PLISKA
STUDIA MATHEMATICA BULGARICA

ПЛИСКА
БЪЛГАРСКИ МАТЕМАТИЧЕСКИ СТУДИИ

ON THE STRUCTURE OF ALGEBRAIC ASSOCIATIVE DIVISION ALGEBRAS OVER SOLVABLE AND NILPOTENT FIELDS

IVAN D. CHIPCHAKOV

In this paper the structure of associative algebras — *LBD* over solvable fields and algebraic over nilpotent fields is considered with special attention to the link between properties algebraic — commutative and algebraic — finite dimensional, as well as to some existence questions.

Definition 1. *A field P_0 is said to be Π-solvable (Π-nilpotent, Π-cyclic etc.) iff the Galois group G of any finite Galois extension of P_0 is a solvable (nilpotent, cyclic etc.) Π-group, i. e. either $G=\{1\}$* or $|G|=p_1^{k_1}\dots p_s^{k_s}$, $p_i \in \Pi$, Π *being any fixed set of prime numbers.*

Characterizations of solvable, nilpotent and cyclic fields are announced in [12, Th. 3]. They will be proved in another paper.

In this paper a complete proof of the results announced in [12] — from Theorem 6 on to the end of [12] — is presented. Some of the results in [12] referred to are generalized, unannounced results are presented in this paper as well.

Algebras in this paper will always mean associative algebras. The definitions supposed to be known may be found in [7].

Definition 2. *A central P_0-algebra is said to be cyclic iff it is a crossed product of a maximal subfield with a cyclic group.*

Definition 3. *A P_0-algebra R is said to be special iff its centre C is a finite extension of P_0, $[R:C]:=\dim_C R=p^2$, p — prime, R is a cyclic C-algebra and the polynomial $x^p-1 \in C[x]$ is a product of linear multiples over C.*

Definition 4. *An algebraic algebra R over a field P_0 is said to be an LBD-algebra over P_0 iff for any finite subset S of R there exists a number n_S such that the degree of the minimal polynomial over P_0 of any element of the linear P_0-subspace of R generated by S is less than n_S.*

In [3, p. 249 Th. 3] it is proved that every algebraic algebra over a nondenumerable field is an LBD-algebra.

Definition 5. *A division algebra R is said to be an automorphic extension of its subalgebra R_0 iff the following conditions are satisfied: The centre of R_0 is a proper extension of the centre of R of finite dimension; there exists a chain of subfields L_i, $i=0, 1, \dots, k$, $k \in N \subsetneqq L_j$, $i>j$, L_0 and L_k being respectively the centres of R_0 and R; for any $i=0, \dots, k-1$ there exists an automorhism α_i of the centralizer R_i of L_i acting as an identity on all elements of L_{i+1} but not on all elements of L_i, however $\alpha_i^{p_i}$ is an inner automorphism of R_i for some prime number p_i besides $R_{i+1}=\sum_{k=0}^{p_i-1} R_i d_i^n$ for an element d_i of R such that $d_i^{-1} r_i d_i=\alpha_i(r_i)$ for any element r_i of R_i.*

PLISKA Studia mathematica bulgarica. Vol. 8, 1986, p. 173—181.

Definition 6. *An algebraic extension K_p of a field K — p being prime — is said to be a $\{p\}$-closure of K iff K_p is a $\{p\}$-nilpotent field which is minimal with respect to that property.*

We list the main results in this paper.

Theorem 1. *Let R be a central division LBD-algebra over a solvable field P_0. Then either $R=R_0$ or there exists a finite separable extension L of P_0 such that $L\otimes_{P_0}R:=R_L$ is a division LBD-algebra containing a special P_0-subalgebra.*

Theorem 2. *Let R be an algebraic noncommutative central division algebra over a nilpotent field P_0. Then either R is of finite dimension over P_0 or there exists a locally finite subalgebra R_1 of R whose centre P_1 is an extension of P_0 and regarded as a P_1-algebra R_1 is isomorphic to a tensor product over P_1 of an infinite set of central special P_1-subalgebras of R_1.*

Theorems 1 and 2 improve the results presented in [12, Th. 6 and the following corollary to it].

The structure of an arbitrary division algebra of finite dimension over its centre P_0, P_0 being nilpotent is considered in the following unannounced previously result.

Theorem 3. *Let R be a central division algebra over a nilpotent field P_0. Then either $R=P_0$ or R is an automorphic extension of any of its maximal subfields which are separable over P_0. For any prime number p dividing $\dim_{P_0}R$ and $p\neq\mathrm{char}\,P_0$ a primitive p-th root of unity exists in P_0 (in this theorem R is assumed to be of finite dimension over P_0).*

The following result generalizes [12. Th. 7] and proves the existence of noncommutative division algebras of finite dimension over certain $\{p\}$-nilpotent fields.

Theorem 4. *Let $\{R_\alpha\}$, $\alpha\in I$, be a set of two-by-two unisomorphic central division algebras over a field P_0 of dimension p^{k_α}, p being a fixed prime number. Then $R_\alpha\otimes_{P_0}P_{0p}$ are two-by-two unisomorphic central division P_{0p}-algebras of dimension p^{K_α} over the $\{p\}$-closure P_{0p} of P_0.*

Corollaries to the main results.

Corollary 1. *Let P_0 be a cyclic field. Then either any algebraic division P_0-algebra is a field or P_0 is a real closed field the unisomorphic algebraic division P_0-algebras being P_0, $P_0(i):i^2=-1$ and the quaternion algebra over P_0.*

Corollary 2. *Let P_0 be a maximal subfield of an algebraically closed field without a set S, S consisting of one or two elements, i. e. P_0 is a maximal subfield of its algebraically closed extension P with respect to disjointness from the fixed subset S of P. Then either any algebraic division P_0-algebra is a field or P_0 is a real closed field.*

Corollary 3. *Let P_0 be a field satisfying the following finite condition: for any algebraic extension L of P_0 and any fixed prime number p, no infinite tensor product over L of central cyclic division L-algebras each of dimension p^2 over L is a division algebra. Then any algebraic division algebra central over an algebraic extension P_1 of P_0, P_1 being a Π-nilpotent field with respect to any fixed finite set of primes Π, proves to be of finite dimension over P_1.*

Any local field as well as any field of algebraic numbers satisfies the finite condition just referred to because a tensor product of two central division algebras of equal dimension over such a field is not a division algebra.

Corollary 5. *For any fixed prime number p the $\{p\}$-closure K_p of a field K, K being the field of rationals or its purely transcendental extension, has the property that there exists an infinite set of two-by-two unisomorphic special cental division K_p-algebras.*

Corollary 6. *There exists a $\{2\}$-nilpotent field not satisfying the finite condition.*

Corollary 7. *If K is a field such that $B(K)\neq\{0\}$, $B(K)$ being the Brauer group of K, then there exists a special division K-algebra.*

Proofs of the main results. Proof of Theorem 1.

Proposition 1. *Let L be an extension of a field K of prime dimension p and let R be a central division K-algebra. Then R_L is a division algebra iff L is not K-isomorphic to any subfield of R.*

Proof. Assume R_L is not a division algebra. Then R_L is a full matrix ring of order $p\times p$ over a division L-algebra [6, Ch. VIII, § 10, Ex. 13]. Due to the one-one lattice correspondence between the lattice of right ideals in R_L and the lattice of right ideals in $R\otimes_K K[x]$ containing the principal ideal generated by the minimal polynomial f over K of a certain fixed primitive element of L over K, it follows that a linear polynomial over R is a multiple in $R\otimes_K K[x]$ of the polynomial f, hence L is K-isomorphic to a subfield of R. Proposition 1 is proved.

The following proposition is a part of [6, Ch. VIII, § 10, Ex. 13].

Proposition 2. *Let R be a division algebra of finite dimension over its centre K. Let L be a finite extension of K such that $[L:K]$ and $[R:K]$ are relatively prime. Then R_L is a division algebra.*

In the situation of Theorem 1 it is enough to assume that R is noncommutative. Due to [11, Th. 3.2.1] there exists a non-central element ξ of P_0 separable over P_0. The first step to be taken is to prove the existence of a finite separable extension L_1 of P_0, such that R_{L_1} contains a subfield which is a cyclic extension of L_1 of prime dimension. If the Galois group over P_0 of the minimal polynomial f of ξ over P_0 is simple cyclic there is nothing to prove. If not, applying the fundamental theorem of Galois theory to the minimal Galois extension M of P_0 containing ξ, it follows — as the Galois group G of M over P_0 is solvable — that a subfield M_1 of M exists which is cyclic over P_0 of prime dimension. If R_{M_1} is not a division algebra then R proves to contain a cyclic extension of P_0 of prime dimension, otherwise, regarding ξ as an element of R_{M_1}, it follows that the Galois group of the minimal polynomial of ξ over M_1 is of smaller order than the order of G and since $\xi\notin M_1$ the proof of the first step is accomplished via induction and using [9, Ch. VII, Th. 9] and the fact [3, p. 249] that R_{M_1} is LBD over M_1.

A second step to the proof of Theorem 1 is to prove the existence of a finite separable extension L of L_1 (hence of P_0), such that either R_L contains a cyclic extension of L of dimension char P_0 or R_L contains a cyclic extension of L of prime dimension $p\neq\text{char}\,P_0$ and that a primitive p-th root of unity exists in L.

Let M_2 be a subfield of R_{L_1} which is a cyclic extension of L_1 of prime dimension q. One may assume $q\neq\text{char}\,P_0$, $q>2$, and there is no primitive q-th root of unity in L_1. If $R_{L_1(\varepsilon_q)}$ (ε_q being a primitive q-th of unity in the algebraic closure of L_1) is a division algebra, then the second step is proved. Otherwise, due to considerations analogous to those taken in the course of proving the first step, it follows that a subfield L_2 of $L_1(\varepsilon_q)$ has the property that

$R_{L_2} \supset R_{L_1}$ is a division algebra containing a subfield which is cyclic over L_2 of prime dimension $q_1 < q$, which is sufficient for proving the second step.

The proof of both steps makes clear that for an appropriate finite separable extension L of P_0, R_L is a division LBD-algebra satisfying the second step condition. Let $L(\xi_1)$ be a subfield of R_L, satisfying the respective condition. Due to [11, Th. 4.3.1] an element η of R_L^* exists, such that $\eta\xi_1 = \xi_2\eta$, $\xi_1 \neq \xi_2$, ξ_2 being a root of the minimal polynomial of ξ_1 over L in $L(\xi_1)$. So $L(\xi_1, \eta)$ is a special P_0-subalgebra of R_L. Theorem 1 is proved.

Theorem 1 remains true if R is a central LBD-algebra over an arbitrary field P_0 and a non-central element ξ of R exists such that the Galois group of the minimal polynomial of ξ over P_0 is solvable.

Proof of Theorem 2. Lemma 1. *Let L be a maximal subfield of a central division K-algebra R and let L be of finite dimension n over K. Then there exists a maximal subfield L_1 of R which is a separable extension of K of dimension n. If K is nilpotent, then R is of finite dimension over K.*

Proof. Assume L is not separable over K. Then $p = \operatorname{char} K \neq 0$, p/n. Let $p = n$, i. e. $L = K(\eta)$, $\eta^p \in K$. There exists an element θ of R such that $\theta\eta \neq \eta\theta$. The K-linear closure $l(S)$, $S := \{\eta^{-i}\theta\eta^i, i = 0, 1, \dots, p-1\}$ is a φ-invariant K-linear subspace of R ($\varphi r := \eta^{-1} r \eta$, for any $r \in R$). As $\varphi^p = id$ but $\varphi \neq id$ on $l(S)$, elements $a, b \in \overline{l(S)}$ exist such that $\varphi a = a$, $\varphi b = b + \alpha a$ for some $\alpha \in K^*$. So $K(\alpha^{-1} b a^{-1}, \eta)$ proves to be a special K-subalgebra of R and due to [11, Th. 4.4.2] it follows that $R = K(\alpha^{-1} b a^{-1}, \eta)$ since L is a maximal subfield of R. Case $p = n$ is proved ($\overline{l(S)} := l(S) \setminus \{0\}$).

Case $p < n$. As L is assumed not to be separable a proper subfield of L, $L_2 \supset K$, $L_2 \neq K$, exists. Using induction one may assume that a maximal subfield L_3 of the centralizer of L_2 exists, L_3 being separable over L_2 and $[L_3 : L_2] = [L : L_2]$. Even if L_3 is not separable over K, a proper extension M of K, separable over K and lying in L_3 exists. Since L_3 is a maximal subfield of dimension n over K, repeating the same consideration to the centralizer of M we prove the existence of a subfield L_1 of R, satisfying the conditions of Lemma 1.

If K is also nilpotent a subfield of L_1 exists which is a cyclic extension of K of prime degree and its centralizer R_* may be assumed to be an algebra of finite dimension over its centre C. As C is cyclic over K it follows that R is an automorphic extension of the centralizer of C (with respect to any automorphism of R_* induced by a non-identical automorphism of C over K). Consequently R is of finite dimension over K. Lemma 1 is proved.

The proof of Theorem 2 is based on the fact that any cyclic extension of P_0 of prime dimension p, p being the smallest number realized as a dimension of a proper extension of P_0 in R, satisfies the second step condition (see the proof of Theorem 1). Consequently R contains a special subalgebra S_1. Let $k \in N$ and assume S_k to be a subalgebra of R whose centre B_k is a finite extension of P_0, such that S_k is isomorphic to a tensor product over B_k of k central special B_k-subalgebras of S_k. If the centralizer in R of R_k differs from S_k, then S_k proves to be a subalgebra of a subalgebra S_{k+1} of R whose centre B_{k+1} is a finite extension of B_k, the centralizer in S_{k+1} of $B_{k+1} \otimes_{B_k} S_k$ being a special B_{k+1}-subalgebra of S_{k+1}. Lemma 1 makes clear that if the centralizer of B_k in R is S_k, for some natural k, then R if of finite dimension over P_0. Otherwise $R_1 := \bigcup_{k=1}^{\infty} S_k$ satisfies the conditions of Theorem 2. Theorem 2 is proved.

Proof of Theorem 3. It is realized via induction to the index n ($n^2=[R:P_0]$). If $n=1$, then $R=P_0$. If $n=p$, p — prime, then R is a special central P_0-algebra. As P_0 is nilpotent any maximal subfield L of R, L — separable over P_0 is s cyclic extension of P_0, hence R is an automorphic extenston of L.

If n is not prime, then any maximal subfield L of R separable over P_0 contains a subfield P_1 which is a cyclic extension of P_0. The centralizer R_1 of P_1 may be assumed by induction — as P_1 is nilpotent — to be an automorphic extension of L. Moreover, the respective subfields of R_1 all contain P_1, therefore they as well as their centralizers and their automorphisms satisfying the conditions of Definition 5, prove to satisfy the conditions of this definition related to R as well. Besides, any non-identical P_0-automorphism of P_1 induces an automorphism of R_1 satisfying Definition 5 in R. So R is proved to be an automorphic extension of L.

The second statement of Theorem 3 follows directly from Theorem 2 and [11, Th. 4.4.6] — a theorem a la Sylow. Theorem 3 is proved.

Proof of Theorem 4. The definition of a $\{p\}$-closure K_p of a field K makes clear that K_p is separable over K. Applying the fundamental theorem of infinite Galois theory and Sylow's theorem on profinite groups to K and the field of all separable elements over K in the algebraic closure $\bar{K}$ of K [10, Ch. I, §1, 1.4, Props. 3, 4] we prove the following proposition.

Proposition 3. *The $\{p\}$-closure of a field K exists, it is unique up-to a K-isomorphism and any $\{p\}$-field containing K is K-isomorphic to an extension of the $\{p\}$-closure of K.*

The set of fields $S:=\{U: P_0 \subseteq U \subseteq \bar{P}_0;\ R_{\alpha_U}$ is a division algebra for any $\alpha \in I$; R_{α_U} is not isomophic, too, R_{β_U} if $\alpha \neq \beta\}$ is inductive with respect to set theory inclusion hence a maximal element M on S exists due to Zorn's lemma. Assume a proper extension L of M exists of dimension prime-to-p. Then, R_{α_L} is a division algebra for any $\alpha \in I$. As $L \in S$, $R_{\alpha_L} \cong R_{\beta_L}$ for a couple of different indices $\alpha, \beta \in I$. The tensor product over M of R_{α_M} and $R'_{\beta M}$ — the M-algebra antiisomorphic to R_{β_M} — is a central simple M-algebra [11. Th, 4.1.1) isomorphic to a full matrix ring over a central division M-algebra V, $[V:M]=p^{2k}$, $k>0$, as R_{α_M} is not isomorphic, too, R_{β_M} — due to Wedderburn — Artin's theorem and [11, Th. 4.1.3] — consequently $R_{\alpha_L} \otimes_L R'_{\beta_L} = L_n = (V_L)_S = (R_{\alpha_M} \otimes_M R'_{\beta_M})_L$. This contradiction proves the assertion that no proper extension of M of dimension prime-to-p exists. Let L_1 be any fixed finite Galois extension of M. Applying the fundamental theorem of Galois theory to some Sylow $\{p\}$-subgroup of the Galois group of L_1 over M, we prove that M is a $\{p\}$-field (i. e. a $\{p\}$-nilpotent field). Due to Proposition 3 Theorem 4 is proved.

Remark. In this paper the full ring of $n \times n$ matrices over a division algebra A is signed by A_n or by $(A)_n$.

Proofs of corollaries to the main results.

Corollary 2 is a partial case of Corollary 1 due to [4, 5]. Corollary 3 is a direct result of Theorem 2. As for local fields, two facts — that a central division algebra R over a local field K contains a maximal subfield which is e cyclic extension of K (1, C) and also that if $[R:K]=n^2$, any extension of K of dimension n is isomorphic to a maximal subfield of R [8,Ch,IV, §1, p. 215] — prove that they satisfy the finite condition. So do fields of algebraic numbers as any central division algebra R over a field of algebraic (or p-adic) numbers satisfies the condition $[R:K]=s^2$, s being the order of $[R]\in B(K)$ — see [11, Ch. 4, p. 118].

Proof of corollary 6. Let $K=K_0(x_1,\dots,x_n,\dots,y_1,\dots,y_n,\dots)$, K_0 being a field, char $K_0\neq 2$. There exists a locally finite central division K-algebra $D=\otimes_n D_n$ (over K), D_n being a central division K-algebra of dimension 4 for any natural n [6, Ch. VIII, § 12, Ex. 14]. For any K-subalgebra E of D either $[E:K]=\infty$ or $[E:K]=2^k$, $k\geq 0$. Consequently D_{K_2} is a central division K_2-algebra, $D_{K_2}=\otimes_n D_{nK_2}$ (over K_2 — the $\{2\}$-closure of K). Corollary 6 is proved.

Proof of Corollary 7. It is a result of the following fact.

Proposition 4. *Let L be an extension of a field K and let R be a central L-algebra of finite dimension. For any fixed basis $x_1,\dots,x_n$, $x_i x_j=\Sigma_{k=1}^{n} c_{ijk}x_k$, $1\leq i\leq n$, $1\leq j\leq n$, $c_{ijk}\in L$. Let L_1 be the minimal subfield of L containing K and all the structural constants c_{ijk}. Then there exists a central L_1-algebra S of dimension n such that $R=S\otimes_{L_1}L=S_L$.*

The proof of Proposition 4 is clear as the minimal subring of R containing $x_1,\dots,x_n$ and L_1 may be regarded as the respective L_1-algebra S (if R is special we fix $\{x_1,\dots,x_n\}$ as in Definition 7).

If $B(K)\neq\{0\}$, then a central K-algebra R exists of dimension p^{2k}, $k>0$, for some prime p. Then R_{K_p} is a division algebra containing a special subalgebra R_1. Due to Proposition 4 $R_1=S_{1C(R)}$, S_1 being a special K-algebra as its centre is algebraic over K. Corollary 7 is proved.

Proof of Corollary 1. First we shall notice that an ordered field is cyclic iff it is a real closed field — combining the fact that any algebraic extension of a cyclic field is normal with [9, Ch. 11, Ths. 1, 3]. Any algebraic division algebra R over a real closed field P_0 is of finite dimension over P_0 since the degree over P_0 of the minimal polynomial of ony element of R is bounded by two, hence R is a PI-algebra of finite dimension over its centre due to Kaplansky [11, Th. 6.3.1]. Moreover, the theorem of Frobenius describing all division algebras of finite dimension over the field of real numbers is naturally extended to cover division algebras of finite dimension over a real closed field. Thus Corollary 1 is proved in case of P_0 being an ordered field.

Clearly Corollary 1 is reduced to the fact that no special central division algebra over an unorderable cyclic field exists. Assuming the opposite, we consider the case of a central special division algebra R of dimension p^2, $p=\mathrm{char}\,P_0\neq 0$ over a cyclic field P_0. Due to Zorn there exists an algebraic extension M of P_0 such that R_M is a division algebra unlike R_L, L being any proper algebraic extension of M. So any extension of M of dimension p is isomorphic to a maximal subfield of R_M — Proposition 1. Due to [9, Ch. VIII, Th. 11] $R_M=M(\xi,\eta)$, $\xi\eta=\eta(\xi+1)$, $\xi^p-\xi+a=0$, $\eta^p=b$, $a,b\in M$, while $M_p=M(\alpha,\beta)$, $\alpha\beta=\beta(\alpha+1)$, $\beta^p=c$, $\alpha^p-\alpha+d=0$, $c,d\in M$. Using the maximum condition on M as well as the fact that there exists a single separable extension of M in $\bar{M}$ of dimension p over M, by applying [2, Th. 2] and [11, Th. 4.3.1] we prove that d and c may be fixed among elements of $M\setminus M^p(M^p:=\{g\in M, \exists\, h\in M: h^p=g\})$ and reduce our problem to the case $b=c$, $a=kd$ for some $k\in GF(p)^*$. Due to cross product theory [11, Ths. 4.4.3, 4.4.5] $[R_M]=l[M_p]$, $l\in N$, $kl\equiv 1 \pmod p$, hence $[R_M]=[M_p]=0_{B(M)}$ which is a contradiction proving the assertion that no central special division P_0-algebra of dimension p^2, $p=\mathrm{char}\,P_0$ over a cyclic field P_0 exists.

Proposition 5. *Let K be a field containing a primitive p-th root of unity ε, p—prime. Let $L=K(\xi)=K(\eta)$ be a proper extension of K such that $\xi^p=a$, $\eta^p=b$, $a,b\in K$. Then $b=\alpha^p a^k$ for some $\alpha\in K$, $k\in\{1,\dots,p-1\}$.*

P r o o f. As $K \neq L$ it is well known that the polynomial $x^p - a \in K[x]$ is irreducible over K, hence $\eta = \sum_{i=1}^{p-1} \alpha_i \xi^i$, $\alpha_i \in K$, $i = 0, \ldots, p-1$. Being a root of the polynomial $x^p - b$, the element $\eta_1 = \sum_{i=0}^{p-1} \alpha_i \varepsilon^i \xi^i$ is equal to $\varepsilon^k \eta$ for some $k \in \{1, \ldots, p-1\}$. Proposition 5 is proved.

Proposition 4 proves that any central special algebra of dimension p^2, $p \neq \operatorname{char} P_0$ over a cyclic field p_0 is isomorphic to $R = P_0(\xi, \eta)\ \eta\xi = \varepsilon\xi\eta$, $\xi^p = \eta^p = a$, ε being a primitive p-th root of unity. A P_0-basis of R is the set $\{\xi^i \eta^j, 0 \leq i \leq p-1, 0 \leq j \leq p-1\}$. If p is odd then $\varepsilon^u a$, $u = 0, \ldots, p-1$, $\xi\eta^{p-1}$ are two-by-two different roots of the polynomial $x^p - a^p$ in $P_0(\xi\eta^{p-1})$ which proves that R is not a division algebra in this case. If $p = 2 \neq \operatorname{char} P_0$ we may assume that $a = -1$ as there exists a single extension of P_0 of dimension 2 in the algebraic closure P_0 of P_0, unless P_0 contains an element i such that $i^2 = -1$. If $i \in P_0$, $i^2 = -1$ then $(\xi + i\eta)^2 = 0$, i. e. R is not a division algebra. If $R = P_0(\xi, \eta)$, $\xi\eta = -\eta\xi$, $\xi^2 = \eta^2 = -1$, then either R is not a division algebra (as there exists a non-trivial P_0^3 zero (x_0, y_0, z_0) of the polynomial $x^2 + y^2 + z^2$, hence $(x_0\xi + y_0\eta + z_0\xi\eta)^2 = 0$) or any sum of squares in P_0 is a square in P_0. However, the second alternative means that P_0 may be ordered. Corollary 1 is proved.

P r o o f o f C o r o l l a r y 5. Let R be a central division algebra of dimension n^2, $n \in N$, over a field K and let L be a purely transcendental extension of K. Then R_L is a central division L-algebra of dimension n^2 [6, Ch. VIII, § 7, Ex. 24]. Thus Corollary 5 is reduced to the fact that for any fixed natural number k and prime number p, there exist k two-by-two unisomorphic special central division $Q(\varepsilon)$-algebras of dimension p^2 (the field of rational numbers is signed by Q, a primitive p-th root of unity — by ε).

D e f i n i t i o n 7. *A basis B of a central special K-algebra of dimension p^2 is said to be standard iff* $B = \{\xi^i \eta^j, 0 \leq i \leq p-1, 0 \leq j \leq p-1 : \xi\eta = \varepsilon\eta\xi, \varepsilon \neq 1 = \varepsilon^p$ *if* $\operatorname{char} K \neq p$ *or* $\xi\eta = \eta(\xi + 1)$ *if* $\operatorname{char} K = p\}$.

The existence of a standard basis is a direct result of Galois theory on cyclic extensions [9, Ch. VIII, § 6] and Noether-Skolem's theorem.

L e m m a 2. *Let L, F be extensions of finite relatively prime dimensions m, n, over a field K. Let also L be separable over K and let for some element c of K there exists no root of the norm equation $N_K(z) = c$ in L. Then $N_F(B) \neq c$ for any element* β of $L.F$.

P r o o f. It is sufficient to assume F to be simple over K. So let $L = K(\xi_1)$, $F = K(\theta_1)$, $L.F = F(\xi_1)$ for some $\xi_1 \in L$, $\theta_1 \in F$, $\xi_1, \ldots, \xi_m(\theta_1, \ldots, \theta_n)$ being all the roots in the algebraic closure $\bar{K}$ of K of the minimal polynomial of $\xi_1(\theta_1)$ over K. Assume $N_F(\beta) = c$ for some $\beta \in L.F$. Then for $k = 1, \ldots, m$ $g_k = \prod_{j=1}^{n} (\sum_{i=0}^{m-1} f_i(\theta_j)\xi_k^i) = \sum_{s=0}^{n(m-1)} (\sum_{j_1 + \cdots + i_n = s} f_{i_1}(\theta_1) \ldots f_{i_n}(\theta_n))\xi_k^s$ is an element of $K(\xi_k)$ as any transposition (hence any substitution) of $\{\theta_1, \ldots, \theta_n\}$ causes a substitution of $\{f_{i_1}(\theta_1) \ldots f_{i_n}(\theta_n) : 0 \leq i_j \leq m-1, j = 1, \ldots, n, i_1 + \cdots + i_n = s\}$, $s = 0, 1, \ldots, n(m-1)$ and as $f_0, \ldots, f_{m-1}$ are assumed to be polynomials of one variable x over K. On the other hand, for any fixed polynomials $h_0, h_1, \ldots, n_{n-1} \in K[x]$ for the same reasons $\delta_l = \prod_{i=1}^{m} (\sum_{j=0}^{n-1} h_j(\xi_i)\theta_l^j)$ is an element of $K(\theta_l)$. Moreover, it follows directly that $N_K(g_1) = g_1 \ldots g_m$, $N_K(\delta_1) = \delta_1 \ldots \delta_n$ (the norm of δ_1 is in F over K, $l = 1, \ldots, n$). As β belongs to L, F, $\beta = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} f_{ij}\xi_1^i\theta_1^j$, $f_{ij} \in K$,

$i=0, \ldots, m-1, j=0, 1, \ldots, n-1$, i. e. $\beta = \sum_{i=0}^{m-1} f_i(\theta_1)\xi_1^i = \sum_{j=0}^{n-1} h_j(\xi_1)\theta_1^j$ for some polynomials $f_0, \ldots, f_{m-1}, h_0, \ldots, h_{n-1}$ belonging to $K[x]$, therefore we have

$$N_K(g_1) = g_1 \ldots g_m = N_K(\delta_1) = \delta_1 \ldots \delta_n = c^n.$$

As m, n are relatively prime it follows that $N_K(\theta) = c$ for some $\theta \in L$ — the norm function is multiplicative. This contradiction proves Lemma 2.

Proposition 6. *For any two different prime numbers p, p_1 and any natural $k \geq 4$, there exist prime numbers $p_2, \ldots, p_k$ satisfying the conditions: $p_i \equiv 1 \pmod{p^2}$, $i=2, \ldots, k$; $pl \equiv 1 \pmod{p_j}$, $l=2, \ldots, k-1$, $j=1, \ldots, l-1$; $p_k \equiv a_s \times \pmod{p_s}$, a_s being a natural number such that $p_1 \ldots p_{s-1} a_s \pmod{p_s}$ generates $GF(p_s)^*$, $s=2, \ldots, k-1$.*

Proof. As p, p_1 are fixed we fix one by one $p_2, \ldots, p_{k-1}$ as follows: if $p_1, \ldots, p_{l-1}$ are fixed, then pl is fixed such that $pl \equiv 1 \pmod{p_j}$, $p_l \equiv 1 \pmod{p^2}$, $j=1, \ldots, l-1$; p_l — prime; as the fixed primes $p_2, \ldots, p_{k-1}$ are two-by-two different a_s can be fixed in a way that $p_1 \ldots p_{s-1} a_s \pmod{p_s}$ generates the cyclic group $GF(p_s)^*$, for $s=2, \ldots, k-1$. At last a prime number p_k is fixed such that $p_k \equiv 1 \pmod{p^2 . p_1}$, $p_k \equiv a_s \pmod{p_s}$, $s=2, \ldots, k-1$. Each step in that series can be taken due to Dirichlet's theorem about the prime numbers in an arithmetic progression and the Chinese theorem about residua. Proposition 6 is proved.

The following proposition is a direct result of Euler — Fermat's theorem.

Proposition 7. *Let $p, p_1, \ldots, p_k, k$, be fixed in accordance with Proposition 5. Let λ, μ be natural numbers such that for some i, j: $i \in \{1, \ldots, k-2\}$, $j \in \{i+1, \ldots, k-1\}$ $p_1 \ldots p_i p_{j+1} \ldots p_k \lambda^p - \mu^p \equiv 0 \pmod{p_{i+1}}$. Then $\lambda \equiv 0 \pmod{p_{i+1}}$ and $\mu \equiv 0 \pmod{p_{i+1}}$.*

Lemma 3. *Let $L = Q(\xi_k)$, $\xi_k^p = p_1 \ldots p_k$, $k, p_1, \ldots, p_k$ and p be fixed in accordance with Proposition 5. Then $N_Q(\alpha) p_1 \ldots p_i \neq p_1 \ldots p_j$ for any elemen α of L and any i, j such that $1 \leq i \leq j-1 \leq k-2$, $i, j \in N$.*

Proof. The polynomial $f(x_0, \ldots, x_{p-1}) = \prod_{j=0}^{p-1} (\sum_{i=0}^{p-1} \varepsilon^{ji} \xi_k^i x_i)$ over the ring of integer rational numbers Z is homogeneous of degree p. Moreover, $f(x_0, \ldots, x_{p-1}) = \Sigma_{m=0}^{p-1} \Sigma_{w(x_\alpha)=pm} r_k^m n_\alpha x_\alpha$, $n_\alpha \in Z$, $r_j := p_1 \ldots p_j$, $j=1, \ldots, k$ (α means $(\alpha_0, \ldots \alpha_{p-1})$, $x_\alpha - x_0^{\alpha_0} \ldots x_{p-1}^{\alpha_{p-1}}$, $\lambda_\alpha - \lambda_0^{\alpha_0} \ldots \lambda_{p-1}^{\alpha_{p-1}}$, $\lambda_u \in Z$, $u=0, \ldots, p-1$, $w(x_\alpha) = \Sigma_{u=1}^{p-1} u\alpha_u$, we shall sign by S the set of monomials x_α present in the ordinary representation of f as a sum of monomials x_α).

In terms of Lemma 3 let $g_{ij}(x_0, \ldots, x_p) = r_i f(x_0, \ldots, x_{p-1}) - r_j x_p^p$. Lemma 3 is equivalent to the fact that g_{ij} has only the trivial zero belonging to Z^{p+1}. As g_{ij} is homogeneous it is enough to prove that if $g_{ij}(\lambda)=0$ for some $\lambda = (\lambda_0, \ldots, \lambda_p) \in Z^{p+1}$, then $\lambda_u \equiv 0 \pmod{p_{i+1}}$, $u=0, \ldots, p$. As $i<j$ $\lambda_0 \equiv 0 \pmod{p_{i+1}}$, so $r_k^{m_\alpha} \lambda_\alpha \equiv 0 \pmod{p_{i+1}^2}$ for any $x_\alpha \in S$ with the eventual exception of λ_1^p and λ_p^p but as $g_{ij}(\lambda)=0$ due to proposition 6 $\lambda_i \equiv \lambda_p \equiv 0 \pmod{p_{i+1}}$. Assume $\lambda_u \equiv 0 \pmod{p_{i+1}}$, $u=0, 1, \ldots, m$. If $m=p-1$ there is nothing to prove. Let $m<p-1$. For any $x_\alpha \in S$, $s := \Sigma_{u=0}^m \alpha_u$. If $s \geq m+2$ then $\lambda_\alpha \equiv 0 \pmod{p_{i+1}^{m+2}}$. If $0<s \leq m+1$, then $w(x_\alpha) \geq (p-s)(m+1) > p(m+1-s)$, i. e. $r_k^{m_\alpha} \lambda_\alpha \equiv \pmod{p_{i+1}^{m+2}}$. If $x_\alpha \in S \setminus \{\lambda_{m+1}^p\}$ $s=0$, then $w(x_\alpha) = pm_\alpha$, $m_\alpha > m+1$, hence $r_k^{m_\alpha} \lambda_\alpha \equiv 0 \pmod{p_{i+1}^{m+2}}$. As $g_{ij}(\lambda)=0$, then

$r_k^{m+1}\lambda_{m+1}^p \equiv \alpha \pmod{p_{i+1}^{m+2}}$, i. e. $\lambda_{m+1} \equiv 0 \pmod{p_{i+1}}$, hence $\lambda_u \equiv 0 \pmod{p_{i+1}}$, $u=0, \ldots, p$. Lemma 3 is proved.

Let $R_{kj}=Q(\varepsilon)(\xi_k, \xi_j)$ be central special $Q(\varepsilon)$-algebras of dimension p^2, $j=1, \ldots, k-1$, $\{\xi_k^s \xi_j^r,\ 0 \leqq s \leqq p-1,\ 0 \leqq r \leqq p-1,\ \xi_k^p = r_k,\ \xi_j^p = r_j\}$ being its standard $Q(\varepsilon)$-basis. Due to Lemmas 2, 3 $N_{Q(\varepsilon)}(\alpha) r_i \neq r_j$, $i<j$, for any α belonging to $Q(\varepsilon, \xi_k)$, therefore $R_{k1}, \ldots, R_{kk-1}$ are two-by-two unisomorphic [7, Ch. V, Ex. 24]. At least $k-2$ of them are division algebras due to Wedderburn-Artin's theorem. Corollary 5 is proved.

As any field extension L of a field K is isomorphic to a maximal subfield of $K_{[L:K]}$, the norm condition in [7] referred to is always applicable to prove whether a special algebra is a division algebra. For example as a finite extension of a C_1-fields is C_1, too [10, Ch. II, § 3, Prop. 8(a)], the norm condition and Corollary 7 prove that any division of finite dimension over a C_1-field is a field from a somewhat different point of view in comparison with the proof of this result in [10, Ch. II, § 3]. In fact the proof of Corollary 7 indicates that there exists no special division algebra over a field K iff $\dim(K) \leq 1$ in terms of [10, Ch. II, § 3].

Due to the proof of Theorem 3 we can define that a central simple artinian algebra R over a nilpotent field P_0 is an automorphic extension of its proper subalgebra R_0 iff R_0 is the centralizer in R of a finite separable extension of P_0 (extending Definition 5 in the case of a nilpotent centre P_0).

If $R, R_i, \alpha_i, d_i, p_i \neq \operatorname{char} L_k$, $0 \leqq i \leqq k-1$, k and L_k are as in Definition 5 and a primitive p_i-th root of unity exists in L_k then $\Pi_{j=1}^{p} \alpha_i^{p-j}(r_i) \neq l_i$ $(l_i := d_i^{p_i} \in R_i)$ for any element r_i of R_i due to [6, Ch. VIII, § 12, Ex. 8].

Question. Does there exist a nilpotent field P_0 and a central division algebra of finite dimension over P_0 which is not a power of a prime number?

Acknowledgements. The author wishes to thank P. N. Siderov for the attention to this paper and for the encouragement.

REFERENCES

1. S. A. Amitsur. Division algebras. A Survey. *Amer. Math. Soc., Contemp. Math.*, **13**, 1982, 3—26.
2. E. Artin, O. Schreier. Eine Kennzeichnung der reell algeschlossenen Korper. The collected papers of Emil Artin. Addison — Wesley Publ. Comp., Inc., 1965, 289—295.
3. N. Jacobson. Structure of rings. *Amer. Math. Soc.*, **37**, 1956.
4. P. J McCarthy. Maximal fields disjoint from certain sets. *Proc. Amer. Math. Soc.*, **18**, 1967, 347—351.
5. F. Quigley. Maximal subfields of an algebraically closed field not containing a given element. *Proc. Amer. Math. Soc.*, **13**, 1962, 562—566.
6. Н. Бурбаки. Алгебра. Модули, кольца, формы. Москва, 1966.
7. Ю. А. Дрозд, В. В. Кириченко. Конечномерные алгебры. Киев, 1980.
8. Дж. Касселс, А. Фрелих. Алгебраическая теория чисел. Ж.-П. Серр., Локальная теория полей классов. Москва, 1969 (Гл. VI).
9. С. Ленг. Алгебра. Москва, 1968.
10. Ж.-П. Серр. Когомологии Галуа. Москва, 1968.
11. И. Херстейн. Некоммутативные кольца, Москва, 1972.
12. 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.

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

Received 17. 2. 1984