0 so that $G(L \mid K)$ and $G(L \cdot K_0 \mid K_0)$ are isomorphic profinite groups. The main facts on profinite groups may be found in [7], the definition of a Hall-Π-subgroup is analogous to the definition of a Sylow p-subgroup. Moreover using the Hall theory on finite solvable groups [14, Ch. 7, § 20, Th. 20.1.1] one can easily reformulate the Hall theorem to cover the class of prosolvable groups (and characterize this class in the class of all profinite groups). The proof of the Hall theorem in the case of prosolvable groups can be realized just repeating with appropriate changes the proof of the Sylow theorem on profinite groups. Remark 1 has been used to prove that example (ii) is correct.

Acknowledgements. Special thanks of the author are due to P. N. Siderov for his encouragement and support.

REFERENCES

1. I. D. Chipchakov. On algebraic associative division algebras over fields characterized by means of maximum conditions. *C. R. Acad. Bulg. Sci*, **37**, 1984, 1147—1149.
2. I. D. Chipchakov. On the structure of algebraic associative division algebras over solvable and nilpotent fields. *Pliska*, **6**, 1986, 173—181.

3. K. W. Gruenberg. Projective profinite groups. *J. London Math. Soc.*, **42**, 1967, No 1, 155—165.
4. P. J. McCarthy. Maximal fields disjoint from certain sets. *Proc. Amer. Math. Soc.*, **18**, 1967, 347—351.
5. M. J. Norris, W. Y. Velez. A characterization of the splitting of inseparable algebraic extensions. *Amer. Math. Mon.*, **85**, 1979, No 1, 338—341.
6. F. Quigley. Maximal subfields of an algebraically closed field not containing a given element. *Proc. Amer. Math. Soc.*, **13**, 1962, 562—566.
7. L. Ribes. Introduction to profinite groups and Galois cohomology. *Kingston, Qeen's Univ.*, 1970.
8. J. -P. Serre. Corps. locaux. Hermann. Paris, 1968.
9. W. C. Waterhouse. Profinite groups are Galois groups. *Proc. Amer. Math. Soc.*, **42**, 1974, No 2, 639—640.
10. З. И. Боревич, И. Р. Шафаревич. Теория чисел. Москва, 1972.
11. Н. Бурбаки. Алгебра. Многочлены и поля. Упорядоченные группы. Москва, 1965.
12. Ю. А. Дрозд, В. В. Кириченко. Конечномерные алгебры. Киев, 1980.
13. К. Ивасава. Локальная теория полей классов. Москва, 1983.
14. М. И. Каргаполов, Ю. И. Мерзляков. Основы теории групп. Москва, 1982.
15. С. Ленг. Алгебра. Москва, 1968.
16. И. Р. Шафаревич. Построение полей алгебраических чисел с заданной разрешимой группой Галуа. *Изв. АН СССР*, **18**, 1954, 525—578.

Centre for Mathematics and Mechanics
1090 Sofia P. O. Box 373

Received 29. 4. 1984