ON MAXIMALLY CENTRAL ALGEBRAS

GORÔ AZUMAYA

Introduction

Let A be a primary algebra with unit element over a field K and Z its center. Let $\bar{A}$ be the simple residue class algebra of A modulo its radical. Then it is known, and can readily be seen, that there holds the inequality $[A : K] \geqq t^2[Z : K]$, where t is the rank of A over its center. We call A maximally central if in particular $[A : K] = t^2[Z : K]$ i.e. if the rank $[Z : K]$ takes its maximum value. Further, an algebra which is a direct sum of those primary algebras will be called maximally central too. The notion was introduced in Azumaya-Nakayama [5], as a by-product of the study of absolutely uni-serial algebras.

In the present paper, we shall investigate maximally central algebras as a main subject. For this purpose, it seems very natural to the writer to extend the definition of these from coefficient fields to coefficient rings.[1] From this view point, we consider throughout this paper algebras[2] over coefficient rings, and show that maximally central algebras behave quite similarly as simple algebras in the theory of ordinary algebras. In the former part of this paper, we introduce, after some considerations about general rings and algebras, the notion of maximally central algebras over general coefficient rings in an apparently different way from above, and in the latter part we confine ourselves to particular type of coefficient rings called Hensel rings. Our methods used in this paper are related not only to the algebraic theory of ordinary algebras but also to the arithmetical theory of $\mathfrak{p}$-adic algebras, particularly obtained by Witt and Nakayama.[3]

The main object of this paper is however to prove, in the last section 7, an existence theorem of inertial algebras, which may be seen as a generalization of the Wedderburn-Malcev's theorem[4] as well as that of Nakayama's theorem.[5]

Received Dec. 25, 1950.

1) Cf. also the footnote (3) in Azumaya-Nakayama [5].

2) As for the term "algebra," see p. 125 below.

3) Witt [13], Nakayama [12].

4) Albert [1], III, Theorem 23; Deuring [5], II, § 11, Satz 1; Malcev [10].

5) Nakayama [11], Satz 3.

Although most properties concerning simple algebras can be transferred, without much difficulty, to maximally central algebras over general coefficient rings, our existence theorem does not hold untill the coefficient rings are assumed to be Hensel rings, and it seems to the writer that this is a principal theorem that has a deeper significance in the theory of maximally central algebras; most results from §1 to §6 should rather be regarded as preparation for this theorem.

The writer is grateful to Prof. T. Nakayama for his useful advices during the investigation of this subject.

1. Preliminaries on radicals

Let R be an (associative) ring. R may have an operater domain K such that $\alpha(a+b) = \alpha a + \alpha b$, $\alpha(ab) = (\alpha a)b = a(\alpha b)$ for every $\alpha \in K$ and $a, b \in R$. An element c of R is called *right quasi-regular*[6] if there exists an element c' in R such that $cc' = c + c'$; c' is then called a *right quasi-inverse* of c. In order that an element c is right quasi-regular it is necessary and sufficient that the right ideal $q(c)$ consisting of all elements of the form $x - cx$ with $x \in R$ is identical with R. The notions of the left quasi-regularity and the left quasi-inverse are also defined in the similar way. Further, an element c is called *quasi-regular* simply if it is right as well as left quasi-regular; in this case every right quasi-inverse and every left quasi-inverse of c coincides with each other and is called the *quasi-inverse* of c. For a quasi-regular element c with quasi-inverse c' we put $x^c = x - c'x - xc + c'xc$ for every $x \in R$. Then the mapping $x \to x^c$ is an automorphism of R, which we call the *inner automorphism generated by* c. If d is a second quasi-regular element then $c + d - cd$ is also quasi-regular and $(x^c)^d = x^{c+d-cd}$ holds for every $x \in R$. In case R has a unit element 1, c is quasi-regular if and only if $1 - c$ is regular; and when this is the case the inner automorphism $x \to x^c$ is nothing but the ordinary inner automorphism $x \to (1-c)^{-1}x(1-c)$. Finally, it is to be noted that *there exists no non-zero right (or left) quasi-regular idempotent element*, because from $e^2 = e$ and $e + e' = ee'$ it follows that $e + ee' = ee'$.

A (right or left) ideal consists merely of right quasi-regular elements if and only if it consists merely of left quasi-regular elments, and such an ideal we call a *quasi-regular ideal*. Let $\mathfrak{q}$ be a quasi-regular two-sided ideal. Then an element of R is quasi-regular if and only if it is quasi-regular modulo $\mathfrak{q}$.

LEMMA 1. *Let $\mathfrak{q}$ be a quasi-regular two-sided ideal of R and $\mathfrak{a}$ any two-sided ideal of R. Then an idempotent element lies in $\mathfrak{a}$ if (and only if) it lies in $\mathfrak{q} + \mathfrak{a}$.*

[6] For the following statements, see Jacobson [9].

Proof. Let e be an idempotent element of R lying in $\mathfrak{q}+\mathfrak{a}$. Then the residue class of e modulo $\mathfrak{a}$ is also idempotent and lies in $\mathfrak{q}+\mathfrak{a}/\mathfrak{a}$. But since $\mathfrak{q}+\mathfrak{a}/\mathfrak{a}$ is a quasi-regular ideal of $R/\mathfrak{a}$ it follows $e \equiv 0 \pmod{\mathfrak{a}}$.

Following N. Jacobson[7] the *radical* N of R is defined to be the join of all quasi-regular right ideals of R. Then N is itself a quasi-regular two-sided ideal of R and is also the join of all quasi-regular left ideals of R. Further, N is characterized as the intersection of all maximal right (or left) ideals of R that has left- (or right-)modulo units.[8] An element of R is quasi-regular if and only if it is quasi-regular modulo N, and hence the residue class ring R/N has the radical zero. Let us call a ring *semi-primitive* if it possesses the radical zero; if moreover it satisfies the minimum condition for right, or equivalently, for left ideals then we call it *semi-simple*.[9]

THEOREM 1. *Let $\mathfrak{M}$ be a finitely generated R-right-module such that $\mathfrak{M}N=\mathfrak{M}$. Then necessarily $\mathfrak{M}=0$.*

The proof is virtually the same as that of Jacobson [9], Theorem 10, but we give it here for completeness. Let $u_1, u_2, \ldots, u_n$ be finite generators of $\mathfrak{M}$. Then $\mathfrak{M}=\mathfrak{M}N=u_1N+u_2N+\ldots+u_nN$, and u_1 is expressed in a form $u_1z_1+u_2z_2+\ldots+u_nz_n$ with each z_i in N. Denoting by z_1' the quasi-inverse of z_1, $u_1=u_1-u_1(z_1+z_1'-z_1z_1')=(u_1-u_1z_1)-(u_1-u_1z_1)z_1'$ is in $u_2N+\ldots+u_nN$, and we have $M=u_2N+\ldots+u_nN$. Proceeding in this way it follows finally $\mathfrak{M}=0$.

Consider an idempotent element e and the subring eRe. Let c be in eRe and be quasi-regular in R. Then denoting by c' the quasi-inverse of c we have $cec'e=ec'ec=e(c+c')e=c+ec'e$, that is, $ec'e$ is a right quasi-inverse of c, and similarly $ec'e$ is a left quasi-inverse of c. Thus an element of eRe is quasi-regular in eRe if (and only if) c is quasi-regular in R; in particular, if $\mathfrak{q}$ is a quasi-regular two-sided ideal of R $e\mathfrak{q}e=\mathfrak{q}\cap eRe$ is a quasi-regular two-sided ideal of eRe.

Now two idempotent elements e and f are said to be *isomorphic* in R if there exist two elements a and b in R such that $ab=e$ and $ba=f$; here we may assume without loss of generality that $a\in eRf$ and $b\in fRe$. e and f are isomorphic if and only if the right ideals eR and fR, or by symmetry, the left ideals Re and Rf are operator-isomorphic.[10]

---

[7] Jacobson [9].

[8] An element u of R is called a left-modulo unit of a right ideal $\mathfrak{r}$ of R if $ua\equiv a \pmod{\mathfrak{r}}$ for every $a\in R$.

[9] In Jacobson [9], the term "semi-simple" was used for "semi-primitive" in our sense.

[10] For these, see Azumaya [3], I.

THEOREM 2. *Let $\mathfrak{q}$ be a quasi-regular two-sided ideal of R and let e and f be two idempotent elements of R. Then:*

i) *$e = f$ whenever $ef = fe$ and $e \equiv f$ (mod $\mathfrak{q}$).*

ii) *e and f are isomorphic in R if and only if their residue classes $\tilde{e}$ and $\tilde{f}$ modulo $\mathfrak{q}$ are isomorphic in $\tilde{R} = R/\mathfrak{q}$; further, for any given residue classes $\tilde{a} \in \tilde{e}\tilde{R}\tilde{f}$ and $\tilde{b} \in \tilde{f}\tilde{R}\tilde{e}$ such that $\tilde{a}\tilde{b} = \tilde{e}$ and $\tilde{b}\tilde{a} = \tilde{f}$ we can find representatives $a \in eRf$ and $b \in fRe$ of $\tilde{a}$ and $\tilde{b}$ respectively such that $ab = e$ and $ba = f$.*

Proof. i) If $ef = fe$ then $e - ef = e(e - f)$ is idempotent, while if $e \equiv f$ (mod $\mathfrak{q}$) it lies necessarily in $\mathfrak{q}$. Therefore it follows that $e - ef = 0$ i.e. $e = ef$, and similarly we have $f = ef$; this shows that $e = f$.

ii) Suppose that $\tilde{e}$ and $\tilde{f}$ are isomorphic and there are given residue classes $\tilde{a} \in \tilde{e}\tilde{R}\tilde{f}$ and $\tilde{b} \in \tilde{f}\tilde{R}\tilde{e}$ such that $\tilde{a}\tilde{b} = \tilde{e}$ and $\tilde{b}\tilde{a} = \tilde{f}$. Take from eRf and fRe two elements a_1 and b_1 so that a_1 and b_1 are representatives of $\tilde{a}$ and $\tilde{b}$ respectively. Then $a_1 b_1 \in eRe$ and $a_1 b_1 \equiv e$ (mod $e\mathfrak{q}e$). Since e is the unit element of the subring eRe and $e\mathfrak{q}e$ is a quasi-regular ideal of eRe, $a_1 b_1$ must be regular in eRe, that is, there exists an element $x \in eRe$ such that $a_1 b_1 x = e$. Similarly there exists an element $y \in fRf$ such that $y b_1 a_1 = f$. From this follows that $y b_1 = y b_1 e = y b_1 a_1 b_1 x = f b_1 x = b_1 x$. Hence $a = a_1$ and $b = b_1 x$ are required representatives of $\tilde{a}$ and $\tilde{b}$, and e and f are isomorphic. That conversely if e and f are isomorphic then $\tilde{e}$ and $\tilde{f}$ are isomorphic is clear.

THEOREM 3. *Let $\mathfrak{q}$ be a quasi-regular two-sided ideal of R. Then:*

i) *If $e_1, e_2, \ldots, e_n$ and $e_1^*, e_2^*, \ldots, e_n^*$ are two systems of mutually orthogonal idempotent elements of R such that $e_i \equiv e_i^*$ (mod $\mathfrak{q}$) for every i, there exists a (quasi-regular) element c in $\mathfrak{q}$ such that $e_i^c = e_i^*$ for every i.*

ii) *If $\{e_{ij};\ i, i = 1, 2, \ldots, n\}$ and $\{e_{ij}^*;\ i, j = 1, 2, \ldots, n\}$ are two systems of matrix units in R such that $e_{ij} \equiv e_{ij}^*$ (mod $\mathfrak{q}$) for every i, j, there exists a (quasi-regular) element c in $\mathfrak{q}$ such that $e_{ij}^c = e_{ij}^*$ for every i, j.*

Proof. Indeed, we have only to put $c = e + e^* - ee^* - \sum_{i=1}^{n} e_i e_i^*$ in the first case, while $c = e + e^* - ee^* - \sum_{i=1}^{n} e_{i1} e_{i1}^*$ in the second case; where $e = \sum_{i=1}^{n} e_i$, $e^* = \sum_{i=1}^{n} e_i^*$ or $e = \sum_{i=1}^{n} e_{ii}$, $e^* = \sum_{i=1}^{n} e_{ii}^*$, respectively.

Now we say that R is of the type (S) if R satisfies the following condition:

(S) *The residue class ring R/N modulo the radical N is semi-simple (i.e. R/N satisfies the minimum condition for right, or eqviualently, for left ideals).*

THEOREM 4. *Let R be of the type* (S) *and let $\{e_{ij};\ i, j = 1, 2, \ldots, n\}$ and $\{f_{ij};\ i, j = 1, 2, \ldots, n\}$ be two systems of matrix units of R such that two*

idempotent elements $e = \sum_{i=1}^{n} e_{ii}$ *and* $f = \sum_{i=1}^{n} f_{ii}$ *are isomorphic. Then there exists a quasi-regular element* c *in* R *such that* $e_{ij}^{c} = f_{ij}$ *for every* i, j.

Proof. By virtue of Theorem 3, ii), it suffices to treat the case where R is itself semi-simple. Then R possesses a unit element and is the direct sum of the left ideals Re and $R(1-e)$ as well as Rf and $R(1-f)$. Further Re and Rf are operator-isomorphic and are the direct sum of $Re_{11}, Re_{22}, \ldots, Re_{nn}$ and $Rf_{11}, Rf_{22}, \ldots, Rf_{nn}$ respectively. From these follows, since R is completely reducible for left ideals, that e_{11} and f_{11} as well as $1-e$ and $1-f$ are isomorphic, that is, there exist elements $a_1 \in e_{11}Rf_{11}$, $b_1 \in f_{11}Re_{11}$ and $a' \in (1-e)R(1-f)$, $b' \in (1-f)R(1-e)$ such that $a_1b_1 = e_{11}$, $b_1a_1 = f_{11}$ and $a'b' = 1-e$, $b'a' = 1-f$. Now we put $a = \sum_{i=1}^{n} e_{i1}a_1f_{1i} + a'$ and $b = \sum_{i=1}^{n} f_{i1}b_1e_{1i} + b'$. Then it can readily be seen that $ab = ba = 1$ and $e_{ij}a = e_{i1}a_1f_{1j} = af_{ij}$ for every i, j, and our assertion is proved.

COROLLARY. *Let* $\mathfrak{M}$ *be a module with operator domain and let* $\mathfrak{M}$ *be a direct sum of mutually operator-isomorphic (allowable) submoduli* $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_n$ *as well as of similar submoduli* $\mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_n$. *Suppose further that the operator-endomorphism ring of* $\mathfrak{M}$, *or equivalently, that of* $\mathfrak{M}_i$ *is of the type* (S). *Then* $\mathfrak{M}_i$ *and* $\mathfrak{N}_i$ *are operator-isomorphic.*

Proof. Let R be the operator-endomorphism ring of $\mathfrak{M}$. Then we can construct, as usual, two systems of matrix units $\{e_{ij}\}$ and $\{f_{ij}\}$ so that $\sum e_{ii} = \sum f_{ii} = 1$, the identity endomorphism, and $\mathfrak{M}e_{ii} = \mathfrak{M}_i$, $\mathfrak{M}f_{ii} = \mathfrak{N}_i$ for $i = 1, 2, \ldots, n$. Since R is of the type (S) there exists, by Theorem 4, a quasi-regular element c such that $e_{ii}^{c} = f_{ii}$, and so e_{ii} and f_{ii} are isomorphic; this means that $\mathfrak{M}_i$ and $\mathfrak{N}_i$ are operator-isomorphic.

2. Algebras over a general coefficient ring

From now on, we assume that K *is a commutative ring with unit element and when we deal with moduli with operator ring* K *we assume always that the unit element of* K *operates as an identity endomorphism.*

THEOREM 5. *Let* $\mathfrak{M}$ *be a finite* K*-module such that* $\mathfrak{p}\mathfrak{M} = \mathfrak{M}$ *for every maximal ideal* $\mathfrak{p}$ *of* K. *Then we have* $\mathfrak{M} = 0$.

Proof. Let $(u_1, u_2, \ldots, u_n)$ be a finite (but not necessarily linearly independent) basis of $\mathfrak{M}$ over K and let $\mathfrak{a}$ be the ideal of K consisting of all elements α of K such that $\alpha u_1 \in Ku_2 + \ldots + Ku_n$. Suppose that $\mathfrak{a} \neq K$. Then there exists a maximal ideal $\mathfrak{p}$ of K such that $\mathfrak{p}$ contains $\mathfrak{a}$ so that $\mathfrak{p}u_1 + Ku_2 + \ldots + Ku_n \neq Ku_1 + Ku_2 + \ldots + Ku_n = \mathfrak{M}$. But this contradicts to our assumption that $\mathfrak{p}u_1 + \mathfrak{p}u_2 + \ldots + \mathfrak{p}u_n (= \mathfrak{p}\mathfrak{M}) = \mathfrak{M}$, and therefore $\mathfrak{a} = K$ i.e. $\mathfrak{M} = Ku_2 + \ldots$

$+ Ku_n$. Continuing this way we have finally $\mathfrak{M} = 0$.

COROLLARY. *Let $\mathfrak{M}$ be a K-module and $\mathfrak{N}$ its K-submodule such that $\mathfrak{M} = \mathfrak{N} + \mathfrak{p}\mathfrak{M}$ for every maximal ideal $\mathfrak{p}$ of K. Then $\mathfrak{M} = \mathfrak{N}$ whenever $\mathfrak{M}$ is, or more generally, the residue class module $\mathfrak{M}/\mathfrak{N}$ is finite with respect to K.*

A K-module $\mathfrak{M}$ is called *regular* (with respect to K) if $\mathfrak{M}$ has a linearly independent finite basis over K.

THEOREM 6. *Let $\mathfrak{M}$ be a finite K-module. Then a finite system of element $(u_1, u_2, \ldots, u_n)$ in $\mathfrak{M}$ forms a basis of $\mathfrak{M}$ (over K) if (and only if) it is a basis of $\mathfrak{M}$ modulo $\mathfrak{p}\mathfrak{M}$ for every maximal ideal $\mathfrak{p}$ of K. If moreover $\mathfrak{M}$ is regular, then the system $(u_1, u_2, \ldots, u_n)$ is a linearly independent basis of $\mathfrak{M}$ if (and only if) it is a linearly independent basis of $\mathfrak{M}$ modulo $\mathfrak{p}\mathfrak{M}$ over the residue class field $K/\mathfrak{p}$ for every $\mathfrak{p}$.*

Proof. The first part follows from Corollary to Theorem 5 if we apply it to the submodule $\mathfrak{N} = Ku_1 + Ku_2 + \ldots + Ku_n$. To prove the second part, let $(v_1, v_2, \ldots, v_m)$ be a linearly independent basis of the regular module $\mathfrak{M}$. Then it forms modulo $\mathfrak{p}\mathfrak{M}$ also a linearly independent basis over $K/\mathfrak{p}$. It follows therefore that $m = n$ and if we put $u_i = \sum_{j=1}^{n} \alpha_{ij} v_j$ $(\alpha_{ij} \in K)$ the square matrix $\|\alpha_{ij}\|$ is regular modulo $\mathfrak{p}$, that is, the determinant $|\alpha_{ij}| \not\equiv 0 \pmod{\mathfrak{p}}$. This is the case for every $\mathfrak{p}$, and $|\alpha_{ij}|$ is a regular element of K, that is, $\|\alpha_{ij}\|$ is a regular matrix in K, which means nothing but that $(u_1, u_2, \ldots, u_n)$ is a linearly independent basis of $\mathfrak{M}$ over K.

As was shown in the above proof, the number n of the basis elements is independent of the choice of the basis, and we call it the *rank* of $\mathfrak{M}$ over K.

THEOREM 7. *Let $\mathfrak{M}$ be a finite K-module with a finite (but not necessarily linearly independent) basis $(u_1, u_2, \ldots, u_n)$ over K. Let θ be a K-endomorphism of $\mathfrak{M}$ and let M be a square matrix of degree n in K such that $(u_1 u_2 \ldots u_n)\theta = (u_1 u_2 \ldots u_n)M$. Then θ is a root of the (so-called) characteristic polynomial $|tE - M|$ of M.*

Proof. Consider the square matrix $\theta E - M$ in the commutative ring $K[\theta]$, the totality of polynomials of θ with coefficients in K. Let J be its "adjoint matrix," so that there holds $(\theta E - M)J = J(\theta E - M) = |\theta E - M| \cdot E$. It follows then $(u_1 u_2 \ldots u_n)\,|\theta E - M| = (u_1 u_2 \ldots u_n)(\theta E - M)J = ((u_1 u_2 \ldots u_n)\theta - (u_1 u_2 \ldots u_n)M)J = 0$, and we have $|\theta E - M| = 0$.

Now, let R be a ring. We say that R is a ring with *coefficient ring* K if R is a K-module such that $\alpha(ab) = (\alpha a)b = a(\alpha b)$ holds for every $a, b \in R$ and $\alpha \in K$. R is called *faithful* with respect to K if $\alpha = 0$ is the only element of K such that $\alpha R = 0$. If R has a unit element and is faithful with respect to K

then K is regarded in the natural manner as a subring of the center of R containing the unit element; if moreover K coincides with the center we call R *normal* over K. Let us call a ring R with coefficient ring K an *algebra* over K if R is finite with respect to K.

Let R be a ring with coefficient ring K and let $c_1, c_2, \ldots, c_s$ be a finite number of mutually commutative elements of R. Then we denote by $K\langle c_1, c_2, \ldots, c_s\rangle$ the commutative subring of R consisting of all polynomials of $c_1, c_2, \ldots, c_s$ with coefficients in K and without constant terms, while in case R has a unit element we mean by $K[c_1, c_2, \ldots, c_s]$, as usual, the commutative subring consisting of all polynomials of $c_1, c_2, \ldots, c_s$ with coefficients in K but with perhaps constant terms. We may assert here that if R is an algebra over K so are also both subrings $K\langle c_1, c_2, \ldots, c_s\rangle$ and $K[c_1, c_2, \ldots, c_s]$; in fact from Theorem 7 we have immediately

THEOREM 8.[11] *Let R be an algebra over K with a finite basis $(a_1, a_2, \ldots, a_n)$. Let c be an element of R and M a square matrix of degree n in K such that $c(a_1 a_2 \ldots a_n) = (a_1 a_2 \ldots a_n)M$. Then c is a root of the polynomial $t|tE - M|$, while in case R has a unit element c is indeed a root of the polynomial $|tE - M|$.*

Now let c be an element of an algebra R and denote by $q(c)$ the right ideal consisting of all elements of the form $x - cx$ with $x \in R$. Then the right quasi-regularity of c means that $q(c) = R$. Therefore for a maximal ideal $\mathfrak{p}$ of K the right quasi-regularity of c modulo $\mathfrak{p}R$ means that $q(c) + \mathfrak{p}R = R$. Hence if we apply Corollary to Theorem 5 to $\mathfrak{M} = R$ and $\mathfrak{N} = q(c)$, we have

LEMMA 2. *Let R be an algebra over K. Then an element of R is right (or left) quasi-regular if and only if it is right (or left) quasi-regular modulo $\mathfrak{p}R$ for every maximal ideal $\mathfrak{p}$ of K.*

COROLLARY. *Let R be an algebra over K and let $N(\mathfrak{p})$ be, for each maximal ideal $\mathfrak{p}$ of K, the two-sided ideal of R such that $N(\mathfrak{p}) \supseteq \mathfrak{p}R$ and $N(\mathfrak{p})/\mathfrak{p}R$ is the radical of the residue class algebra $R/\mathfrak{p}R$. Then the radical N of R is the intersection of all $N(\mathfrak{p})$'s: $N = \bigcap_{\mathfrak{p}} N(\mathfrak{p})$.*

Now we prove

THEOREM 9. *Let R be an algebra over K. Then every right (or left) quasi-regular element c is left (or right) quasi-regular too, and moreover its quasi-inverse c' is expressible as a polynomial of c with coefficients in K and without constant term: $c' \in K\langle c\rangle$.*

Proof. First, we prove the theorem in the special case where K is a field.

[11] This theorem was suggested to the writer by Nagata.

Let $(a_1, a_2, \ldots, a_n)$ be a linearly independent basis of R over K and let $M(x)$ be the left regular representation of R with respect to this basis: $x(a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, a_n)M(x)$. Then the right quasi-regularity of c implies the right quasi-regularity of the corresponding matrix $M(c)$: $M(c)M(c') = M(c) + M(c')$, and this means also that $E - M(c)$ is a regular matrix, that is, the determinant $|E - M(c)| \neq 0$. Now we put $|tE - M(c)| = t^n + \gamma_1 t^{n-1} + \gamma_2 t^{n-2} + \ldots + \gamma_n$ then it follows $1 + \gamma_1 + \gamma_2 + \ldots + \gamma_n (= |E - M(c)|) \neq 0$. Put then $\alpha = -(\gamma_1 + \gamma_2 + \ldots + \gamma_n)^{-1}$ and further $\alpha_1 = \alpha$, $\alpha_2 = \alpha(1 + \gamma_1)$, $\ldots$, $\alpha_n = \alpha(1 + \gamma_1 + \gamma_2 + \ldots + \gamma_{n-1})$. Then we have $\alpha_2 - \alpha_1 = \alpha\gamma_1$, $\alpha_3 - \alpha_2 = \alpha\gamma_2$, $\ldots$, $\alpha_n - \alpha_{n-1} = \alpha\gamma_{n-1}$ and $\alpha_n + 1 = -\alpha\gamma_n$. These show, combined with the fact that c is by Theorem 8 a root of the polynomial $t|tE - M(e)| = t^{n+1} + \gamma_1 t^n + \gamma_2 t^{n-1} + \ldots + \gamma_n t$, that $c' = \alpha_1 c^n + \alpha_2 c^{n-1} + \ldots + \alpha_n c$ is the (right as well as left) quasi-inverse of c: $cc' = c + c'$.

Next we turn to the case of general coefficient ring K. Let $\mathfrak{p}$ be a maximal ideal of K. Then the right quasi-regular element c is of course right quasi-regular modulo $\mathfrak{p}R$, and since $R/\mathfrak{p}R$ is an (ordinary) algebra over the residue class field $K/\mathfrak{p}$ c is quasi-regular modulo $\mathfrak{p}R$, as was shown just above. This is the case for every $\mathfrak{p}$, and by virtue of Lemma 2 c is indeed quasi-regular in R.

We want now to show that the quasi-inverse c' lies in $K\langle c\rangle$. For this purpose, we may assume without loss of generality that R coincides with the (commutative) subalgebra $K\langle c, c'\rangle$: $R = K\langle c, c'\rangle$. Let $\mathfrak{p}$ be a maximal ideal of K and consider again the residue class algebra $R/\mathfrak{p}R$ over the field $K/\mathfrak{p}$. Then it was also shown above that c' lies in $K\langle c\rangle$ modulo $\mathfrak{p}R$: $c' \in K\langle c\rangle + \mathfrak{p}R$ i.e. $R = K\langle c\rangle + \mathfrak{p}R$. Since this is the case for every $\mathfrak{p}$ we have $R = K\langle c\rangle$ by Corollary to Theorem 5, and this completes our proof.

COROLLARY. *Let R be an algebra over K and S its subalgebra. Then an element of S is quasi-regular in R (if and) only if it is quasi-regular in S.*

Now let $\mathfrak{M}$ be a module with operator ring K and Q a regular algebra over K with unit element. Then we can readily construct their *direct product* $\mathfrak{M} \times Q$ over K to be an Q-double-module in which $\mathfrak{M}$ is contained as a submodule element-wise commutative with Q and such that every linearly independent basis of Q over K is also the same of $\mathfrak{M} \times Q$ over $\mathfrak{M}$.[12] When $\mathfrak{M}$ forms further a ring R with coefficient ring K, so is also the direct product $R \times Q$; if moreover R possesses a unit element and is faithful with respect to K then Q (as well as R) may be regarded as a subalgebra of $R \times Q$ so that R and Q are element-wise commutative and they have, with $R \times Q$, a unit element in common.

[12] For the general definition of direct products, cf. Artin-Nesbitt-Thrall [2], VI.

Now we can assert

THEOREM 10. *Let N be the radical of R. Then $N \times Q$ is a quasi-regular two-sided ideal of $R \times Q$.*

Proof. Consider an arbitrary element c of $N \times Q$ and denote by $q(c)$ the right ideal of $R \times Q$ consisting of all elements of the form $x - cx$ with $x \in R \times Q$. Then we have evidently $R \times Q = q(c) + c(R \times Q) = q(c) + N \times Q$, which implies by virtue of Theorem 1 that $R \times Q = q(c)$, i.e., c is right quasi-regular in $R \times Q$.

A commutative ring Ω in which K is contained as a subring is called an *extention ring* of K if the unit element of K is also the unit element of Ω. If moreover Ω is finite with respect to K, Ω is called a *finite extension ring* of K; such an extension ring may be regarded as a faithful algebra over K. If R is an algebra over K and if Ω is a (finite and) regular extension ring of K. Then the direct product $R \times \Omega$ may be looked upon as an algebra over Ω, which we shall somtimes denote by R_Ω.

Finally we prove the following

THEOREM 11.[13] *Let R be a ring with coefficient ring K and possessing a unit element and let S be its subring such that the commuter ring $V_R(S)$ of S in R is of the type* (S). *Further, let Q be a regular algebra over K with unit element, and consider the direct product $R \times Q$ over K. Then an isomorphism φ of S into R can be extended to an inner automorphism of R if (and only if) it can be extended to an inner automorphism of $R \times Q$.*

Proof. Suppose that φ can be extended to an inner automorphism $x \to u^{-1}xu$ of $R \times Q$: $u^{-1}au = a^\varphi$ $(a \in S)$. Then uR may be seen as an S-R-double-module. Let $(b_1, b_2, \ldots, b_n)$ be a linearly independent basis of Q over K. Then it forms also a linearly independent basis of $R \times Q$ over R, that is, $R \times Q$ is a direct sum of submoduli $Rb_1, Rb_2, \ldots, Rb_n$ each (R-R-whence) S-R-isomomorphic to R. On the other hand, since $R \times Q = u(R \times Q)$, $R \times Q$ is a direct sum of submoduli $uRb_1, uRb_2, \ldots, uRb_n$ each S-R-isomorphic to uR. The operater-endomorphism ring of the S-R-double-module R is, regarded as a right operator ring, inverse-isomorphic to $V_R(S)$,[14] and hence is of the type (S). We may therefore apply Corollary to Theorem 4 to these two direct decompositions of $R \times Q$, so that R and uR are S-R-isomorphic. Let v be the element of R corresponding to u in uR, under an S-R-isomorphism between R and uR. Then v is evidently

[13] Cf. Azumaya [4], Theorem 8, 1).

[14] Observe that R has a unit element.

a regular element of R and, moreover, since $au = ua^{\varphi}$ for every $a \in S$ there must hold $av = va^{\varphi}$ for every $a \in S$. These show that φ can be extended to an inner automorphism $x \to v^{-1}xv$ of R.

3. Proper maximally central algebras over a general coefficient ring

Let A be a regular algebra over K possessing a unit element 1. Let A' be an algebra inverse-isomorphic to A. under a correspondence $a \leftrightarrow a'$, and construct the direct product $A \times A'$ over K. Then every A-double-module $\mathfrak{M}$ can be looked upon, in the usual fashion, as an $A \times A'$-right-module by defining the multiplication of $a' \in A'$ on the right as the multiplication of $a \in A$ on the left. In particular, A itself may be seen as an $A \times A'$-right-module. Let us call A proper maximally central over K if $A \times A'$ coincides with the K-endomorphism ring of A.

THEOREM 12. *Let A be a faithful algebra over K with unit element. Then in order that A is proper maximally central over K it is necessary and sufficient that there exists a basis $(a_1, a_2, \ldots, a_m)$ of A over K such that the square matrix*

$$\| a_j a_i \| = \begin{bmatrix} a_1a_1 & a_2a_1 & \cdots & a_ma_1 \\ a_1a_2 & a_2a_2 & \cdots & a_ma_2 \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_1a_m & a_2a_m & \cdots & a_ma_m \end{bmatrix}$$

is regular; and in fact, when this is the case, this condition is satisfied for every linearly independent basis $(a_1, a_2, \ldots, a_m)$.

Proof. First, we observe that the regularity of $\| a_j a_i \|$ implies the linear independency of $(a_1, a_2, \ldots, a_m)$. For, if elements $\alpha_1, \alpha_2, \ldots, \alpha_m$ of K satisfy the relation $\sum_{i=1}^{m} \alpha_i a_i = 0$ then $\sum_{i=1}^{m} \alpha_i a_j a_i = 0$ for $j = 1, 2, \ldots, m$, and hence we have $\alpha_1 = \alpha_2 = \cdots = \alpha_m = 0$.

Now the regularity of the matrix $\| a_j a_i \|$ means that for any system of m elements $(b_1, b_2, \ldots, b_m)$ of A there exists a uniquely determined system of elements $(x_1, x_2, \ldots, x_m)$ of A such that $(x_1x_2 \cdots x_m) \| a_j a_i \| = (b_1b_2 \cdots b_m)$. But this is also equivalent to saying that $\chi = \sum_{i=1}^{m} a_i x_i'$ is the only element of $A \times A'$ such that $(a_1\chi, a_2\chi, \ldots, a_m\chi) (= (a_1, a_2, \ldots, a_m)\chi = (a_1, a_2, \ldots, a_m) \sum_{i=1}^{m} a_i x_i') = (b_1, b_2, \ldots, b_m)$, which means nothing but the proper maximal centrality of A.

COROLLARY 1. *Let A be a proper maximally central algebra of rank m over K. Then $A \times A'$ is, as $A \times A'$-right-module, operator-isomorphic to the m-times direct sum A^m of A.*

In fact, if we associate with each $\chi \in A \times A'$ the vector $(a_1, a_2, \ldots, a_m)\chi = (a_1\chi, a_2\chi, \ldots, a_m\chi) \in A^m$ we obtain a desired operator-isomorphism of $A \times A'$ onto A^m.

COROLLARY 2. *Every full matrix ring $(K)_n$ over K of degree n is proper maximally central over K.*

In fact, if $\{e_{ij}: i, j = 1, 2, \ldots, n\}$ is a system of matrix units in $(K)_n$, it forms a linearly independent basis of $(K)_n$ over K and the corresponding square matrix $\| e_{kl}e_{ij} \|_{(ij),(kl)}$ (of degree n^2) has an inverse matrix $\|e_{lk}e_{ji}\|$ because $\sum_{p,q} e_{pq}e_{ij}e_{lk}e_{qp} = \sum_{p,q} e_{qp}e_{ji}e_{kl}e_{qp} = \delta_{(ij),(kl)}$.

THEOREM 13. *Let A be a proper maximally central algebra over K. Then K coincides with the center of A, and two-sided ideals $\mathfrak{a}$ of A and ideals $\mathfrak{k}$ of K correspond one-to-one by the following relation:*

$$\mathfrak{a} = \mathfrak{k}A, \quad \mathfrak{k} = \mathfrak{a} \cap K.$$

Further, when $\mathfrak{a}$ and $\mathfrak{k}$ correspond, $A/\mathfrak{a}$ is a proper maximally central algebra over $K/\mathfrak{k}$.

Proof. Let $(a_1, a_2, \ldots, a_m)$ be a linearly independent basis of A over K. Then there exists, for each $i = 1, 2, \ldots, m$, an element χ_i in $A \times A'$ such that $a_i\chi_i = 1$ and $a_j\chi_i = 0$ $(j \neq i)$.

Consider an element γ from the center of A and let $\gamma a_1 = \kappa_1 a_1 + \kappa_2 a_2 + \ldots + \kappa_m a_m$ with every κ_i in K. Then we have $\gamma = \gamma a_1\chi_1 = \kappa_1 a_1\chi_1 + \kappa_2 a_2\chi_1 + \ldots + \kappa_m a_m\chi_1 = \kappa_1$, and thus the center coincides with K.

Next let $\mathfrak{a}$ be a two-sided ideal of A and take an element $a = \alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_m a_m (\alpha_i \in K)$ from it. Since $\mathfrak{a}$ is then allowable with respect to $A \times A'$, $a\chi_i$ is in $\mathfrak{a}$; on the other hand, we have $a\chi_i = \alpha_1 a_1\chi_i + \ldots + \alpha_i a_i\chi_i + \ldots + \alpha_m a_m\chi_i = \alpha_i$, and α_i lies in $\mathfrak{k} = \mathfrak{a} \cap K$. This is the case for every $a \in \mathfrak{a}$ and for every $i = 1, 2, \ldots, m$, and therefore $\mathfrak{a} = \mathfrak{k}a_1 + \mathfrak{k}a_2 + \ldots + \mathfrak{k}a_m = \mathfrak{k}A$. The converse direction follows readily from the regularity of A over K.

The last assertion is an immediate consequence of Theorem 12, since every linearly independent basis of A over K is also the same of A modulo $\mathfrak{a}$ over $K/\mathfrak{k}$.

THEOREM 14. *In case K is a field, proper maximally central algebras over K are nothing but normal simple algebras over K.*

Proof. That every proper maximally central algebra is normal simple follows from Theorem 13, while the converse is a well-known fact in the theory of simple algebras.[15]

[15] Cf. Artin-Nesbett-Thrall [2], Theorem 7.1F, for instance.

THEOREM 15. *Let A be a regular algebra over K with unit element. Then A is proper maximally central over K if and only if for every maximal ideal $\mathfrak{p}$ of K $A/\mathfrak{p}A$ is a normal simple algebra over the residue class field $K/\mathfrak{p}$.*

Proof. Let $(a_1, a_2, \ldots, a_m)$ be a linearly independent basis of A over K. Then it is also the same of A modulo $\mathfrak{p}A$ over $K/\mathfrak{p}$, for every $\mathfrak{p}$. Consider the full matrix ring $(A)_m$ of degree m over A. If we apply Lemma 2 to the algebra $(A)_m$ we know that the matrix $\|a_j a_i\|$ is regular in $(A)_m$ if and only if it is regular modulo $\mathfrak{p}(A)_m = (\mathfrak{p}A)_m$ for every $\mathfrak{p}$, and this means, by Theorem 12 and in view of Theorem 14, the validity of our theorem.

COROLLARY. *The rank of a proper maximally central algebra A over (its center) K is a complete square number.*

Proof. Let $\mathfrak{p}$ be a maximal ideal of K. Then $A/\mathfrak{p}A$ is, by Theorem 15, a normal simple algebra over $K/\mathfrak{p}$ and has the same rank (over $K/\mathfrak{p}$) as the rank of A, and our assertion can be reduced to the well-known theorem of simple algebras.

Now we prove a theorem which may be seen as a generalization of (the second part) of Theorem 13:

THEOREM 16.[16] *Let A be a proper maximally central algebra over K. Let $\mathfrak{M}$ be an A-double-module for which the unit element of A is an identity operator on both sides and let $\mathfrak{N}$ be the K-submodule consisting of all elements of $\mathfrak{M}$ element-wise commutative with A. Then $\mathfrak{M}$ is a direct product of $\mathfrak{N}$ and A over K: $\mathfrak{M} = \mathfrak{N} \times A$. A-double-submoduli $\mathfrak{M}_0$ of $\mathfrak{M}$ and K-submoduli $\mathfrak{N}_0$ of $\mathfrak{N}$ correspond one-to-one by the following relation:*

$$\mathfrak{M}_0 = \mathfrak{N}_0 \times A, \quad \mathfrak{N}_0 = \mathfrak{M}_0 \cap \mathfrak{N}.$$

Proof. Looking upon $\mathfrak{M}$ as an $A \times A'$-right-module, $\mathfrak{M}$ is a sum of submoduli of the form $u(A \times A')$ with $u \in \mathfrak{M}$. But since $u(A \times A')$ is operator-homomorphic to $A \times A'$ and $A \times A'$ is by Corollary to Theorem 12 operator-isomorphic to the m-times direct sum A^m of A, $\mathfrak{M}$ is expressible as a sum of submoduli $\mathfrak{m}_\mu$ each operator-homomorpic to A. Let u_μ be the element of $\mathfrak{m}_\mu$ corresponding to the unit element 1 of A, under an operator-homomorphism of A onto $\mathfrak{m}_\mu$. Considered $\mathfrak{M}$ again as A-double-module, u_μ is element-wise commutative with A and moreover $\mathfrak{m}_\mu = u_\mu A$. We have therefore $\mathfrak{M} = \sum \mathfrak{m}_\mu = \sum u_\mu A = \mathfrak{N}A$. Now let $(a_1, a_2, \ldots, a_m)$ be a linearly independent basis of A over K and let χ_i be, for each $i = 1, 2, \ldots, m$, the element of $A \times A'$ such that $a_i \chi_i = 1$ and $a_j \chi_i = 0$ $(j \neq i)$, as in the proof of Theorem 13. Suppose that $v_1, v_2, \ldots, v_m$

[16] Cf. Azumaya [4], Lemma 1.

are elements of $\mathfrak{N}$ satisfying the relation $v_1a_1 + v_2a_2 + \ldots + v_ma_m = 0$. Then it follows $v_i = v_1a_1\chi_1 + \ldots + v_ia_i\chi_i + \ldots + v_ma_m\chi_i = 0$ for every i, and thus $a_1, a_2, \ldots, a_m$ are linearly independent with respect to $\mathfrak{N}$: $\mathfrak{M} = \mathfrak{N} \times A$.

The second assertion follows immediately from the first one, just proved.

COROLLARY.[17] *Let R be a ring with coefficient ring K and possessing a unit element and let A be its proper maximally central subalgebra containing the unit element of R. Then R is a direct product of A and its commuter ring $Q = V_R(A)$ in R: $R = Q \times A$. Between two-sided ideals R_0 of R and two-sided ideals Q_0 of Q, or between subrings R_0 of R containing A and subrings Q_0 of Q containing K, there exists a one-to-one correspondence by the following relation:*

$$R_0 = Q_0 \times A, \quad Q_0 = R_0 \cap Q.$$

THEOREM 17. *Let A and B are both proper maximally central algebras over K. Then the direct product $A \times B$ over K is also proper maximally central.*

Proof. Let $(a_1, a_2, \ldots, a_m)$ and $(b_1, b_2, \ldots, b_n)$ be respectively a linearly independent basis of A and B over K. Then a_ib_k $(i=1, 2, \ldots, m;\ k=1, 2, \ldots, n)$ form a linearly independent basis of $A \times B$ and the corresponding matrix $\| a_jb_l\ a_ib_k \|_{(ik),(jl)}$ is the so-called Kronecker product of $\| a_ja_i \|$ and $\| b_lb_k \|$. The regularities of $\| a_ja_i \|$ and $\| b_lb_k \|$ implies therefore the regularity of $\| a_jb_la_ib_k \|$, and this proves our theorem by virtue of Theorem 12.

Now let A be a faithful algebra over K with unit element and consider a full matrix ring $(A)_r$ over A of degree r, then for every maximal ideal $\mathfrak{p}$ of K the residue class algebra $(A)_r/\mathfrak{p}(A)_r$ is a full matrix ring over $A/\mathfrak{p}A$, and $(A)_r/\mathfrak{p}(A)_r$ is normal simple over $K/\mathfrak{p}$ if and only if so is $A/\mathfrak{p}A$. It follows therefore from Theorem 15 that $(A)_r$ is proper maximally central over K if and only if so is A. This fact enables us to introduce the notion of algebra classes over K, as in the case of simple algebras; namely, two proper maximally central algebras A and B over K are called *similar* (notation: $A \sim B$) if there exist two natural number r and s such that $(A)_r$ and $(B)_s$ are isomorphic. Similarity is an equivalent relation, and divides the set of all proper maximally central algebras over K into classes; every class we shall call an *algebra class* over K. Since the direct product of two proper maximally central algebras over K is also proper maximally central by Theorem 17 and since $A \sim B$ implies $A \times C \sim B \times C$ for every proper maximally central algebra C, there is defined in the natural manner a multiplication among algebra classes over K. The tatality of algebra classes over K forms then an abelian group, which we shall call the *algebra*

[17] Cf. Azumaya [4], Theorem 1. Cf. also Artin-Nesbitt-Thrall [2], Theorems 7.1B and 7.3F.

class group over K. Indeed, the class $\{K\}$ of all full matrix rings over K is the unit class, and for every class $\{A\}$ the class $\{A'\}$ represented by an algebra A' inverse-isomorphic to A is the inverse class of $\{A\}$ because of the very definition of the proper maximal centrality: $A \times A' \sim K$.

Finally we define the general notion of maximal centrality: an algebra A is called *maximally central* over K simply if A is decomposable into a (finite) direct sum of mutually orthogonal subalgebras $A_1, A_2, \ldots, A_k$, such that each A_κ is proper maximally central over its center. Once the notion is defined it can readily be seen from Theorem 12 that *proper maximally central algebras are nothing but regular, normal maximally central algebras.*

4. Algebras over a completely primary coefficient ring

A (not necessarily commutative) ring with unit element is called *completely primary* if the sum of any two non-regular elements is always non-regular too, or what defines the same, if it has a unique maximal right (or left) ideal; indeed, when this is the case, the maximal (right as well as left) ideal is the radical of the ring and consists of all non-regular elements.

Throughout the following we assume that K is a completely primary commutative ring with unit element and with unique maximal ideal ($=$ *radical*) $\mathfrak{p}$ *and shall consider those rings or algebras which have K as their coefficient ring; further we denote by $\overline{K}$ the residue class field $K/\mathfrak{p}$.*

Let R be an algebra over K. From Corollary to Lemma 2, it follows that the radical N of R contains $\mathfrak{p}R$ and $N/\mathfrak{p}R$ is the radical of the residue class algebra $R/\mathfrak{p}R$. Since $R/\mathfrak{p}R$ is an (ordinary) algebra over $\overline{K} = K/\mathfrak{p}$, the residue class ring R/N is semi-simple, i.e., R is of the type (S). Let us say that R is *unramified* over K if $\mathfrak{p}R$ is the radical of R, that is, if $R/\mathfrak{p}R$ is semi-simple.

Suppose now that R is not necessarily unramified but a subalgebra A is unramified. Then evidently $A \cap N \supseteq A \cap \mathfrak{p}R \supseteq \mathfrak{p}A$. On the other hand, $A \cap N$ is by Corollary to Theorem 9 a quasi-regular ideal of A, i.e., $A \cap N$ is contained in the radical $\mathfrak{p}A$ of A: $A \cap N \subseteq \mathfrak{p}A$. We have therefore $A \cap N = A \cap \mathfrak{p}R = \mathfrak{p}A$; or in other words, the natural homomorphism of R onto its residue class algebra R/N or $R/\mathfrak{p}R$ induces on A the natural homomorphism onto its residue class algebra $A/\mathfrak{p}A$. Finally, we call (the unramified subalgebra) A an *inertial algebra* of R if every residue class of R modulo N is represented by elements from A, that is, if $R = A + N$.

Now, from Theorem 15 it follows in particular that a regular algebra A with unit element is proper maximally central over K if (and only if) $A/\mathfrak{p}A$ is normal simple over $\overline{K}$. We can however assert that *this is the case even if we assume the faithfulness of A instead of its regularity.* For, if $a_1, a_2, \ldots, a_m$

be elements of A which form modulo $\mathfrak{p}A$ a linearly independent basis of $A/\mathfrak{p}A$ over $\overline{K}$ then they form by Theorem 6 a (not necessarily linearly independent) basis of A over K. Further, since $A/\mathfrak{p}A$ is normal simple, that is, proper maximally central over $\overline{K}$ (Theorem 14), the square matrix $\| a_j a_i \|$ is regular modulo $\mathfrak{p}(A)_m = (\mathfrak{p}A)_m$, and so $\| a_j a_i \|$ is by Lemma 2 regular in $(A)_m$, which means again by Theorem 12 the proper maximal centrality of A over K.

THEOREM 18. *Let R be a faithful algebra with unit element 1 over (completely primary) K and A its proper maximally central subalgebra containing K. Then every isomorphism φ of A into R which leaves K element-wise fixed can be extended to an inner automorphism of R.*

Proof. Consider the direct product $R \times A'$, where A' is a (proper maximally central) algebra over K inverse-isomorphic to A. Then it contains the subalgebra $A \times A'$, and $A \times A'$ is a (full) matrix algebra over K, i.e., there exists a system of matrix units $\{e_{ij}\}$ such that $\sum Ke_{ij} = A \times A'$ and $\sum e_{ii} = 1$. Now φ can be extended in the natural way to an isomorphism of $A \times A'$ into $R \times A'$ which leaves invariant every element of A'. Let f_{ij} be the element of $R \times A'$ corresponding to e_{ij}, under this extended isomorphism. Then $\{f_{ij}\}$ is also a system of matrix units and $\sum f_{ii} = 1$. Hence there exists, by Theorem 4, a regular element u in R such that $u^{-1}e_{ij}u = f_{ij}$ for every i, j. The inner automorphism $x \to u^{-1}xu$ induces therefore the extended isomorphism on $A \times A'$, that is, there holds $u^{-1}au = a^{\varphi}$ and $u^{-1}a'u = a'$ for every $a \in A$ and $a' \in A'$. Since R is by Corollary to Theorem 16 the commuter ring of A' in $R \times A'$, the latter relation implies that both u and u^{-1} lie in R, and the proof is completed.

COROLLARY. *Let A be a proper maximally central algebra over K. Then every automorphism of A which leaves K element-wise fixed is an inner automorphism.*

Now we want to see that in case K is a field our definition of maximal centrality coincides with the definition formerly given in Azumaya-Nakayama [5]. For this purpose, it is evident from Theorem 13 that we have only to treat the case of primary algebras. Let K be a field, and consider a primary algebra A over K with unit element. Let $\overline{A}$ be the simple residue class algebra of A modulo its radical N and t^2 the rank of $\overline{A}$ over its center. Let further Z be the center of A. Then Z is a completely primary commutative ring and in fact $\mathfrak{z} = N \cap Z$ is the unique maximal ideal of Z. Suppose that A is maximally central in our sense. Then, since A is two-sided directly indecomposable, A is necessarily proper maximally central over Z. Hence A is regular over Z and $\overline{A} = A/N$ is by Theorem 13 (also proper maximally central whence) normal over the residue class field $\overline{Z} = Z/\mathfrak{z}$. We have therfore that $[A : Z] = [\overline{A} : \overline{Z}]$

$= t^2$ whence $[A : K] = [A : Z][Z : K] = t^2[Z : K]$, which shows the maximal centrality of A in the sense of Azumaya-Nakayama [5]. Suppose conversely that $[A : K] \leqq t^2[Z : K]$. Then it was shown in (the proof of) Azumaya-Nakayama [5], Theorem 2 that $N = \mathfrak{z}A$ and $\bar{A} = A/N$ is normal over $\bar{Z} = Z/\mathfrak{z}$. Hence A is, as was pointed out in the above, proper maximally central over Z. Thus our assertion is proved.

5. Algebras over a Hensel ring

Let K be a completely primary commutative ring with unit element and with maximal ideal $\mathfrak{p}$.

First, we consider a polynomial rings $K[t]$ and $\bar{K}[t]$ of one variable t over K and $\bar{K} = K/\mathfrak{p}$ respectively. If we associate with each polynomial $f(t)$ in $K[t]$ the polynomial $\bar{f}(t)$ in $\bar{K}[t]$ which is obtained by replacing every coefficient of $f(t)$ by its residue class modulo $\mathfrak{p}$, then we have the natural homomorphism of $K[t]$ onto $\bar{K}[t]$; in this case, we call $\bar{f}(t)$ an *image polynomial* of $f(t)$ and $f(t)$ a *representative polynomial* of $\bar{f}(t)$ respectively. We say that two polynomials $f(t)$ and $g(t)$ in $K[t]$ are *relatively prime* if $(f(t)) + (g(t)) = K[t]$,[18] i.e., if there exist two polynomials $\varphi(t)$ and $\psi(t)$ such that $f(t)\varphi(t) + g(t)\psi(t) = 1$. When this is the case, every polynomial $l(t)$ divisible by both $f(t)$ and $g(t)$ is also divisible by $f(t)g(t)$, because $l(t) = l(t)f(t)\varphi(t) + l(t)g(t)\psi(t)$. This means that $(f(t)) \cap (g((t)) = (f(t)g(t))$, and therefore the residue class ring $K[t]/(f(t)g(t))$ is a direct sum of two ideals $(f(t))/(f(t)g(t))$ and $(g(t))/(f(t)g(t))$. Now we note that two polynomials $f(t)$ and $g(t)$ in $K[t]$ are relatively prime if (and only if) they are relatively prime modulo $\mathfrak{p}[t]$, provided that $f(t)$ has the highest coefficient 1. For, since that $f(t)$ and $g(t)$ are relatively prime modulo $\mathfrak{p}[t]$ means that $K[t] = (f(t)) + (g(t)) + \mathfrak{p}[t]$ and since $K[t]/(f(t))$ whence $K[t]/(f(t)) + (g(t))$ is finite with respect to K we have $K[t] = (f(t)) + (g(t))$, by virtue of Corollary to Theorem 5. We can moreover assert:

LEMMA 3.[19] *Let $f(t)$ be a polynomial in $K[t]$ with highest coefficient 1. Then every decomposition of the residue class ring $K[t]/(f(t))$ into a direct sum of two ideals is always given in the following form:*

$$K([t]/(f(t)) = (g(t))/(f(t)) \oplus (h(t))/(f(t)),$$

where $g(t)$ and $h(t)$ are relatively prime polynomials both with highest coefficients 1 and such that $g(t)h(t) = f(t)$.

---

[18] Under $(f(t))$ we mean the principal ideal $f(t)K[t]$.

[19] The validity of this Lemma and that of Theorem 19 were pointed out to the writer by Nakayama.

Proof. Suppose that I and I' be two ideals of $K[t]$ containing $(f(t))$ such that $K[t]/(f(t))$ is a direct sum of $I/(f(t))$ and $I'/(f(t))$: $K[t]/(f(t)) = I/(f(t)) \oplus I'/(f((t)))$. Then I and I' consists of all polynomials which annihilate I' and I modulo $(f(t))$ respectively. Let $\bar{f}(t)$, $\bar{I}$, $\bar{I}'$ be the homomorphic images of $f(t)$, I, I' respectively, by the natural homomorphism of $K[t]$ onto $\bar{K}[t]$. Then the residue class ring $\bar{K}[t]/(\bar{f}(t))$ is a direct sum of $\bar{I}/(\bar{f}(t))$ and $\bar{I}'/(\bar{f}(t))$: $\bar{K}[t]/(\bar{f}(t)) = \bar{I}/(\bar{f}(t)) \oplus \bar{I}'/(\bar{f}(t))$. Since $\bar{K}$ is a field, ideals $\bar{I}$ and $\bar{I}'$ of $\bar{K}[t]$ are principal, i.e., there exist polynomials $\bar{g}(t)$ and $\bar{h}(t)$ in $\bar{K}[t]$ such that $(\bar{g}(t)) = \bar{I}$ and $(\bar{h}(t)) = \bar{I}'$. Suppose that $\bar{g}(t)$ and $\bar{h}(t)$ are of degrees r and s respectively. Then the $r+s$ polynomials $\bar{g}(t), t\bar{g}(t), \ldots, t^{s-1}\bar{g}(t), \bar{h}(t), t\bar{h}(t), \ldots, t^{r-1}\bar{h}(t)$ form modulo $(\bar{f}(t))$ a linearly independent basis of $\bar{K}[t]/(\bar{f}(t))$ over $\bar{K}$. Now take from I and I' two polynomials $g_0(t)$ and $h_0(t)$ respectively so that they are representaive polynomials of $\bar{g}(t)$ and $\bar{h}(t)$. Then, since $\bar{K}[t]/(\bar{f}(t))$ is the residue class ring of $K[t]/(f(t))$ modulo its ideal $\mathfrak{p}(K[t]/(f(t))) = (\mathfrak{p}[t] + (f(t)))/(f(t))$, the $r+s$ polynomials $g_0(t), tg_0(t), \ldots, t^{s-1}g_0(t), h_0(t), th_0(t), \ldots, t^{r-1}h_0(t)$ form modulo $(f(t))$ a linearly independent basis of $K[t]/(f(t))$ over K, by virtue of Theorem 6. Observing further that $K[t]/(f(t))$ is a direct sum of $I/(f(t))$ and $I'/(f(t))$, we can conclude that the s polynomials $g_0(t), tg_0(t), \ldots, t^{s-1}g_0(t)$ and the r polynomials $h_0(t), th_0(t), \ldots, t^{r-1}h_0(t)$ form modulo $(f(t))$ a linearly independent basis of $I/(f(t))$ and $I'/(f(t))$ over K, respectively. It follows therefore that the polynomial $t^s g_0(t)$ in I is modulo $(f(t))$ expressible in the following form: $t^s g_0(t) \equiv \alpha_0 g_0(t) + \alpha_1 t g_0(t) + \ldots + \alpha_{s-1} t^{s-1} g_0(t) \pmod{f(t)}$, with α_i in K. Now we put $h(t) = t^s - \alpha_{s-1}t^{s-1} - \ldots - \alpha_1 t - \alpha_0$ then we have $h(t)g_0(t) \equiv 0 \pmod{f(t)}$, and $h(t)$ annihilates I modulo $(f(t))$ i.e. $h(t)$ lies in I'. Conversely, take any polynomial $k(t)$ from I'. Then it annihilates $g_0(t)$ modulo $(f(t))$: $k(t)g_0(t) \equiv 0 \pmod{f(t)}$. Since $h(t)$ is a polynomial of degree s and with highest coefficient 1, we can find a polynomial $r(t)$ of degree at most $s-1$ such that $k(t) \equiv r(t) \pmod{h(t)}$ whence $k(t)g_0(t) \equiv r(t)g_0(t) \pmod{h(t)g_0(t)}$. We have therfore $r(t)g_0(t) \equiv 0 \pmod{f(t)}$. But from the linear independency of $g_0(t), tg_0(t), \ldots, t^{s-1}g_0(t)$ modulo $(f(t))$ it follows that $r(t) = 0$, and thus every polynomial $k(t)$ in I' is divisible by $h(t)$ i.e. we have $I' = (h(t))$. Similarly, if we denote by $g(t)$ the polynomial of degree r and with highest coefficient 1 such that $g(t)h_0(t) \equiv 0 \pmod{f(t)}$ then we have $I = (g(t))$. Since $I + I' = K[t]$, $g(t)$ and $h(t)$ are relatively prime. Hence $(g(t)h(t)) = (g(t)) \cap (h(t)) = (f(t))$; but since both $g(t)h(t)$ and $f(t)$ have the highest coefficients 1 it follows that $g(t)h(t) = f(t)$, and the proof is completed.

Now let $f(t)$ be a polynomial in $K[t]$ and let $\bar{f}(t)$ be its image polynomial in $\bar{K}[t]$ (by the natural homomorphism of $K[t]$ onto $\bar{K}[t]$). Let us say that the

Hensel lemma holds for $f(t)$ if for any given relatively prime polynomials $\bar{g}(t)$ and $\bar{h}(t)$ in $\bar{K}[t]$ such that $\bar{g}(t)\bar{h}(t) = \bar{f}(t)$ and $\bar{g}(t)$ has the highest coefficient 1 there exist in $K[t]$ two representative polynomials $g(t)$ and $h(t)$ of $\bar{g}(t)$ and $\bar{h}(t)$ respectively such that $g(t)h(t) = f(t)$ and $g(t)$ has the highest coefficient 1. Here, we note that $g(t)$ and $h(t)$ are relatively prime (since they are relatively prime modulo $\mathfrak{p}[t]$ and $g(t)$ has the highest coefficient 1).

Noticing the fact that in every commutative ring with unit element there exists a one-to-one correspondence in a definite manner between idempotent elements and direct decompositions into two ideals, we have immediately from Lemma 3 the following

THEOREM 19. *Let* $f(t)$ *be a polynomial in* $K[t]$ *with highest coefficient 1. Then in order that the Hensel lemma holds for* $f(t)$ *it is necessary and sufficient that for every idempotent element of (the residue class ring)* $\bar{K}[t]/(\bar{f}(t))$ *there exists in* $K[t]/(f(t))$ *an idempotent representative of it.*

COROLLARY. *Let* $f(t)$ *be a polynomial in* $K[t]$ *with highest coefficient 1 for which the Hensel lemma holds and let* $g(t)$ *be a polynomial in* $K[t]$ *by which* $f(t)$ *is divisible. Then for every idempotent element of* $(\bar{g}(t))/(\bar{f}(t))$ *there exists in* $(g(t))/(f(t))$ *an idempotent representative of it.*

Proof. $\bar{K}[t]/(\bar{f}(t))$ is the residue class ring of $K[t]/(f(t))$ modulo its ideal $\mathfrak{p}(K[t]/(f(t)))$, which is quasi-regular since $K[t]/(f(t))$ is finite with respect to K. Hence it follows from Lemma 1 that an idempotent element of $K[t]/(f(t))$ lies in the ideal $(g(t))/(f(t))$ if its residue class ($\in \bar{K}[t]/\bar{f}(t)$) lies in $(\bar{g}(t))/(\bar{f}(t))$.

THEOREM 20. *Let* $f(t)$ *be a polynomial in* $K[t]$ *with highest coefficient 1 for which the Hensel lemma holds. Let* Z *be a finite extension ring of* K *such that* $Z = K[c]$ *with* $f(c) = 0$ *and let* $\mathfrak{z}$ *be an ideal of* Z. *Then for every idempotent element* $\tilde{e}$ *of the residue class ring* $\tilde{Z} = Z/\mathfrak{z}$ *there exists in* Z *an idempotent representative* e *of* $\tilde{e}$.

Proof. First, we treat the special case where $\mathfrak{z} = \mathfrak{p}Z$. Since $Z = K[c]$ with $f(c) = 0$, Z is K-homomorphic to $K[t]/(f(t))$ by associating with $t \pmod{f(t)}$ the element c. Similarly, if we put $\bar{c}$ the residue class of c modulo $\mathfrak{p}Z$, $\bar{Z} = Z/\mathfrak{p}Z$ is $\bar{K}$-homomorphic to $\bar{K}[t]/(\bar{f}(t))$ by associating with $t \pmod{\bar{f}(t)}$ the element $\bar{c}$. Suppose that there is given an idempotent element $\bar{e}$ in $\bar{Z}$. Then, since $\bar{K}[t]/(\bar{f}(t))$ may be looked upon as an (ordinary) algebra over the field $\bar{K} = K/\mathfrak{p}$, there exists in $\bar{K}[t]/(\bar{f}(t))$ an idempotent representative of $\bar{e}$, as is well-known. Hence there exists in $K[t]/(f(t))$ an idempotent representative of it by virtue of Theorem 19. Let e be the homomorphic image of this idempotent element (of $K[t]/(f(t))$) in Z. Then e is evidently a required idempotent

representative of $\bar{e}$.

Next, we proceed to the general case. Consider the residue class ring $\tilde{Z}/\mathfrak{p}\tilde{Z}$. Then the residue class of $\tilde{e}$ modulo $\mathfrak{p}\tilde{Z}$ is an idempotent element of $\tilde{Z}/\mathfrak{p}\tilde{Z}$. On the other hand, since $\tilde{Z}/\mathfrak{p}\tilde{Z}$ $(= Z/\mathfrak{p}Z + \mathfrak{z})$ is a residue class ring of $\bar{Z} = Z/\mathfrak{p}Z$ and since $\bar{Z}$ is an (ordinary) algebra over $\bar{K} = K/\mathfrak{p}$, we can find in $\bar{Z}$ an idempotent representative $\bar{e}$ of $\tilde{e}$ (mod $\mathfrak{p}\tilde{Z}$). Then we can find further an idempotent element e in Z so that $\bar{e}$ is the residue class of e modulo $\mathfrak{p}Z$, as was shown just above. If we take the residue class of e modulo $\mathfrak{z}$ we have a second idempotent representative of $\tilde{e}$ (mod $\mathfrak{p}\tilde{Z}$) in $\tilde{Z}$. Since $\mathfrak{p}\tilde{Z}$ is however a quasi-regular two-sided ideal of $\tilde{Z}$ this must coincide with the given $\tilde{e}$ by virtue of Theorem 2, i), and thus our theorem is proved.

THEOREM 21. *Let $f(t)$ be a polynomial in $K[t]$ with highest coefficient 1 and without constant term for which the Hensel lemma holds. Let Z be a (commutative) algebra over K such that $Z = K\langle c\rangle$ with $f(c) = 0$ and let $\mathfrak{z}$ be an ideal of Z. Then for every idempotent element $\tilde{e}$ of the residue class algebra $\tilde{Z} = Z/\mathfrak{z}$ there exists in Z an idempotent representative e of $\tilde{e}$.*

Proof. The proof can be obtained in the same way as that of the preceding theorem if we consider the algebras $K\langle t\rangle/(f(t)) = (t)/(f(t))$ and $\bar{K}\langle t\rangle/(\bar{f}(t))$ $= (t)/(\bar{f}(t))$ instead of $K[t]/(f(t))$ and $\bar{K}[t]/(\bar{f}(t))$ and make use of Corollary to Theorem 19 to these algebras.

Now let us call (completely primary) K a *Hensel ring* if the Hensel lemma holds for every polynomial in $K[t]$ with highest coefficient 1.

THEOREM 22. *In order that K is a Hensel ring it is necessary and sufficient that the following condition holds for every finite extension Z of K and for every ideal $\mathfrak{z}$ of Z:*

For any given idempotent element $\tilde{e}$ of the residue class ring $\tilde{Z} = Z/\mathfrak{z}$ there exists in Z an idempotent representative e of $\tilde{e}$.

Proof. Assume that K is a Hensel ring. Take from Z a representative c of the residue class $\tilde{e}$ and consider the subring $K[c]$. Then c is a root of a polynomial $f(t)$ in $K[t]$ with highest coefficient 1 (Theorem 8), and the Hensel lemma holds for $f(t)$. Hence there exists by Theorem 20 an idempotent element e in $K[c]$ which is a representative of $\tilde{e}$ $(\in K[\tilde{c}])$.

The sufficiency follows directly from Theorem 19.

THEOREM 23. *Let K be a Hensel ring. Then every residue class ring of K as well as every completely primary finite extension ring of K is also a Hensel ring.*

Proof. That every residue class ring of K is a Hensel ring is clear. The other assertion is an immediate consequence of Theorem 22, since every finite

extension of a finite extension of K is also a finite extension of K.

Example. The valuation ring of a $\mathfrak{p}$-adic number field is a Hensel ring. More generally, Let K be a completly primary commutative ring with unit element and suppose that the intersection of all powers of the maximal ideal $\mathfrak{p}$ is zero: $\bigcap_{\nu=1}^{\infty} \mathfrak{p}^{\nu} = 0$. Then we introduce in K a topology by taking all the powers $\mathfrak{p}^{\nu}$ as a neighbourhood system of 0 so that K becoms a topological ring. Suppose further that K is complete with respect to this uniform topology; such K is called a complete local ring[20] in the generalized sense. Then for every polynomial in $K[t]$ (not necessarily with highest coefficient 1) the Hensel lemma holds,[21] and hence K is a Hensel ring. The proof may be obtained by modifying slightly the proof of the usual Hensel lemma in the case of $\mathfrak{p}$-adic number fields, and should be omitted.

THEOREM 24. *Let R be an algebra over a Hensel ring K and let $\mathfrak{a}$ be its two-sided ideal. Then for any given system of mutually orthogonal idempotent elements $\tilde{e}_1, \tilde{e}_2, \ldots, \tilde{e}_n$ in the residue class algebra $\tilde{R} = R/\mathfrak{a}$ we can find actually a system of mutually orthogonal idempotent elements $e_1, e_2, \ldots, e_n$ in R such that each e_i is a representative of $\tilde{e}_i$.*

Proof. It is evidently sufficient to show that if e_0 is an idempotent element of R and if $\tilde{e}$ is an idempotent element of $\tilde{R} = R/\mathfrak{a}$ which is orthogonal to the residue class $\tilde{e}_0$ of e_0 modulo a then there exists in R an idempotent representative e of $\tilde{e}$ which is orthogonal to e_0: $ee_0 = e_0e = 0$. To prove this, consider the subalgebra $t(e_0)$ of R consisting of all two-sided annihilators of e_0 in R. As is well-known, $t(e_0)$ coincides with the set of all elements of the form $x - e_0x - xe_0 + e_0xe_0$ with $x \in R$, and so the homomorphic image of $t(e_0)$ by the natural homomorphism of R onto $\tilde{R} = R/\mathfrak{a}$ is nothing but the subalgebra $t(\tilde{e}_0)$ of R consisting of all two-sided annihilators of $\tilde{e}_0$ in $\tilde{R}$. Since $\tilde{e}$ is orthogonal to $\tilde{e}_0$, that is, since $\tilde{e}$ lies in $t(\tilde{e}_0)$, we can find in $t(e_0)$ a representative c of $\tilde{e}$; c is by Theorem 8 a root of a polynomial $f(t)$ in $K[t]$ with highest coefficient 1 and without constant term, and the Hensel lemma holds for $f(t)$. Consider further the subalgebra $K\langle c\rangle$ of $t(e_0)$. Then there exists in $K\langle c\rangle$ an idempotent representative e of $\tilde{e}$ by virtue of Theorem 21, and e is the required idempotent element.

THEOREM 25. *Let R be an algebra over a Hensel ring K and let $\mathfrak{q}$ be its quasi-regular two-sided ideal. Suppose that there is given a system of matrix units $\{\tilde{e}_{ij}; i, j = 1, 2, \ldots, n\}$ in the residue class algebra $\tilde{R} = R/\mathfrak{q}$. Then there exists in R a system of matrix units $\{e_{ij}; i, j = 1, 2, \ldots, n\}$ such that each*

[20] The notion was introduced by W. Krull and was generalized by Nogata [11].

[21] Nagata [11], Proposition 5; cf. also Cohen [7], Theorem 4.

e_{ij} is a representative of $\tilde{e}_{ij}$.

Proof. Since $\tilde{e}_{11}, \tilde{e}_{22}, \ldots, \tilde{e}_{nn}$ are mutually orthogonal idempotent elements of R, there exist by the preceding theorem mutually orthogonal idempotent elements $e_1, e_2, \ldots, e_n$ in R such that each e_i is a representative of $\tilde{e}_{ii}$. Further, since $\tilde{e}_{11}\tilde{e}_{1i} = \tilde{e}_{1i}\tilde{e}_{ii} = \tilde{e}_{1i}$, $\tilde{e}_{ii}\tilde{e}_{i1} = \tilde{e}_{i1}\tilde{e}_{11} = \tilde{e}_{i1}$ and $\tilde{e}_{1i}\tilde{e}_{i1} = \tilde{e}_{11}$, $\tilde{e}_{i1}\tilde{e}_{1i} = \tilde{e}_{ii}$ for every $i \neq 1$, we can find, by applying Theorem 2, ii) to $\tilde{e} = \tilde{e}_{11}$, $\tilde{f} = \tilde{e}_{ii}$ and $\tilde{a} = \tilde{e}_{1i}$, $\tilde{b} = \tilde{e}_{i1}$, representatives e_{1i} and e_{i1} of $\tilde{e}_{1i}$ and $\tilde{e}_{i1}$ such that $e_1e_{1i} = e_{1i}e_i = e_{1i}$, $e_ie_{i1} = e_{i1}e_1 = e_{i1}$ and $e_{1i}e_{i1} = e_1$, $e_{i1}e_{1i} = e_i$ for every $i \neq 1$. Put now $e_{11} = e_1$ and $e_{ij} = e_{i1}e_{1j}$ for $i \neq 1$, $j \neq 1$. Then $e_{ii} = e_i$ for every i, and $\{e_{ij}; i, j = 1, 2, \ldots, n\}$ is a desired system of matrix units in R, as can readily be verified.

Now an algebra R with unit element over a Hensel ring K is called *primary* if the residue class algebra $\bar{R} = R/N$ modulo its radical N is a simple algebra.

THEOREM 26. *An algebra R with unit element over a Hensel ring K is primary if and only if R is a full matrix ring over a completly primary algebra; and such a completely primary algebra is uniquely determined by R up to K-isomorphisms.*

Proof. Let R be primary. Then the simple residue class algebra $\bar{R} = R/N$ is a full matrix ring over a division subalgebra $\bar{R}_0$, that is, there exists a system of matrix unit $\{\bar{e}_{ij}\}$ in $\bar{R}$ such that $\bar{R} = \sum \bar{e}_{ij}\bar{R}_0$ and $\bar{R}_0$ is the commuter ring of $\{\bar{e}_{ij}\}$. Hence we can find by virtue of Theorem 25 a system of matrix units $\{e_{ij}\}$ in R such that each e_{ij} is a representative of $\bar{e}_{ij}$. Denoting by R_0 the commuter ring of $\{e_{ij}\}$ in R, R is a full matrix ring over R_0: $R = \sum e_{ij}R_0$; further, the radical N of R is the totality of matrices in the radical N_0 of R_0. $\bar{R} = R/N$ is therefore a full matix ring over R_0/N_0, and we have $\bar{R}_0 = R_0/N_0$. Thus R_0 is completely primary. The uniqueness of such R_0 follows readily from Theorem 4.

Let us turn to an arbitrary algebra R over a Hensel ring K. Then the residue class algebra $\bar{R} = R/N$ modulo its radical N is semi-simple, that is, a direct sum of mutually orthogonal simple subalgebras $\bar{R}_1, \bar{R}_2, \ldots, \bar{R}_k$:

$$\bar{R} = \bar{R}_1 \oplus \bar{R}_2 \oplus \ldots \oplus \bar{R}_k.$$

Let $\bar{E}_\kappa$ be, for each κ, the unit element of $\bar{R}_\kappa$. Then $\bar{E}_1, \bar{E}_2, \ldots, \bar{E}_k$ are mutually orthogonal idempotent elements of $\bar{R}$, and there exist by Theorem 24 mutually orthogonal idempotent elements $E_1, E_2, \ldots, E_k$ in R such that each E_κ is a representative of $\bar{E}_\kappa$. Every subalgebra $E_\kappa RE_\kappa$ has the unit element E_κ and if we take it modulo its quasi-regular two-sided ideal $E_\kappa NE_\kappa$ we have the simple residue class algebra $\bar{R}_\kappa = \bar{E}_\kappa \bar{R} \bar{E}_\kappa$, that is, ($E_\kappa NE_\kappa$ is the radical of $E_\kappa RE_\kappa$ and) $E_\kappa RE_\kappa$ is primary. Furthermore there holds the following direct decomposition of R:

$$R = E_1RE_1 \oplus E_2RE_2 \oplus \ldots \oplus E_kRE_k \oplus \mathfrak{n},$$

where $\mathfrak{n}$ is a K-submodule of the radical N. Therefore if in particular R is unramified over K, that is, if $N = \mathfrak{p}R$ it follows from Corollary to Theorem 5 that $R = E_1RE_1 \oplus E_2RE_2 \oplus \ldots \oplus E_kRE_k$:

THEOREM 27. *Every unramified algebra over a Hensel ring K has a unit element and is a direct sum of mutually orthogonal primary subalgebras.*

Remark. The notion of radicals considered throughout this paper was first introduced by Jacobson. The writer has however defined in his previous paper[22] another notion of radicals; a two-sided ideal C of a ring R was called a radical if all its (right as well as left) subideals, including C itself, and only those contain no non-zero idempotent element. This radical C does not always exist, and even when it exists, it does not coincide in general with the Jacobson's radical N; but it contains always N. However in case R is an algebra over a Hensel ring K both notions of radicals coincide. In fact, if I is a (right or left) ideal of R not contained in (the Jacobson's radical) N then it contains modulo N a non-zero idempotent element $\bar{e}$, because $\bar{R} = R/N$ is semi-simple. Hence if we apply Theorem 24 to the algebra I it contains indeed a (non-zero) idempotent representative e of $\bar{e}$, and this shows that N is the radical in the writer's sense too; R is in fact a strongly semi-primary ring. Furthermore, the notion of primary as well as completely primary algebras coincides with the same ones given in the writer's paper, provided that the existence of unit elements is assumed.

6. Unramified extensions, crossed products and algebra class groups

Throughout this section we assume that K is a Hensel ring (with maximal ideal $\mathfrak{p}$ and with residue class field $\bar{K} = K/\mathfrak{p}$). Then every completely primary finite extension ring of K is also a Hensel ring by virtue of Theorem 23.

LEMMA 4. *Let $f(t)$ be a polynomial with highest coefficient 1 in $K[t]$ and let $\bar{f}(t)$ be its image polynomial in $\bar{K}[t]$ (by the natural homomorphism of $K[t]$ onto $\bar{K}[t]$). Suppose that $\bar{f}(t)$ has a non-multiple root $\bar{a}$ in $\bar{K}$. Then $f(t)$ has one and only one root a in K which is a representative of $\bar{a}$.*

Proof. Since $\bar{a}$ is a non-multiple root of $\bar{f}(t)$, we have $\bar{f}(t) = (t - \bar{a})\bar{f}_1(t)$ where $\bar{f}_1(t)$ is a polynomial in $\bar{K}[t]$ such that $\bar{f}_1(\bar{a}) \neq 0$, i.e., $t - \bar{a}$ and $\bar{f}_1(t)$ are relatively prime. Hence we can choose suitable representative polynomials $t - a$ and $f_1(t)$ of $t - \bar{a}$ and $\bar{f}_1(t)$ respectively such that $f(t) = (t - a)f_1(t)$. The element a is then a root of $f(t)$ in K which is a representative of $\bar{a}$.

[22] Azumaya [3].

Suppose that a_1 is a second such root of $f(t)$. Then $(a_1 - a)f_1(a_1) = 0$ and $f_1(a_1)$ is, since $\bar{f}_1(\bar{a}_1) \neq 0$, a regular element of K, and therefore a_1 must be equal to a. This shows the uniqueness of a.

LEMMA 5. *Let Z be a completely primary unramified and regular extension ring of K such that its residue class field $\bar{Z} = Z/\mathfrak{p}Z$ is separable over $\bar{K}$ and let L be a completely primary finite extension ring of K whose residue class field $\bar{L}$ is $\bar{K}$-isomorphic to $\bar{Z}$. Then for any $\bar{K}$-isomorphism of $\bar{Z}$ onto $\bar{L}$ there exists one and only one K-homomorphism of Z into L which induces modulo $\mathfrak{p}Z$ the given isomorphism on $\bar{Z}$; this homomorphism is an onto-mapping if and only if L is unramified over K, and moreover this is an (onto-)isomorphism if and only if L is regular with respect to K.*

Proof. Since $\bar{Z}$ is finite and separable over $\bar{K}$, there exists an element $\bar{a}$ in $\bar{Z}$ such that $\bar{Z} = \bar{K}[\bar{a}]$. Then $\bar{a}$ is a root of an irreducible polynomial $\bar{f}(t)$ in $\bar{K}[t]$ with highest coefficient 1 and of degree n, where n is the degree of $\bar{Z}$ over $\bar{K}$. Let $f(t)$ be a representative polynomial of $\bar{f}(t)$ in $K[t]$ also with highest coefficient 1 and of degree n. Then, since $\bar{a}$ is a non-multiple root of $\bar{f}(t)$, $f(t)$ has by Lemma 4 one and only one root a in Z which is a representative of $\bar{a}$. Since Z is unramified over K and since $1, \bar{a}, \bar{a}^2, \ldots \bar{a}^{n-1}$ form a basis of $\bar{Z}$ over $\bar{K}$ it follows from Corollary to Theorem 5 that $1, a, a^2, \ldots a^{n-1}$ form a basis of Z over K; further since Z is regular with respect K and $1, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{n-1}$ are linearly independent with respect to $\bar{K}$ it follows again from Corollary to Theorem 5 that $1, a, a^2, \ldots, a^{n-1}$ form in fact a linearly independent basis of Z over K.

Now let $\bar{a}_0$ be the image of $\bar{a}$ by the given $\bar{K}$-isomorphism of $\bar{Z}$ onto $\bar{L}$. Then $\bar{L} = \bar{K}[\bar{a}_0]$ and $\bar{a}_0$ is also a root of $\bar{f}(t)$. Hence it can be seen similarly as just above that $f(t)$ has one and only one root a_0 in L which is a representative of $\bar{a}_0$. Therefore if we associate with a the conjugate a_0 we obtain a K-homomorphism of Z into L which induces the given isomorphism $(\bar{a} \to \bar{a}_0)$ on $\bar{Z}$. On the other hand, any K-homomorphism of Z into L inducing on $\bar{Z}$ the isomorphism $(\bar{a} \to \bar{a}_0)$ maps a on a root of $f(t)$ in L which is a representative of $\bar{a}_0$, and this must coincide with $\bar{a}_0$ because of its uniqueness, i.e., this homomorphism is the homomorphism $(a \to a_0)$ defined above.

Now let the K-homomorphism $(a \to a_0)$ be an onto-mapping (i.e. $L \simeq K[a_0]$). Then L is evidently unramified over K. Suppose conversely that L is unramified over K. Then, since $1, \bar{a}_0, \bar{a}_0^2, \ldots, \bar{a}_0^{n-1}$ form a basis of $\bar{L}$ over $\bar{K}$, it follows from Corollary to Theorem 5 that $1, a_0, a_0^2, \ldots, a_0^{n-1}$ form a basis of L over K, and the K-homomorphism $(a \to a_0)$ is an onto-mapping. The last assertion is also clear, if we observe that the regularity of (the unramified extension)

L/K means the linear independency of $1, a_0, a_0^2, \ldots, a_0^{n-1}$.

THEOREM 28. *For any given finite separable extension field $\bar{Z}$ of $\bar{K}$ there exists one and—up-to-K-isomorphisms—only one completely primary unramified and regular extension ring Z of K whose residue class field is $\bar{Z}$.*

Proof. Let $\bar{a}$ be the element of $\bar{Z}$ such that $\bar{Z} = \bar{K}[\bar{a}]$ and let $\bar{f}(t)$ and $f(t)$ have the same significances as in the proof of Lemma 5. Then the residue class ring $Z = K[t]/(f(t))$ is a required extension ring of K, as one can readily see. The uniqueness of Z/K is an immediate consequence of Lemma 5.

THEOREM 29.[23] *Let L be a completely primary finite extension ring of K such that its residue class field $\bar{L}$ is separable over $\bar{K}$. Then there exists one and only one inertial ring*[24] *of L/K.*

Proof. Let Z be a completely primary unramified and regular extension ring of K whose residue class field is $\bar{L}$ (Theorem 28). There exists by Lemma 5 one and only one K-homomorphism of Z into L which leaves every residue class modulo $\mathfrak{p}Z$. Then the homomorphic image of Z by the homomorphism is unramified over K by virtue of Lemma 5, and is the inertial ring of L/K; that this is the only inertial ring follows also from Lemma 5.

Let us now call a completely primary finite extension ring Z of K a *Galois extension ring* of K if it is regular and unramified over K and moreover its residue class field $\bar{Z}$ is a (separable) Galois extension of $\bar{K}$. Let then G be the Galois group of $\bar{Z}/\bar{K}$. Then for every $\sigma \in G$ there exists by virtue of Lemma 5 one and only one K-automorphism of Z which induces σ on $\bar{Z}$; this automorphism we may and shall denote also by σ. The totality of those σ's exhausts all K-automorphisms of Z and so it forms a group isomorphic to G; we shall call it the *Galois group* of Z/K and shall denote it also by G.

Once the notion of Galois extensions is defined we can now introduce the notion of *crossed products* similarly as in the case of ordinary algebras. Namely, let Z be a Galois extension ring of K with Galois group G and suppose that there is associated with each pair (σ, τ) of elements of G a regular element $a_{\sigma,\tau}$ of Z such that

$$a_{\rho,\sigma\tau}a_{\sigma,\tau} = a_{\rho\sigma,\tau}a_{\rho,\sigma}^{\tau},$$

for every ρ, σ and τ in G; such a system $\{a_{\sigma,\tau}\}$ we shall call a *factor set* of Z/K. Then we define a crossed product $(Z/K, a_{\sigma,\tau})$ of Z/K (with respect to the factor set $\{a_{\sigma,\tau}\}$) as follows:

---

[23] Cf. Chevalley [6], III, Proposition 3.

[24] =inertial algebra.

$$(Z/K,\ a_{\sigma,\tau}) = \sum_{\sigma\in G} u_\sigma Z\ ;$$
$$zu_\sigma = u_\sigma z^\sigma\ (z\in Z),\quad u_\sigma u_\tau = u_{\sigma\tau}a_{\sigma,\tau},$$

where $\{u_\sigma\ ;\ \sigma\in G\}$ are linearly independent with respect to Z. Then it is ready to see that $(Z/K,\ a_{\sigma,\tau})$ is a regular algebra over K with unit element $u_1a_{1,1}^{-1}$, Z is looked upon as its subring in a natural manner and every u_σ is a regular element. Taking the factor set $\{a_{\sigma,\tau}\}$ modulo $\mathfrak{p}Z$, we obtain a (ordinary) factor set $\{\bar{a}_{\sigma,\tau}\}$ of the residue class field $\bar{Z} = Z/\mathfrak{p}Z$, and the corresponding crossed product $(\bar{Z}/\bar{K}, \bar{a}_{\sigma,\tau})$ of the Galois extension field $\bar{Z}/\bar{K}$ is a normal, simple algebra over $\bar{K}$. Furthermore, $(\bar{Z}/\bar{K}, \bar{a}_{\sigma,\tau})$ is the residue class algebra of $(Z/K, a_{\sigma,\tau})$ modulo its two-sided ideal $\mathfrak{p}(Z/K, a_{\sigma,\tau})$, and we have from Theorem 15 the following

THEOREM 30. *Every crossed product $(Z/K, a_{\sigma,\tau})$ of a Galois extension ring Z/K is proper maximally central over K and has $(\bar{Z}/\bar{K}, \bar{a}_{\sigma,\tau})$ as its simple residue class algebra.*

A Galois extension ring Z is called *cyclic* over K if its Galois group is cyclic. For a cyclic extension ring Z/K with rank n and with generating automorphism σ and for a regular element α of K we can also construct a *cyclic crossed product* $(Z/K, \sigma, \alpha) = Z + uZ + u^2Z + \ldots + u^{n-1}Z$ by the relations $zu = uz^\sigma$ $(z\in Z)$ and $u^n = \alpha$. Then $(Z/K, \sigma, \alpha)$ is a proper maximally central algebra over K whose simple residue class algebra is the cyclic crossed product $(\bar{Z}/\bar{K}, \sigma, \bar{\alpha})$ of $\bar{Z}/\bar{K}$, where $\bar{\alpha}(\neq 0)$ is the residue class of α modulo $\mathfrak{p}$.

Let A be a proper maximally central algebra over K and let $\bar{A} = A/\mathfrak{p}A$ be its simple residue class algebra. Then A and $\bar{A}$ determine respectively an algebra class $\{A\}$ over K and an (ordinary) algebra class $\{\bar{A}\}$ over $\bar{K}$. Suppose that B is a second proper maximally central algebra over K with simple residue class algebra $\bar{B} = B/\mathfrak{p}B$. Then it is clear that if $A\sim B$ then we have $\bar{A}\sim\bar{B}$, while it can also readily be seen that $\bar{A}\times\bar{B}$ is the simple residue class algebra of the proper maximally central algebra $A\times B$: $\bar{A}\times\bar{B} = (A\times B)/\mathfrak{p}(A\times B)$. These show that by means of $\{A\}\to\{\bar{A}\}$ the algebra class group over K is mapped homomorphically into the algebra class group over $\bar{K}$. But this homomorphism is in fact an isomorphism. For, if $\bar{A}\sim\bar{K}$ i.e. if there exists a system of matrix units $\{\bar{e}_{ij}\}$ in $\bar{A}$ such that $\bar{A} = \sum\bar{K}\bar{e}_{ij}$, then we can find by Theorem 25 a system of matrix units $\{e_{ij}\}$ in A such that each e_{ij} is a representative of $\bar{e}_{ij}$, since A is unramified over K, it follows from Theorem 6 that $A = \sum Ke_{ij}$ i.e. $A\sim K$. Now we shall moreover show that this isomorphism is an onto-mapping. The proof is virtually the same as that of Nakayama [12], Satz 1, but we give it here for completeness. Let $\{\bar{A}\}$ be a given algebra class over $\bar{K}$ with exponent e. First, suppose that e is not divisible by the

characteristic of $\overline{K}$. Then there exists a (finite and separable) Galois extension field $\overline{Z}$ of $\overline{K}$, such that $\overline{A}$ is similar to a crossed product $(\overline{Z}/\overline{K}, \bar{a}_{\sigma,\tau})$ of $\overline{Z}/\overline{K}$ with factor set $\{\bar{a}_{\sigma,\tau}\}$ consisting of e-th roots of unity only.[25] Let Z be a Galois extensions ring of K whose residue class field is $\overline{Z}$ (Theorem 28). Since every e-th root of unity in $\overline{Z}$ is a non-multiple root of the polynomial $x^e - 1$, there exists by Lemma 4 one and only one representative $a_{\sigma,\tau}$ of $\bar{a}_{\sigma,\tau}$ which is an e-th root of unity in Z, for every σ, τ. Then $\{a_{\sigma,\tau}\}$ forms a factor set of Z/K, as can readily be seen, and the crossed product $(Z/K, a_{\sigma,\tau})$ determines, by virtue of Theorem 30, the required algebra class over K corresponbing to the given class $\{\overline{A}\}$. Next, assume that e is a power of the (prime) characteristic of $\overline{K}$. Then there exists a cyclic extension field $\overline{Z}$ of $\overline{K}$ such that $\overline{A}$ is similar to a cyclic crossed product $(\overline{Z}/\overline{K}, \sigma, \bar{\alpha})$ of $\overline{Z}/\overline{K}$ with generating automorphism σ of $\overline{Z}/\overline{K}$ and with non-zero element $\bar{\alpha}$ of $\overline{K}$.[26] Let Z be a cyclic extension ring of K whose residue class field is $\overline{Z}$ and let α be an arbitrary representative of $\bar{\alpha}$ in K. Then the cyclic crossed product $(Z/K, \sigma, \alpha)$ determines also the required algebra class over K. Observing that every algebra class over $\overline{K}$ is expressible as a product of two types of algebra classes mentioned above, we complete the proof of

THEOREM 31. *By associating with every algebra class $\{A\}$ the algebra class $\{\overline{A}\}$, where A is a proper maximally central algebra over K and $\overline{A} = A/\mathfrak{p}A$ its simple residue class algebra, the algebra class group over K is mapped isomorphically upon the algebra class group over $\overline{K}$.*

Let A be a proper maximally central algebra over K. Then, since A is primary, A is according to Theorem 26 a full matrix ring over a completely primary algebra A_0 over K, and A_0 is also proper maximally central. Suppose that A_1 is a second completely primary proper maximally central algebra over K which is similar (to A whence) to A_0, i.e., there exist natural numbers r and s such that $(A_0)_r \cong (A_1)_s$ then it follows again from (the second half of) Theorem 26 that $A_0 \cong A_1$. Thus we have that *every algebra class over K contains one and only one completely primary algebra A_0 and consists of all full matrix rings over A_0.* From this and from the preceding theorem we can readily obtain

THEOREM 32. *For any given normal simple algebra $\overline{A}$ over $\overline{K}$ there exists one and—up-to-K-isomorphisms—only one proper maximally central algebra A over K such that $\overline{A}$ is the residue class algebra of A modulo $\mathfrak{p}A$: $\overline{A} = A/\mathfrak{p}A$.*

---

[25] Deuring [8], V, § 7, Satz 1.

[26] Albert [1], VII, Theorem 31.

7. Existence of inertial algebras

After above preparations we can now prove an existence theorem of inertial algebras, which is a main purpose of the present paper. In this section we assume also that K is a Hensel ring with maximal ideal $\mathfrak{p}$ and with residue class field $\overline{K} = K/\mathfrak{p}$. First, we treat the following special case:

LEMMA 6. *Let R be a faithful primary algebra over K with unit element such that the simple residue class algebra $\overline{R} = R/N$ modulo its radical N is normal over K. Then there exists a proper maximally central inertial algebra A of R which is uniquely determined up to inner automorphisms of R generated by elements of N.*

Proof. Let $\overline{R}'$ be a normal simple algebra over $\overline{K}$ inverse-isomorphic to $\overline{R}$. Then there exists by virtue of Theorem 32 a proper maximally central algebra A' over K whose simple residue class algebra is $\overline{R}'$. Construct then the direct product $R \times A'$ over K; R and A' being contained in it as element-wise commutative subalgebras. Then evidently the direct product $\overline{R} \times \overline{R}'$ (over $\overline{K}$) is the residue class algebra $R \times A'/N \times A'$. Since $\overline{R} \times \overline{R}'$ is a full matrix algebra $(\overline{K})_m$ of degree $m = [\overline{R}: \overline{K}]$ over $\overline{K}$ and since $N \times A'$ is a quasi-regular (two-sided) ideal of $R \times A'$, it follows from Theorem 25 that $R \times A'$ contains a full matrix algebra $(K)_m$ of degree m over K. Since $m = [A': K]$, $(K)_m$ is a direct product of two element-wise commutative proper maximally central subalgebras A_1 and A_1' which are inverse-isomorphic and isomorphic to A' respectively.

Now the (K-)isomorphism of A_1' onto A' can, according to Theorem 18, be extended to an (inner) automorphism of $R \times A'$, and under this automorphism A_1 is carried isomorphically onto a proper maximally central subalgebra A of $R \times A'$ which is element-wise commutative with A'. But since R is the commuter ring of A' in $R \times A'$ by Corollary to Theorem 16, A is contained in R and A is a required inertial algebra of R.

Now suppose that A^* is a second proper maximally central inertial algebra of R. Then there exists, by Theorem 32, a K-isomorphism of A onto A^*, and the isomorphism can, again by Theorem 18, be extended to an inner automorphism $x \to u^{-1}xu$ of R: $u^{-1}Au = A^*$. Since A^* is an inertial algebra of R there exists a (regular) element v in A^* such that $u \equiv v \pmod{N}$. It follows then that $uv^{-1} \equiv 1 \pmod{N}$ and $(uv^{-1})^{-1}Auv^{-1} = vu^{-1}Avu^{-1} = vA^*v^{-1} = A^*$, and this completes our proof.

Now we proceed to the following general existence theorem:

THEOREM 33. (*Generalized Wedderburn-Malcev's theorem.*) *Let R be an alge-*

bra over (a Hensel ring) K such that the semi-simple residue class algebra $\bar{R} = R/N$ modulo its radical N is separable over $\bar{K}(= K/\mathfrak{p})$. Then there exists a maximally central inertial algebra of R, and such an inertial algebra is uniquely determined up to inner automorphisms of R generated by elements of N.

Proof. a) First, we prove the theorem in the case where R is a faithful completely primary algebra over K (with unit element). Then the residue class algebra $\bar{R} = R/N$ is a division algebra. For every subalgebra S of R, the homomorphic image $\bar{S}$ by the natural homomorphism of R onto $\bar{R}$ is, being as a subalgebra of $\bar{R}$, a division algebra, so that the kernel $S \cap N$ is the radical of S because it is quasi-regular in S by Corollary to Theorem 9. Now let $\bar{Z}$ be the center of $\bar{R}$. Then $\bar{Z}$ is a finite and separable extension field of $\bar{K}$ by our asumption. Hence there exists an element $\bar{a}$ of $\bar{Z}$ such that $\bar{Z} = \bar{K}[\bar{a}]$. Take from R an arbitrary representative b of $\bar{a}$ and consider the subring $K[b]$ of R. Since $K[b]$ is a completely primary finite extension ring of K whose residue class field is $\bar{Z}$, $K[b]$ contains by Theorem 29 an inertial ring Z; Z is a completely primary finite and unramified extension ring of K which is mapped on $\bar{Z}$ by the natural homomorphism of R onto $\bar{R}$.

Now consider a finite and separable splitting field $\bar{\Omega}$ of $\bar{Z}/\bar{K}$ over $\bar{K}$. Then the direct product $\bar{Z} \times \bar{\Omega}$ is directly decomposable in the following manner:

$$\bar{Z} \times \bar{\Omega} = \bar{e}_1\bar{\Omega} \oplus \bar{e}_2\bar{\Omega} \oplus \cdots \oplus \bar{e}_n\bar{\Omega},$$

where $\bar{e}_1, \bar{e}_2, \ldots, \bar{e}_n$ are mutually orthogonal (primitive) idempotent elements of $\bar{Z} \times \bar{\Omega}$ whose sum is the unit element and $n = [Z : K] = [\bar{Z} : \bar{K}]$. Let Ω be a completely primary unramified and regular extension ring of K whose residue class field is $\bar{\Omega}$ (Theorem 28), and construct the direct product $Z \times \Omega$. Then $\bar{Z} \times \bar{\Omega}$ is the residue class algebra of $Z \times \Omega$ modulo $\mathfrak{p}(Z \times \Omega)$: $\bar{Z} \times \bar{\Omega} = Z \times \Omega/\mathfrak{p}(Z \times \Omega)$. Hence there exist by Theorem 24 mutually orthogonal idempotent elements $e_1, e_2, \ldots, e_n$ in $Z \times \Omega$ such that each e_i is a representative of $\bar{e}_i$, and we have by Corollary to Theorem 5 that

$$Z \times \Omega = e_1\Omega \oplus e_2\Omega \oplus \cdots \oplus e_n\Omega.$$

Construct furthermore the direct products $R \times \Omega$ (over K) and $\bar{R} \times \bar{\Omega}$ (over $\bar{K}$). Then $\bar{R} \times \bar{\Omega}$ is evidently the residue class algebra of $R \times \Omega$ modulo $N \times \Omega$; but since $N \times \Omega$ is quasi-regular (Theorem 10) and R is semi-simple $N \times \Omega$ is the radical of $R \times \Omega$. And it is also clear that the natural homomorphism of $R \times \Omega$ onto $\bar{R} \times \bar{\Omega}$ induces on R and $Z \times \Omega$ the sames onto $\bar{R}$ and $\bar{Z} \times \bar{\Omega}$ respectively.

Now let Q be the commuter ring of Z in R: $Q = V_R(Z)$. Then from the fact that every linearly independent basis of Ω over K is also the same of $R \times \Omega$ over R it follows that $Q \times \Omega$ is the commuter ring of (Z whence) $Z \times \Omega$

in $R \times \Omega$. On the other hand, the commuter ring of $Z \times \Omega$ in $R \times \Omega$ is evidently the commuter ring of $\{e_1, e_2, \ldots, e_n\}$ in $R \times \Omega$, and this is nothing but $e_1(R \times \Omega)e_1 \oplus e_2(R \times \Omega)e_2 \oplus \ldots \oplus e_n(R \times \Omega)e_n$, as can readily be verifed[27]: $Q \times \Omega = e_1(R \times \Omega)e_1 \oplus e_2(R \times \Omega)e_2 \oplus \ldots \oplus e_n(R \times \Omega)e_n$. From this it follows that Q is an algebra over K; because $e_1(R \times \Omega)e_1 \oplus e_2(R \times \Omega)e_2 \oplus \ldots \oplus e_n(R \times \Omega)e_n$ is an algebra over K and $Q \times \Omega$ is K-isomorphic to the $[\Omega : K]$-times direct sum of Q. Furthermore, denoting by $\bar{Q}$ the image of Q by the natural homomorphism of R onto $\bar{R}$ it follows that $\bar{Q} \times \bar{\Omega} = \bar{e}_1(\bar{R} \times \bar{\Omega})\bar{e}_1 \oplus \bar{e}_2(\bar{R} \times \bar{\Omega})\bar{e}_2 \oplus \ldots \oplus \bar{e}_n(\bar{R} \times \bar{\Omega})\bar{e}_n$. But since every $\bar{e}_i$ lies in the center $\bar{Z} \times \bar{\Omega}$ of $\bar{R} \times \bar{\Omega}$, we have that $\bar{Q} \times \bar{\Omega} (= \bar{e}_1(\bar{R} \times \bar{\Omega}) \oplus \bar{e}_2(\bar{R} \times \bar{\Omega}) \oplus \ldots \oplus \bar{e}_n(\bar{R} \times \bar{\Omega})) = \bar{R} \times \bar{\Omega}$, whence $\bar{Q} = \bar{R}$. Since Q is the commuter ring of Z in R, Z is contained in the center of Q, and Q may be considered as a (faithful completely primary) algebra over Z. Hence, by applying Lemma 6 to $(R =)Q$ and $(K =)Z$, we can obtain a proper maximally central inertial algebra A of Q over Z: $A/\mathfrak{p}A (= \bar{Q}) = \bar{R}$. Since Z is unramified over K so is also A over K, and A is a desired inertial algebra of R.

Suppose that A^* is a second maximally central inertial algebra of R with center Z^*. Then Z^* is unramified over K, by virtue of Theorem 13, and is mapped on the center $\bar{Z}$ of $\bar{R}$ by the natural homomorphism of R onto $\bar{R}$. Therefore, we can find, similarly as $Z \times \Omega$ above, mutually orthogonal idempotent elements $e_1^*, e_2^*, \ldots, e_n^*$ in $Z^* \times \Omega$ such that each e_i^* is a representative of $\bar{e}_i$ and the following direct decomposition holds:

$$Z^* \times \Omega = e_1^*\Omega \oplus e_2^*\Omega \oplus \ldots \oplus e_n^*\Omega.$$

Since $e_i \equiv e_i^* \pmod{N \times \Omega}$ for every i, there exists by Theorem 3 a (quasi-regular) element c in $N \times \Omega$ such that $e_i^c = e_i^*$ for every i. Since Ω is contained in the center of $R \times \Omega$ $\omega^c = \omega$ for every $\omega \in \Omega$, and therefore we have $Z^c \times \Omega = (Z \times \Omega)^c = Z^* \times \Omega$. Now let $\bar{a}$ be an element of $\bar{Z}$ such that $\bar{Z} = \bar{K}[\bar{a}]$, as above. Then $\bar{a}$ is a non-multiple root of an irreducible polynomial $\bar{f}(t)$ in $\bar{K}[t]$ with highest coefficient 1. Let $f(t)$ be a representative polynomial of $\bar{f}(t)$ in $K[t]$ with highest coefficient 1. Then, by applying Lemma 4 to Z, we can find, as in the proof of Lemma 5, a root a of $f(t)$ in Z which is a representative of $\bar{a}$, so that we have $Z = K[a]$. Similarly, there is obtained a root a^* of $f(t)$ in Z^* which is a representative of $\bar{a}$ and such that $Z^* = K[a^*]$. And we have $f(t) = (t - a^*)f_1^*(t)$ with a polynomial $f_1^*(t)$ in $Z^*[t]$; necessarily $f_1^*(a^*) \not\equiv 0$

[27] Generally, if $e_1, e_2, \ldots, e_n$ are mutually orthogonal idempotent elements in a ring R then their commuter ring in R is $e_1Re_1 \oplus e_2Re_2 \oplus \ldots \oplus e_nRe_n \oplus t(e_1 + e_2 + \ldots + e_n)$, where $t(e_1 + e_2 \ldots + e_n)$ is the two-sided annihilator of $e_1 + e_2 + \ldots + e_n$ in R.

modulo the maximal ideal $\mathfrak{p}Z^*$ of Z^*, i.e., $f_1^*(a^*)$ is a regular element of Z^*. Consider now the element a^c. Since c is in the radical $N \times \Omega$ of $R \times \Omega$ it follows that $a^c \equiv a \pmod{N \times \Omega}$ whence $a^c \equiv a^* \pmod{N \times \Omega}$. Observing that a^c is in the commutative ring $(Z^c \times \Omega =)\ Z^* \times \Omega$, we have then $f_1^*(a^c) \equiv f_1^*(a^*) \pmod{N \times \Omega}$ whence $f_1^*(a^c)$ is also a regular element; on the other hand, a^c is evidently a root of $f(t)$, and we have $(a^c - a^*)f_1^*(a^*) = 0$, which implies that $a^c = a^*$ (because of the regularity of $f_1^*(a^c)$). Thus we have proved that $Z^c(= K[a^c]) = Z^*$ and the inner automorphism $x \to x^c(= (1-c)^{-1}x(1-c))$ of $R \times \Omega$ induces on $Z(\subseteq R)$ an isomorphism $z \to z^*$ onto $Z^*(\subseteq R)$. Further, since the commuter ring $Q = V_R(Z)$ of Z in R is an algebra over K, as was shown above, Q is necessarily of the type (S), and it follows from Theorem 11 that the isomorphism $z \to z^*$ can be extended to an inner automorphism $x \to v^{-1}xv$ of R with regular element v of R. Since A^* is an inertial algebra of R, there exists an element w in A^* such that $w \equiv v \pmod{N}$, so that w is also regular and $vw^{-1} \equiv 1 \pmod{N}$. Put now $d = 1 - vw^{-1}$. Then d is in N and we have $z^d = wv^{-1}zvw^{-1} = wz^*w^{-1} = z^*$ for every $z \in Z$. Consider then the (maximally central) subalgebra A^d. Since the inner automorphism $x \to x^t$ of R leaves invariant every residue class of R modulo N, A^d is, with A, also an inertial algebra of R, and in fact, since $Z^t = Z^*$ is its center, it is, with A^*, a (proper maximally central) inertial algebra of the commuter algebra Q^t of Z^* in R. Hence we can find, by applying Lemma 6 to $(R =)Q^t$ and $(K =)Z^*$, an element d_1 of N such that $(A^d)^{d_1} = A^*$. Putting then $d_2 = d + d_1 - dd_1$, d_2 is a desired element of N: $A^{d_2}(= (A^d)^{d_1}) = A^*$.

b) Next, assume that R is a primary algebra (with unit element). Then R is a full matrix ring over a completely primary subalgebra R_0, i.e., there exists a system of matix units $\{e_{ij}\}$ such that $R = \sum e_{ij}R_0$ and R_0 is the commuter ring of $\{e_{ij}\}$ in R. If we denote by N_0 the radical of R_0 it follows $N = \sum e_{ij}N_0$, and $\overline{R} = R/N$ is a full matrix ring over $\overline{R}_0 = R_0/N_0$: $\overline{R} = \sum \overline{e}_{ij}\overline{R}_0$. The center of $\overline{R}_0$ conicides therefore with that of $\overline{R}$, and so is separable over $\overline{K}$. Hence there exists, as was showm in a) above, a maximally central inertial algebra A_0 of R_0. Then $A = \sum e_{ij}A_0$ is evidently a maximally central inertial algebra of R.

Now suppose that A^* is a second maximally central inertial algebra of R. Then we can find, by Theorem 25, a system of matrix units $\{e_{ij}^*\}$ in A^* such that $e_{ij}^* \equiv e_{ij} \pmod{N}$ for every i, j, so that there exists by Theorem 3 an element c in N such that $e_{ij}^c = e_{ij}^*$ for every i, j. Therefore it follows that R_0^c is the commuter ring of $\{e_{ij}^*\}$ in R and the commuter ring A_0^* of $\{e_{ij}^*\}$ in A^* is a maximally central inertial algebra of R; on the other hand, A_0^c is, since

c is in N, also a maximally central inertial algebra of R_0^c. Hence there exists, from a) above, an element c_0 in the radical N_0^c of R_0^c such that $(A_0^c)^{c_0} = A_0^*$. Putting $d = c + c_0 - cc_0 (\in N)$ and observing that c_0 commutes with every e_{ij}^*, we have $A^d = (A^c)^{c_0} = (\sum e_{ij}^* A_0^c)^{c_0} = \sum e_{ij}^* (A_0^c)^{c_0} = \sum e_{ij}^* A_0^* = A^*$.

c) Finally, we turn to the case of general algebra R. Let $\overline{R} = \overline{R}_1 \oplus \overline{R}_2 \ldots \oplus \overline{R}_k$ be the (unique) direct decomposition of the semi-simple algebra $\overline{R} = R/N$ into mutually orthogonal simple subalgebras. Then we can find, as in the last part of § 5, mutually orthogonal idempotent elements $E_1, E_2, \ldots, E_k$ in R such that each E_κ is a representative of the unit element of $\overline{R}_\kappa$, and each subalgebra $E_\kappa R E_\kappa$ is a primary algebra with radical $E_\kappa N E_\kappa$ and with simple residue class algebra $\overline{R}_\kappa (= E_\kappa R E_\kappa / E_\kappa N E_\kappa)$. Since the center of $\overline{R}_\kappa$ is separable over $\overline{K}$ by assumption, there exists, from b) above, a maximally central inertial algebra A_κ of $E_\kappa R E_\kappa$, for each κ. Then the direct sum $A = A_1 \oplus A_2 \oplus \ldots \oplus A_k$ is a desired inertial algebra of R.

Now let A^* be a second maximally central inertial algebra of R. Then A^* is (by definition) a direct sum of mutually orthogonal subalgebras $A_1^*, A_2^*, \ldots, A_l^*$ such that each A_κ^* is proper maximally central over its center. Hence, denoting by $\overline{A}_\kappa^*$ the simple residue class algebra of A_κ^* (modulo its radical $\mathfrak{p}A_\kappa^*$), $\overline{R}$ is a direct sum of $\overline{A}_1^*, \overline{A}_2^*, \ldots, \overline{A}_l^*$. It follows therefore that $l = k$ and we may assume that $\overline{A}_\kappa^* = \overline{R}_\kappa$ for every κ. Denote by E_κ^* the unit element of A_κ^*. Then $E_1^*, E_2^*, \ldots, E_k^*$ are mutually orthogonal idempotent elements of the center of A^* such that $E_\kappa^* \equiv E_\kappa \pmod{N}$ for every κ, and there exists by Theorem 3 an element c in N such that $E_\kappa^c = E_\kappa^*$ for every κ. Since A_κ is a maximally central inertial algebra of $E_\kappa R E_\kappa$, A_κ^c is also a maximally central inertial algebra of $((E_\kappa R E_\kappa)^c =) E_\kappa^* R E_\kappa^*$. On the other hand, $A_\kappa^* (= E_\kappa^* A^* E_\kappa^*)$ is evidently a maximally central inertial algebra of $E_\kappa^* R E_\kappa^*$. Hence we can find, by applying b) to the primary algebra $E_\kappa^* R E_\kappa^*$, an element c_κ in the radical $E_\kappa^* N E_\kappa^*$ of $E_\kappa^* R E_\kappa^*$ such that $(A_\kappa^c)^{c_\kappa} = A_\kappa^*$. This is the case for every κ, and if we put $d = c + \sum c_\kappa - c \sum c_\kappa$, d is an element of N and we have $A^d = \sum A_\kappa^d = \sum (A_\kappa^c)^{c_\kappa} = \sum A_\kappa^* = A^*$. This completes the proof.

COROLLARY. *Every unramified algebra A over (a Hensel ring) K is maximally central whenever its semi-simple residue class algebra $\overline{A} = A/\mathfrak{p}A$ modulo the radical $\mathfrak{p}A$ is separable over $\overline{K}$.*

BIBLIOGRAPHY

[1] A. A. Albert, Structure of Algebras, New York (1939).

[2] E. Artin, C. J. Nesbitt and R. M. Thrall, Rings with minimum condition, Michigan Press (1944).

[3] G. Azumaya, On generalized semi-primary rings and Krull-Remak-Schmidt's theorem, Jap. Journ. Math. **19** (1948).

[4] G. Azumaya, Galois theory for uni-serial rings, Journ. Math. Soc. Jap. **1** (1949).

[5] G. Azumaya and T. Nakayama, On absolutely uni-serial algebras, Jap. Journ. Math. **19** (1948).

[6] C. Chevalley, On the theory of local rings, Ann. Math. **44** (1943).

[7] I. S. Cohen, On the structure and ideal theory of complete local rings, Trans. Amer. Math. Soc. **59**, (1946).

[8] M. Deuring, Algebren, Ergeb. Math. **4** (1935).

[9] N. Jacobson, The radical and semi-simplicity for arbitrary rings, Amer. Journ. Math. **67** (1945).

[10] A. Malcev, On the representation of an algebra as a direct sum of the radical and a semi-simple algebra, C. R. URSS. **36** (1942).

[11] M. Nagata, On the structure of complete local rings, Nagoya Math. Journ. **1** (1950).

[12] T. Nakayama, Divisionsalgebren über diskret bewerteten perfekten Körpern, Journ. rein. angew. Math. **178** (1937).

[13] E. Witt, Schiefkörper über diskret bewerteten Körpern, Journ. rein. angew. Math. **176** (1936).

Mathematical Institute,
Nagoya University