On the Structure of Brauer Group of a Discretely-valued Complete Field

By Ichirô SATAKE

Institute of Mathematics, College of General Education, University of Tokyo

(Received July 7, 1951)

Let k be a field which is complete with respect to a discrete valuation and its residue class field $\mathfrak{k}$ be perfect. E. Witt proved[1] that any central division algebra D over k is similar to the direct product of an unramified central division algebra D_0 and a cyclic division algebra (π, Z, S), where Z is unramified over k and π is a prime element in k, and that this decomposition is unique if we take a fixed prime element π. This result has been generalized by T. Nakayama[2] to the case where the residue class field $\mathfrak{k}$ is not necessarily perfect, under the condition that the residue class algebra $\mathfrak{D}$ of D is separable over $\mathfrak{k}$. In this case, all algebra classes of such central division algebras D form a subgroup ${}^s\mathbf{B}$ of the Brauer group $B(k)$ of k, which coincides with $B(k)$ in case $\mathfrak{k}$ is perfect. The structure of ${}^s\mathbf{B}$ is then easily determined. Namely, ${}^s\mathbf{B}$ is the direct product of two subgroups $\mathbf{B}_0$ and $\mathbf{B}_\pi$, the former is isomorphic to the Brauer group $B(\mathfrak{k})$ of $\mathfrak{k}$ and the latter is dual to the Galois group $G(\mathfrak{k}^a/\mathfrak{k})$ of the maximal abelian extension $\mathfrak{k}^a$ of $\mathfrak{k}$. In the following note, we shall give a direct method to define the character-formula expressing this duality between $\mathbf{B}_\pi$ and $G(\mathfrak{k}^a/\mathfrak{k})$ and then reproduce the result mentioned above.

1. Let k be a field which is complete with respect to a discrete (exponential) valuation ν, and $\mathfrak{o}$, $\mathfrak{p}$, $\mathfrak{k}$ be its valuation ring, prime ideal and residue class field, respectively.[3] $\mathfrak{p}$ is a principal ideal $\pi\mathfrak{o}$, π being an arbitrary prime element. Let $\bar{k}$ be an algebraic closure of k. Then the valuation ν can be uniquely extended to a valuation $\bar{\nu}$ of $\bar{k}$, which is also non-archimedean but no longer discrete, nor $\bar{k}$ complete with respect to $\bar{\nu}$. The valuation ring and the prime ideal of $\bar{\nu}$ being denoted by $\bar{\mathfrak{o}}$ and $\bar{\mathfrak{p}}$, the residue class field $\bar{\mathfrak{o}}/\bar{\mathfrak{p}}$ is obviously an

---

1) E. Witt, Schiefkörper über diskret bewerteten Körpern, Crelles J., 176 (1937).

2) T. Nakayama, Divisionsalgebren über diskret bewerteten perfekten Körpern, Crelles J., 178 (1937).

3) For the fundamental notions such as field-extension, valuation, normal simple algebra etc, see van der Waerden, *Moderne Algebra*, 2nd ed., Berlin, v. 1 (1937), v. 2 (1940).

algebraic closure $\bar{\mathfrak{k}}$ of $\mathfrak{k}$. In general, the residue class field of an extension K of k contained in $\bar{k}$ can be identified with a certain extension $\mathfrak{K}$ of $\mathfrak{k}$ contained in $\bar{\mathfrak{k}}$. We shall express this correspondence by the symbol $K \to \mathfrak{K}$. Any algebraic extension K ($\mathfrak{K}$) of k ($\mathfrak{k}$) which we consider in the following is supposed to be contained in $\bar{k}$ ($\bar{\mathfrak{k}}$), whenever the contrary is not explicitly mentioned.

Now let $\mathfrak{K}$ be a separable extension of $\mathfrak{k}$. We shall assert that there exists uniquely a separable unramified extension K of k such that $K \to \mathfrak{K}$. (In this case, we shall denote as $K \longleftrightarrow \mathfrak{K}$.) Suppose first that $[\mathfrak{K}:\mathfrak{k}]=n$ be finite. Then we can find $w_1 \in \bar{\mathfrak{o}}$ such that $\mathfrak{K}=\mathfrak{k}(\bar{w}_1)$, $\bar{w}_1$ denoting the residue class of w_1 mod $\bar{\mathfrak{p}}$, and a polynomial $f(x)$ of degree n with coefficients in $\mathfrak{o}$ such that $f(w_1)\equiv 0$ mod $\bar{\mathfrak{p}}$. $f(x)$ is separable and irreducible in k since it is so mod $\mathfrak{p}$. Applying Hensel's lemma to $f(x)$ in $k(w_1)$, we have w in $k(w_1)$ such that $f(w)=0$ and $w \equiv w_1$ mod $\bar{\mathfrak{p}}$. Then $K=k(w)$ is a separable extension of degree n of k. As the residue class field of K contains $\mathfrak{K}$, it follows that K is unramified over k and $K \to \mathfrak{K}$. If K' be another field such that K' is unramified over k and that $K' \to \mathfrak{K}$, then by Hensel's lemma applied in K' we should have $f(w')=0$ and $w \equiv w'$ mod $\bar{\mathfrak{p}}$ with a suitable w' in K'. But since $f(x)$ is separable mod $\bar{\mathfrak{p}}$, we have $w=w'$ and thus $K=k(w)=k(w')=K'$. From the argument used above, we also see that if the residue class field of K_1 contains $\mathfrak{K}$, the field K corresponding to $\mathfrak{K}$ is contained in K_1. In the general case where $[\mathfrak{K}:\mathfrak{k}]$ is infinite, $\mathfrak{K}$ is a union of an increasing series of finite separable extensions $\mathfrak{K}_i$ of $\mathfrak{k}: \mathfrak{K}_1 \subseteq \mathfrak{K}_2 \subseteq \cdots$, $\mathfrak{K}=\bigcup_{i=1}^{\infty} \mathfrak{K}_i$. Let K_i be the fields such that $K_i \longleftrightarrow \mathfrak{K}_i$. Then by the above remark we have $K_1 \subseteq K_2 \subseteq \cdots$. If we put $K=\bigcup_{i=1}^{\infty} K_i$, it is clear that K is separable unramified over k and that $K \to \mathfrak{K}$. Let K' be another field satisfying the same conditions. w' being any element of K', we have $k(w') \longleftrightarrow \mathfrak{k}(\bar{w}') \subseteq \mathfrak{K}$. Hence $k(w') \subseteq K$ and so $K' \subseteq K$. As we have also $K \subseteq K'$, it follows that $K=K'$, which proves our assertion.

We shall denote by k^s, k^a ($\mathfrak{k}^s$, $\mathfrak{k}^a$) the maximal separable and maximal abelian extension of k ($\mathfrak{k}$) contained in $\bar{k}$ ($\bar{\mathfrak{k}}$), respectively. We denote also by ${}^s k$ and ${}^a k$ the saparable unramified extension of k corresponding in the above sense to $\mathfrak{k}^s$ and $\mathfrak{k}^a$, respectively. Then it can be proved easily that ${}^s k$ is a Galois extension of k and that the Galois group $G({}^s k/k)$ is by the natural correspondence, isomorphic to the Galois group $G(\mathfrak{k}^s/\mathfrak{k})$.*) The lattice isomor-

---

*) We can define a homomorphism of $G(k^s/k)$ onto $G(\mathfrak{k}^s/\mathfrak{k})$ in a natural manner. ${}^s k$ is the subfield corresponding to the kernel of this homomorphism in the sense of Galois theory.

phism between the subextensions of ${}^sk/k$ and those of $\mathfrak{k}^s/\mathfrak{k}$, which we established above, is in accordance with the Galois theory. Namely, if $K \longleftrightarrow \mathfrak{K}$ in the above sense, the closed subgroups[4)] H of $G({}^sk/k)$ and $\mathfrak{H}$ of $G(\mathfrak{k}^s/\mathfrak{k})$ which correspond to K and $\mathfrak{K}$ respectively correspond by the isomorphism $G({}^sk/k) \cong G(\mathfrak{k}^s/\mathfrak{k})$. In particular, ${}^ak$ is the maximal abelian extension of k contained in ${}^sk: {}^ak = {}^sk \frown k^a$, and $G({}^ak/k) \cong G(\mathfrak{k}^a/\mathfrak{k})$.

2. We shall denote by $A, B, \cdots$ central simple algebras over k and especially by $D, \cdots$ central division algebras over k[5)]. Their classes of similarity form an abelian group with respect to direct product. This group is called *Brauer group* of k: we denote it by $\mathbf{B} = B(k)$.

Let D be of degree m. The valuation ν can be extenbed uniquely to a discrete valuation ν_D of D as follows[6)]

$$\nu_D(a) = \frac{1}{m} \nu(N_{D/k}(a)) \quad \text{for } a \in D,$$

$N_{D/k}$ denoting the principal norm. The unique maximal order of D and its unique two-sided prime ideal are given by

$$\mathfrak{o}_D = \{a;\ a \in D,\ \nu_D(a) \geqslant 0\},$$
$$\mathfrak{p}_D = \{a;\ a \in D,\ \nu_D(a) > 0\}.$$

Then $\mathfrak{p}_D$ is a principal ideal $\Pi \mathfrak{o}_D$, Π being a prime element in D of ν_D, and the residue class algebra $\mathfrak{D} = \mathfrak{o}_D/\mathfrak{p}_D$ is a division algebra over $\mathfrak{k}$, whose order we denote by f. If $\mathfrak{p} \cdot \mathfrak{o}_D = \mathfrak{p}_D^e$, we have $ef = m^2$ as in the commutative case. e is called the ramification exponent of D (or of its algebra class) and if $e=1$, D is called unramified. Since $e\nu_D(a)$ is the normalized valuation whenever ν is so, we have $e \mid m$ and thus $m \mid f$[*)].

Generally, A is considered as a matrix ring D_s of degree s over a suitable D. Then $\mathfrak{o}_A = (\mathfrak{o}_D)_s$ is a maximal order of A, with which every maximal orders are conjugate, and $\mathfrak{p}_A = (\mathfrak{p}_D)_s = \Pi \mathfrak{o}_A$ is the unique two-sided prime ideal in $\mathfrak{o}_A$. The residue class algebra $\mathfrak{A} = \mathfrak{o}_A/\mathfrak{p}_A$ is therefore considered as a matrix ring $\mathfrak{D}_s$ of degree s over $\mathfrak{D}$.

We shall give here a criterion of maximal orders, adapted for later considerations. Namely, if $\mathfrak{O}$ is an order and $\mathfrak{P}$ its two-sided ideal in A, they are

4) Galois groups of infinite Galois extensions are always considered in the topology of Krull. Cf. W. Krull, Galoissche Theorie der unendlichen algebraischen Erweiterungen, Math. Ann., 100 (1928).

5) Cf. van der Waerden, l. c. 3), or N. Jacobson, *The theory of rings* (1943).

6) Cf. H. Hasse, Über $\mathfrak{p}$-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme, Math. Ann., 104 (1931).

*) $e \mid m$ reads as 'e is a divisor of m.'

a maximal order and its two-sided prime ideal if and only if the following conditions are satisfied:

1) $A=\bigcup_{i=1}^{\infty}\pi^{-i}\mathfrak{O}$,

2) $\mathfrak{P}$ is principal, i. e. $\mathfrak{P}=\Pi\,\mathfrak{O}$, and $\mathfrak{P}^e=\pi\,\mathfrak{O}$ for some positive integer e,

3) $\mathfrak{O}/\mathfrak{P}$ is simple.

For, if $\mathfrak{O}'$ is an order containing $\mathfrak{O}$, we have by 1) $\pi^k\mathfrak{O}'\subseteq\mathfrak{O}$ for sufficiently large k. Then $\mathfrak{P}^h=\pi^k\mathfrak{O}\subseteq\pi^k\mathfrak{O}'=\Pi^h\mathfrak{O}'$ for $h=ke$. Since it follows from 2), 3) that every two-sided ideal of $\mathfrak{O}/\mathfrak{P}^h$ is a power of $\mathfrak{P}/\mathfrak{P}^h$, we have $\Pi^h\mathfrak{O}'=\mathfrak{P}^{h'}=\Pi^{h'}\mathfrak{O}$, where $h'\leqslant h$. If $h'<h$, we would have $\Pi^{-1}\in\mathfrak{O}'$ and so $\pi^{-1}\in\mathfrak{O}'$, This would imply by 1) $\mathfrak{O}'=A$, what is impossible. Hence it follows that $h'=h$ and $\mathfrak{O}'=\mathfrak{O}$.

Let A be as above and B be another central simple algebra over k, which is unramified, i. e, $\mathfrak{p}_B=\pi\,\mathfrak{o}_B$, and has the residue class algebra $\mathfrak{B}$ central over $\mathfrak{k}$. Then $\mathfrak{o}_A\cdot\mathfrak{o}_B$ is a maximal order of $A\times B$, $\mathfrak{p}_A\cdot\mathfrak{o}_B$ is its two-sided prime ideal and the residue class algebra $\mathfrak{o}_A\cdot\mathfrak{o}_B/\mathfrak{p}_A\cdot\mathfrak{o}_B$ is the direct product of $\mathfrak{A}$ and $\mathfrak{B}$. First it is clear that $\mathfrak{O}=\mathfrak{o}_A\cdot\mathfrak{o}_B$ and $\mathfrak{P}=\mathfrak{p}_A\cdot\mathfrak{o}_B$ are an order and its two-sided ideal in $A\times B$ satisfying the conditions 1) and 2). We shall show that $\mathfrak{P}\frown\mathfrak{o}_A=\mathfrak{p}_A$, $\mathfrak{P}\frown\mathfrak{o}_B=\mathfrak{p}_B$. If these were not the case, we would have, say, $\mathfrak{P}\frown\mathfrak{o}_A=\mathfrak{o}_A$ since $\mathfrak{P}\frown\mathfrak{o}_A$ is a two-sided ideal in $\mathfrak{o}_A$ containing $\mathfrak{p}_A$. Then $\mathfrak{o}_A=\mathfrak{o}_A{}^e\subseteq\mathfrak{P}^e=\pi\,\mathfrak{O}$ and therefore $\pi^{-1}\in\mathfrak{O}$, which is impossible by 1). It follows that $(\mathfrak{P}+\mathfrak{o}_A)/\mathfrak{P}\cong\mathfrak{A}$, $(\mathfrak{P}+\mathfrak{o}_B)/\mathfrak{P}\cong\mathfrak{B}$ and so that $\mathfrak{O}/\mathfrak{P}$ is a homomorphic image of the direct product $\mathfrak{A}\times\mathfrak{B}$. But since both $\mathfrak{A}$ and $\mathfrak{B}$ are simple and $\mathfrak{B}$ is central over $\mathfrak{k}$, $\mathfrak{A}\times\mathfrak{B}$ is also simple. Hence $\mathfrak{O}/\mathfrak{P}$ is isomorphic to $\mathfrak{A}\times\mathfrak{B}$, whence follows 3) and our assertion.

Now we shall show that D splits in ${}^sk$ if and only if $\mathfrak{D}$ is separable over $\mathfrak{k}$[2]. Suppose first D splits in ${}^sk$. Then it splits also in a finite extension K of k contained in ${}^sk$. $[K:k]$ is then a multiple ms of m, the degree of D, and K can be embedded in $A=D_s$ so that 1 of K coincides with that of A[5]. If $K\longleftrightarrow\mathfrak{K}$, $\mathfrak{K}$ is embedded in $\mathfrak{A}=\mathfrak{D}_s$ in a similar fashion. It follows that $\mathfrak{K}$ is a maximal subfield of $\mathfrak{A}$, since $[\mathfrak{K}:\mathfrak{k}]=ms$ and the principal degree of $\mathfrak{A}$ over $\mathfrak{k}$ is not greater than that of A over k, i. e. than ms. This proves the separability of $\mathfrak{A}$, and therefore that of $\mathfrak{D}$. Conversely, let $\mathfrak{D}$ be separable over k. Then $\mathfrak{D}$ has a maximal separable subfield $\mathfrak{K}$ of degree equal to the principal degree of $\mathfrak{D}$. Applying the similar method as in § 1 we can find a subfield K of D such that $K\longleftrightarrow\mathfrak{K}$. Then K is maximal. For if not, the commutator subalgebra D' of K in D has the residue class algebra $\mathfrak{D}'$ whose center contains $\mathfrak{K}$. The degree m' of D' over its center K being greater than 1, the order f' of $\mathfrak{D}'$ over $\mathfrak{K}$ must be also greater than 1, since $m'\,|\,f'$, which contradicts to the maximality of $\mathfrak{K}$. Hence D splits in $K\subseteq{}^sk$. We have proved at the same time that if D has the mentioned property the principal degree of $\mathfrak{D}$ over $\mathfrak{k}$ is equal to the degree m of D. It follows that the degree of the center of $\mathfrak{D}$ over $\mathfrak{k}$ is equal to $m^2/f=e$ and that if in particular D is unramified $\mathfrak{D}$ is central over $\mathfrak{k}$. We shall denote by ${}^s\mathbf{B}$ the subgroup of $\mathbf{B}$ formed of all the algebra classes that split in ${}^sk$.

3. Let A be an algebra in ${}^s\mathbf{B}$. A has an absolutely irreducible representation[3]

$$A \ni a \longrightarrow X_a \in ({}^sk)_m ,$$

m being the degree of A. Given an element σ of $G({}^sk/k)$, $a \longrightarrow X_a^\sigma$ is also an irreducible representation of A, which is therefore equivalent to $\{X_a\}$. Hence we can choose $U_\sigma \in ({}^sk)_m$ such that

$$X_a^\sigma = U_\sigma^{-1} X_a U_\sigma \qquad \text{for } a \in A .$$

The matrix U_σ is determined by σ up to scalar multiple, whence we have

$$(1) \qquad U_\tau U_\sigma^\tau = \alpha_{\sigma,\tau} U_{\sigma\tau} .$$

$\{\alpha_{\sigma,\tau}\}$ forms a factor set of $G({}^sk/k)$ in ${}^sk$, namely it holds

$$\alpha_{\sigma,\tau}^\rho \alpha_{\sigma\tau,\rho} = \alpha_{\sigma,\tau\rho} \alpha_{\tau,\rho} \qquad (\sigma, \tau, \rho \in G({}^sk/k)).$$

As is easily verified the associated class of $\{\alpha_{\sigma,\tau}\}$ is not changed when we replace $\{X_a\}$, $\{U_\sigma\}$ by any other systems and is determined uniquely by the algebra class of A. If $\{Y_b\}$ is an irreducible representation in ${}^sk$ of B and if $Y_b^\sigma = V_\sigma^{-1} Y_b V_\sigma$, $V_\tau V_\sigma^\tau = \beta_{\sigma,\tau} V_{\sigma\tau}$, then $\{X_a \otimes Y_b\}$*) gives an irreducible representation of $A \times B$ in ${}^sk$ and $(X_a \otimes Y_b)^\sigma = (U_\sigma \otimes V_\sigma)^{-1} (X_a \otimes Y_b)(U_\sigma \otimes V_\sigma)$, $(U_\tau \otimes V_\tau)(U_\sigma \otimes V_\sigma)^\tau = \alpha_{\sigma,\tau}\beta_{\sigma,\tau}(U_{\sigma\tau} \otimes V_{\sigma\tau})$. Thus the factor set corresponding to $A \times B$ is the product of those corresponding to A and B.

Now let K be a splitting field of A which is a finite Galois extension of k and contained in ${}^sk$. Then taking the irreducible representation $\{X_a\}$ in K, the above considerations are carried out with equal U_σ for σ in one and the same class S mod $G({}^sk/K)$. In this way we can define U_S for $S \in G(K/k)$ and so $\alpha_{S,T}$ for $S, T \in G(K/k)$. We shall prove that A is similar to the crossed product $(\alpha_{S,T}, K)$[7]. For the purpose let $A = (\alpha'_{S,T}, K)$ and show that $\alpha_{S,T} \sim \alpha'_{S,T}$. We define $\{X_a\}$, $\{U_S\}$ as follows:

$$(2) \qquad A = \sum_S u_S K, \quad u_S u_T = u_{ST}\alpha'_{S,T}, \quad \alpha u_S = u_S \alpha^S \ (\alpha \in K),$$

$$(au_1, au_R, \cdots\cdots) = (u_1, u_R, \cdots) X_a \text{ for } a \in A ,$$

$$(u_1 u_S, u_R u_S, \cdots) = (u_1, u_R, \cdots) U_S \quad \text{for } S \in G(K/k).$$

*) $X_a \otimes Y_b$ denotes Kronecker product of X_a and Y_b.

7) Cf. van der Waerden, *Gruppen von linearen Transformationen*, Berlin, 1935.

Then $\{X_a\}$ is an irreducible representation of A in K and we have $X_a^S = U_S^{-1} X_a U_S$. On the other hand as $U_S = \sum_R \alpha'_{R,S} E_{RS,R}$ *), we have by easy computations $U_T U_S^T = \alpha'_{S,T} U_{ST}$. This proves the above statement. In the following we assume that $\{U_\sigma\}$ and $\{\alpha_{\sigma,\tau}\}$ are adjusted for some K in the above sense.

Let R be the additive group of real numbers, I the subgroup of integers, T the factor group of R by I. We consider them as groups with operators in $G({}^sk/k)$ in the trivial manner. Assume now that ν is normalized; then the extension $\tilde{\nu}$ of ν to ${}^sk$ is also discrete and normalized. By (1) and the invariance of $\tilde{\nu}$, we have

$$\tilde{\nu}(|U_\tau|) + \tilde{\nu}(|U_\sigma|) = m\tilde{\nu}(\alpha_{\sigma,\tau}) + \tilde{\nu}(|U_{\sigma\tau}|).$$

We put

$$f_A(\sigma) = \frac{1}{m}\tilde{\nu}(|U_\sigma|) \qquad \text{for } \sigma \in G({}^sk/k),$$

$$F_A(\sigma,\tau) = \tilde{\nu}(\alpha_{\sigma,\tau}) \qquad \text{for } \sigma,\tau \in G({}^sk/k),$$

and consider them as cochains of $G({}^sk/k)$ in R. These cochains are *continuous* in the sense that they are induced from those of a finite group $G(K/k)$, where K is a sufficiently large finite Galois extension of k such that $A_K \sim 1$. In applying the cohomology theory[8] we restrict ourselves only to consider continuous cochains. Thus we mean by coboundaries only the coboundaries of continuous cochains. Now $F_A(\sigma,\tau)$ is a 2-cocycle in I, which is coboundary in R, i.e. $F_A = \delta f_A$, and $\bar{f}_A(\sigma)$ is a 1-cocycle, i.e. homomorphism, in T, $\bar{f}_A(\sigma)$ denoting the coset of $f_A(\sigma)$ mod I. The cohomology classes of $F_A(\sigma,\tau)$ and $\bar{f}_A(\sigma)$ are uniquely determined by the algebra class of A. Moreover as the operation of $G({}^sk/k)$ on T is trivial, every 1-coboundaries being also trivial, the 1-cocycle $\bar{f}_A(\sigma)$ itself is determined uniquely. It should be also noted that every cohomology class in R is trivial since the divisions are uniquely possible in R. In particular if $F_A = \delta f$ with 1-cochain f in R then we have $f = f_A$. For since $F_A = \delta f_A$. we have $\delta(f - f_A) = 0$. Therefore $f - f_A$ is a 1-coboundary, which is always trivial. Hence we have $f = f_A$.

The image of the homomorphism $\bar{f}_A(\sigma)$ being abelian, its values depend only on the coset of σ mod $G({}^sk/{}^ak)$. Therefore we can define $(A,\sigma) \in T$ for

---

*) $E_{S,T}$ is a matrix unit whose (S, T)-component is 1, but all the other components are zero.

8) S. Eilenberg and S. MacLane, Cohomology theory in abstract groups, Ann. of Math., 48 (1947).

$A \in {}^s\mathbf{B}$ and $\sigma \in G({}^a k/k)$ by the value of $\bar{f}_A$ on the coset σ. We have by what precede

$$(A, \sigma\tau) = (A, \sigma) + (A, \tau),$$

$$(A \times B, \sigma) = (A, \sigma) + (B, \sigma),$$

and that (A, σ) is continuous for σ according to the topology of the Galois group $G({}^a k/k)$.

4. Let χ be a (continuous) character of $G(k^a/k)$. We shall denote by Z_χ the subfield of k^a corresponding to the annihilator of χ in $G(k^a/k)$ in the sense of Galois theory, and by S_χ the generator of the cyclic group $G(Z_\chi/k)$ such that $(\chi, S_\chi) \equiv 1/m \mod 1$, where m is the order of χ. We denote the cyclic algebra (a, Z_χ, S_χ) by (a, χ). Then it is easily proved that

$$(a, \chi) \times (a, \chi') \sim (a, \chi\chi').$$

Hence the classes of cyclic algebras of type (π, χ), where χ is a character of $G({}^a k/k)$, form a subgroup $\mathbf{B}_\pi$ of ${}^s\mathbf{B}$. We shall prove that

$$((\pi, \chi), \sigma) = (\chi, \sigma) \quad \text{for } \sigma \in G({}^a k/k).$$

Let

$$(\pi, \chi) = \sum_{i=0}^{m-1} u^i Z_\chi, \quad u^m = \pi, \quad \alpha u = u\alpha^{S_\chi} \, (\alpha \in Z_\chi).$$

If we define X_a and U_S as in (2), we have

$$U_{S_\chi} = X_u = \begin{pmatrix} 0 & \cdots & & \pi \\ 1 & \ddots & & \vdots \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 \end{pmatrix}.$$

Hence if σ induces S_χ^k in Z_χ, we have

$$((\pi, \chi), \sigma) \equiv \frac{1}{m} \tilde{\nu}(|X_u^k|) = \frac{k}{m} \equiv (\chi, \sigma) \pmod 1.$$

This proves that $\mathbf{B}_\pi$ is isomorphic to the charactor group of $G({}^a k/k)$, or what is the same, to that of $G(\mathfrak{k}^a/\mathfrak{k})$, and that if we put

$$\mathbf{B}_0 = \{A;\ A \in {}^s\mathbf{B},\ (A, \sigma) \equiv 0 \text{ for all } \sigma \in G({}^a k/k)\},$$

${}^s\mathbf{B}$ is the direct product of $\mathbf{B}_0$ and $\mathbf{B}_\pi$.

As the degree m of (π, χ) coincides with its exponent, (π, χ) is a central division algebra, and as $\pi = u^m$ we have $m \mid e$ and thus $e = f = m$. Its maximal order $\mathfrak{o}_D$, two-sided prime ideal $\mathfrak{p}_D$ and the residue class algebra $\mathfrak{D}$ are given as follows:

$$\mathfrak{o}_D = \sum_{i=0}^{m-1} u^i \mathfrak{o}_\chi,$$

$$\mathfrak{p}_D = \mathfrak{p}_\chi + \sum_{i=1}^{m-1} u^i \mathfrak{o}_\chi ,$$

$$\mathfrak{D} = \mathfrak{o}_D/\mathfrak{p}_D = \mathfrak{o}_\chi/\mathfrak{p}_\chi = \mathfrak{Z}_\chi ,$$

where $\mathfrak{o}_\chi$, $\mathfrak{p}_\chi$ are the valuation ring and the prime ideal in Z_χ and $Z_\chi \longleftrightarrow \mathfrak{Z}_\chi$.

If $A \in \mathbf{B}_0$, we have $f_A(\sigma) \in I$ and therefore $F_A(\sigma, \tau)$ is a coboundary in I. Conversely if $F_A(\sigma, \tau)$ is a coboundary in I, we have by a remark in § 3 $f_A(\sigma) \in I$. It follows that $A \in \mathbf{B}_0$, if and only if $A \sim (\alpha_{S, T}, K)$ with $K \subseteq {}^s k$, $\tilde{\nu}(\alpha_{S, T}) = 0$. Let $A = (\alpha_{S, T}, K)$ with $K \subseteq {}^s k$, $\tilde{\nu}(\alpha_{S, T}) = 0$, and $\mathfrak{o}_K$, $\mathfrak{p}_K$ be the valuation ring and the prime ideal in K and $K \longleftrightarrow \mathfrak{K} = \mathfrak{o}_K/\mathfrak{p}_K$. Then a maximal order $\mathfrak{o}_A$, its two-sided prime ideal $\mathfrak{p}_A$ and the residue class algebra $\mathfrak{A}$ of A are given as follows:

$$\mathfrak{o}_A = \sum_S u_S \mathfrak{o}_K ,$$

$$\mathfrak{p}_A = \sum_S u_S \mathfrak{p}_K ,$$

$$\mathfrak{A} = \sum_S \bar{u}_S \mathfrak{K} = (\bar{\alpha}_{S, T}, \mathfrak{K}) ,$$

where $\bar{u}_S, \bar{\alpha}_{S, T}$ represent their classes mod $\mathfrak{p}_A$ or $\mathfrak{p}_K$.*) Thus A is unramified and $\mathfrak{A}$ is central over $\mathfrak{k}$. Conversely it is known that, given a central simple algebra $\mathfrak{A}$ over $\mathfrak{k}$, there exists an unramified central simple algebra A over k such that $A \to \mathfrak{A}$[2]. The classes of these unramified algebras with residue class algebras central over k form a subgroup of ${}^s\mathbf{B}$ containing $\mathbf{B}_0$ and the intersection of this subgroup with $\mathbf{B}_\pi$ is $\{1\}$. Therefore this subgroup is identical with $\mathbf{B}_0$. As the algebra class of $\mathfrak{A}$ is uniquely determined by that of A, we have a homomorphism of $\mathbf{B}_0$ onto $B(\mathfrak{k})$ by the correspondence $A \to \mathfrak{A}$. It is in fact an isomorphism since this correspondence preserves the degree. (We shall denote $A \longleftrightarrow \mathfrak{A}$).

We have thus reached to the theorem of Witt-Nakayama: *If we denote by* $\mathbf{B}_0$ *the subgroup of* ${}^s\mathbf{B}$ *formed of all unramified algebra classes and by* $\mathbf{B}_\pi$ *that of all algebra classes containing cyclic algebras of type* (π, χ), χ *being characters of* $G({}^a k/k)$, ${}^s\mathbf{B}$ *is the direct product of* $\mathbf{B}_0$ *and* $\mathbf{B}_\pi$. $\mathbf{B}_0$ *is isomorphic to the Brauer group* $B(\mathfrak{k})$ *of* $\mathfrak{k}$ *and* $\mathbf{B}_\pi$ *dual to the Galois group* $G(\mathfrak{k}^a/\mathfrak{k})$ *of the maximal abelian extension* $\mathfrak{k}^a$ *of* $\mathfrak{k}$. The structure of ${}^s\mathbf{B}$ is thus completely determined and it depends only on the residue class field $\mathfrak{k}$.

The determination of the structure of $\mathbf{B}$ itself (or $\mathbf{B}/{}^s\mathbf{B}$) is a problem remained still open.

---

*) These statements on maximal orders follow immediately from the criterion given in § 2.

5. We shall give here some supplementary considerations concerning with the isomorphisms and the scalar extensions of k

Let τ be a continuous isomorphism of k onto another discretely-valued complete field k' with the residue class field $\mathfrak{k}'$. Then τ induces in the residue class field an isomorphism of $\mathfrak{k}$ onto $\mathfrak{k}'$, which we denote by $\bar{\tau}$. τ $(\bar{\tau})$ can be extended uniquely to an isomorphism of $B(k)$ $(B(\mathfrak{k}))$ onto $B(k')$ $(B(\mathfrak{k}'))$ and that of $G(k^a/k)$ $(G(\mathfrak{k}^a/\mathfrak{k}))$ onto $G(k'^a/k')$ $(G(\mathfrak{k}'^a/\mathfrak{k}'))$, or that between their character groups. All of these isomorphisms we denote again by τ $(\bar{\tau})$. Then we have obviously

a) if $A\in {}^sB(k)$, $\sigma\in G({}^ak/k)$, then we have $A^\tau\in {}^sB(k')$, $\sigma^\tau\in G({}^ak'/k')$ and

$$(A, \sigma)=(A^\tau, \sigma^\tau),$$

b)
$$(a, X)^\tau=(a^\tau, X^\tau)$$

for $a\in k$, X character of $G(k^a/k)$. If X is a character of $G({}^ak/k)$, then X^τ is a character of $G({}^ak'/k')$,

c) If $A\in B_0(k)$ and $A\longleftrightarrow\mathfrak{A}$ with $\mathfrak{A}\in B(\mathfrak{k})$, then $A^\tau\in B_0(k')$ and $A^\tau\longleftrightarrow\mathfrak{A}^{\bar{\tau}}$ with $\mathfrak{A}^{\bar{\tau}}\in B(\mathfrak{k}')$.

It follows in particular

$${}^sB(k)^\tau={}^sB(k'),\quad B_0(k)^\tau=B_0(k'),\quad B_\pi(k)^\tau=B_{\pi^\tau}(k').$$

Let K be a completion of an algebraic extension of k with a finite ramification exponent e and $\mathfrak{K}$ be its residue class field. The unique extension of ν to K being discrete and complete, our considerations can be also applied to K. We may assume that the algebraic closure $\bar{K}$ of K contains the algebraic closure $\bar{k}$ of k. Then each element $\bar{\sigma}$ of $G(K^a/K)$ induces in k^a an element σ of $G(k^a/k)$. Taking the dual of this correspondence we can define for any character X of $G(k^a/k)$ a character X_K of $G(K^a/K)$ by the relation $(X, \sigma)=(X_K, \bar{\sigma})$ for $\bar{\sigma}\in G(K^a/K)$. Then we have by the criterion given in § 2

a) if $A\in {}^sB(k)$, $\bar{\sigma}\in G({}^aK/K)$, then we have $A_K\in {}^sB(K)$, $\bar{\sigma}$ induces σ in $G({}^ak/k)$ and

$$(A_K, \bar{\sigma})=e(A, \sigma),$$

b)
$$(a, X)_K=(a, X_K)$$

for $a\in k$, X character of $G(k^a/k)$. If X is a character of $G({}^ak/k)$, then X_K is a character of $G({}^aK/K)$,

c) if $A\in B_0(k)$ and $A\longleftrightarrow\mathfrak{A}$ with $\mathfrak{A}\in B(\mathfrak{k})$, then $A_K\in B_0(K)$ and $A_K\longleftrightarrow\mathfrak{A}_{\mathfrak{K}}$ with $\mathfrak{A}_{\mathfrak{K}}\in B(\mathfrak{K})$.

It follows in particular

$${}^sB(k)_K\subseteq {}^sB(K).\quad B_0(k)_K\subseteq B_0(K),$$
$$B_\pi(k)_K\subseteq B_\pi(K).\quad \text{(in case } K \text{ unramified over } k)$$

6. Finally we shall consider the classical case where $\mathfrak{k}$ is a finite field $GF(q)$, $q=p^f$ with a prime number p, as a special case of the above considerations. As is well-known $\mathfrak{k}$ is perfect and there is no essential central division algebra over $\mathfrak{k}$. We have thus $\mathbf{B}={}^s\mathbf{B}=\mathbf{B}_\pi$. On the other hand, $\bar{\mathfrak{k}}=\mathfrak{k}^a$ and so ${}^sk={}^ak$ is the maximal unramified extension of k contained in $\bar{k}$. The automorphism of $\mathfrak{k}^a$ over $\mathfrak{k}$ which corresponds every element a of $\mathfrak{k}^a$ to a^q generates a free cyclic group which is everywhere dense in $G(\mathfrak{k}^a/\mathfrak{k})$. The corresponding automorphism of ${}^ak$ over k is called the Frobenius automorphism of ${}^ak/k$, which we denote by $\left(\frac{{}^ak/k}{\mathfrak{p}}\right)$. Every algebra class of A in $\mathbf{B}=\mathbf{B}_\pi$ is therefore determined uniquely by $\left(\frac{A}{\mathfrak{p}}\right)=(A, \left(\frac{{}^ak/k}{\mathfrak{p}}\right))$. This is nothing other than the Hasse's ***invariant*** of the algebra class of A[9]. It should be also noted that the invariant $\left(\frac{a, \chi}{\mathfrak{p}}\right)$ of the cyclic algebra (a, χ) is the ***norm residue symbol*** of Chevalley.[10]

9) Cf. H. Hasse, 1. c. 6), or Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper, Math. Ann. 107 (1933).

10) C. Chevalley, La théorie du corps de classes, Ann. of Math., 41 (1940).