THEORY OF CYCLIC ALGEBRAS OVER AN ALGEBRAIC NUMBER FIELD*

BY
HELMUT HASSE

I present this paper for publication to an American journal and in English for the following reason:

The theory of linear algebras has been greatly extended through the work of American mathematicians. Of late, German mathematicians have become active in this theory. In particular, they have succeeded in obtaining some apparently remarkable results by using the theory of algebraic numbers, ideals, and abstract algebra, highly developed in Germany in recent decades. These results do not seem to be as well known in America as they should be on account of their importance. This fact is due, perhaps, to the language difference or to the unavailability of the widely scattered sources.

This paper develops a new application of the above mentioned theories to the theory of linear algebras. Of particular importance is the fact that purely algebraic results are obtained from deep-lying arithmetical theorems. In the middle part, an account is given of the fundamental algebraic basis for these arithmetical methods. This account is more extended than is necessary for this paper, and should obviate an extended study of several German papers.

I am very grateful to Professor H. T. Engstrom (New Haven) for going through the manuscript and proof with me and anglicising my many literal translations from the German.

I. Statement of theorems to be proved†

1. Cyclic algebras. In I, the reference field is assumed to be an algebraic number field Ω of finite degree.‡

A *cyclic algebra* of degree n over Ω is defined as an algebra A of the following type:

---

* Presented to the Society, September 9, 1931; received by the editors May 29, 1931.

† This section has also appeared recently in German in the Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, 1931.

‡ In the following, such notations as are only made complete by naming a definite reference field, may be implicitly understood to be with respect to Ω unless another reference field is explicitly named.

Let Z be a cyclic corps* of degree n over Ω, and A an algebra with the Z-basis† $1, u, \cdots, u^{n-1}$ and with the relations

$$zu = uz^S, \text{ for every } z \text{ in } Z, \tag{1.1}$$

where S denotes a generating element of the Galois group of Z and z^S denotes the result of applying the automorphism S to z, and

$$u^n = \alpha \neq 0 \text{ in } \Omega. \tag{1.2}$$

A is an algebra of order n^2 with the basis $u^i z_k (i=0, \cdots, n-1; k=1, \cdots, n)$, where the z_k form a basis of Z. I shall call the generation of A in (1.1), (1.2) a *cyclic generation*, and denote it by

$$A = (\alpha, Z, S).$$

First, the following facts will be proved:

(1.3) *A is a normal simple algebra.*

(1.4) *Z is a maximal sub-corps of A, i.e., the elements of Z are the only elements of A commutative with every element of Z.*

Cyclic algebras were, on a large scale, first studied by Dickson‡ (2, 3 Kap. III, 4). Dickson (1 App. I§, 3 §42), in particular, stated the following criterion:

(1.5) *A sufficient condition that A be a division algebra is that α^n is the least power of α which is the norm of an element of Z.*§

For $n=2$, as Dickson (3 §§31, 32) proved, every normal division algebra is cyclic; the same holds, as Wedderburn (2) showed, for $n=3$.||

2. **Semi-invariants.** While A is completely fixed by the number α, the corps Z, and its automorphism S, conversely, α, Z, S are by no means uniquely determined by A. Hence the following questions arise:

(i) to characterise A by means of *invariant* quantities, and

(ii) to determine *all* cyclic generations of A. In the following, I shall give a complete solution of these problems. I shall develop, in other words, a *theory of invariants* of cyclic algebras.

---

* In the following, I distinguish *fields* (Greek letters) whose elements play the rôle of coefficients, and *corps* (Latin letters) which are to be regarded as commutative division algebras over fields.

† As a *V-basis* of W I denote generally a maximal set of elements of W which are linearly independent with respect to right-hand multiplication with elements of the division algebra V. Further I denote as *V-order* the number of elements of a V-basis, and as *V-coördinates* the right-hand coefficients of V in a representation by a V-basis. Basis, order, coördinates without a prefixed letter refer to Ω (see 181).

‡ Numerals in parentheses following proper names refer to the bibliography at the end of this paper.

§ See also the paper by Wedderburn there quoted, in which for the first time the following criterion was completely established.

|| See also Dickson (1 App. II).

Invariants of a cyclic algebra $A=(\alpha, Z, S)$ must be invariant, in particular, when Z is fixed. If something is invariant when Z is fixed, I call it *semi-invariant.* When emphasising the difference between such semi-invariants and invariants in the usual sense I call the latter also *total-invariants.*

As to semi-invariance, question (ii), and with it implicitly also question (i), will be answered by the following theorem:

(2.1) *For the identity**

$$(\alpha, Z, S) = (\bar{\alpha}, Z, \bar{S}), \text{ where } \bar{S} = S^{\mu} \text{ with } (\mu, n) = 1, \tag{2.1 1}$$

it is necessary and sufficient, that the numbers α and $\bar{\alpha}$ be connected by a substitution

$$\bar{\alpha} = \alpha^{\mu}\mathrm{N}(c), \tag{2.1 2}$$

with $c \neq 0$ in Z.

This substitution reverts to the connection

$$\bar{u} = u^{\mu}c \tag{2.1 3}$$

between the elements u and $\bar{u}$ in the two cyclic generations (2.1 1).

Here $\mathrm{N}(c)$ denotes the norm from Z.

3. **The norm residue symbol.**† As to total-invariants, I have been led to consider the norm residue symbols

$$\left(\frac{\alpha, Z}{\mathfrak{p}}\right) \equiv ((\alpha, Z)/\mathfrak{p})‡$$

for the prime spots (Primstellen) $\mathfrak{p}$ of Ω, in particular by considering simultaneously Dickson's criterion (1.5) for division algebras, the just stated elementary criterion for semi-invariance, and my former results on equivalence of general quadratic forms,§ which, in the case of quaternary forms with quadratic discriminant, are only formally different from the theory of cyclic algebras of degree $n=2$.

The norm residue symbol $((\alpha, Z)/\mathfrak{p})$ is a function of α whose values are elements of the Galois group of Z, i.e., powers of S. That function is essentially characterised by the following two properties:

---

* It is unnecessary to distinguish between isomorphism (equivalence) and identity unless subalgebras of the same algebra are considered.

† In the following, the general norm residue theory, recently developed by the author, is of the greatest importance. See therefore the papers Hasse (11, 12, 13 II).

‡ This alternative form has been introduced by the editors to simplify typography.

§ Hasse (1–4).

(3.1) $((\alpha, Z)/\mathfrak{p}) = 1$ *holds, if and only if* α *is congruent to the norm* $\mathrm{N}(z_\nu)$ *of an element* z_ν *of* Z *for each power* $\mathfrak{p}^\nu$ *as modulus, or, what is equivalent,* if* α *is the norm* $\mathrm{N}(z_\mathfrak{p})$ *of an element* $z_\mathfrak{p}$ *of the* $\mathfrak{p}$*-adic extension corps* $Z^\mathfrak{p}$ *of* Z.

$$\left(\frac{\alpha\bar{\alpha}, Z}{\mathfrak{p}}\right) = \left(\frac{\alpha, Z}{\mathfrak{p}}\right)\left(\frac{\bar{\alpha}, Z}{\mathfrak{p}}\right). \tag{3.2}$$

By (3.1) and (3.2), the symbol $((\alpha, Z)/\mathfrak{p})$ is indeed fixed except an arbitrary exponent prime to n and independent of α which may be attached.† It is a pity that one is not able to-day to fix that exponent in a quite natural manner, i.e., without having to consider also the congruence behavior of α for prime spots different from $\mathfrak{p}$ and with it, in principle, the law of reciprocity. Therefore, in order to obtain the complete definition of the symbol, one has to take the following round-about way:

Let $\mathfrak{f}$ be the conductor (Führer) of Z,‡ $\mathfrak{f}_\mathfrak{p}$ the exact power of $\mathfrak{p}$ contained in $\mathfrak{f}$, and α_0 a number in Ω with the following properties:

$$\alpha_0 \equiv \alpha \bmod \mathfrak{f}_\mathfrak{p}, \tag{3.3}$$

$$\alpha_0 \equiv 1 \bmod \frac{\mathfrak{f}}{\mathfrak{f}_\mathfrak{p}}, \tag{3.4}$$

$$\alpha_0 = \mathfrak{p}^\mu\mathfrak{q},\ \mathfrak{q} \text{ prime ideal} \neq \mathfrak{p} \text{ of } \Omega. \tag{3.5}$$

The existence of such a number α_0 is guaranteed by the generalised theorem of the arithemetical progression.§ Further, let $(Z/\mathfrak{q})$ be that uniquely determined automorphism of Z which satisfies the relation

$$z^{(Z/\mathfrak{q})} \equiv z^{N(\mathfrak{q})} \bmod \mathfrak{q}, \textit{ for every integer } z \textit{ in } Z, \tag{3.6}$$

where $N(\ )$ denotes the norm with respect to the rational corps.

Then the definition of the symbol is as follows:

$$\left(\frac{\alpha, Z}{\mathfrak{p}}\right) = \left(\frac{Z}{\mathfrak{q}}\right). \tag{3.7}$$

The symbol so defined is independent of the choice of the auxiliary number α_0 according to (3.3)–(3.5), and it satisfies the relations (3.1) and (3.2). Of course, these statements require particular proofs. These proofs are rather

* Hasse (12 p. 150).

† This follows immediately from the fact that Z is cyclic.

‡ I.e., the conductor of the ideal class group to which Z belongs as class corps (Klassenkörper) See Hasse (7, 9).

§ Hasse (7 Satz 13). Incidentally (3.5) may also be omitted; see Hasse (11, 13 §6). I adjoined it here only in order to get a formal simplification in the later proof of Theorem 1, (i).

intricate, in particular as to (3.1). They depend on the general law of reciprocity of Artin (1).

The general law of reciprocity itself may be expressed by means of the norm residue symbol in the very simple and pregnant form

$$\prod_{\mathfrak{p}} \left(\frac{\alpha, Z}{\mathfrak{p}}\right) = E, \tag{3.8}$$

where $\mathfrak{p}$ runs through all prime spots of Ω, and E denotes the unit automorphism of Z. More explicitly, (3.8) means that the symbol $((\alpha, Z)/\mathfrak{p})$ is different from E only for a finite number of prime spots $\mathfrak{p}$, and between the symbol values for these $\mathfrak{p}$, the dependence expressed in the product relation (3.8) holds.

The prime spots $\mathfrak{p}$ for which the symbol $((\alpha, Z)/\mathfrak{p})$ is, at most, different from E, may be found from the fact

(3.9) $((\alpha, Z)/\mathfrak{p}) = E$, *if* $\mathfrak{p}$ *is not contained in* $\mathfrak{f}$ *and not in* α.

This fact is a special case of the following:

$$\left(\frac{\alpha, Z}{\mathfrak{p}}\right) = \left(\frac{Z}{\mathfrak{p}}\right)^{\mu}, \tag{3.10}$$

if $\mathfrak{p}$ *is not contained in* $\mathfrak{f}$ *and is contained in* α *with exactly the exponent* μ.

Finally, I shall quote the following theorem, which is of fundamental importance for the purpose I have to deal with in this paper:

(3.11) α *is a norm of an element of* Z, *if and only if*

$$\left(\frac{\alpha, Z}{\mathfrak{p}}\right) = E$$

for all prime spots $\mathfrak{p}$ *of* Ω.*

4. **Total-invariants.** The norm residue symbols $((\alpha, Z)/\mathfrak{p})$ are by no means total-invariants of $A = (\alpha, Z, S)$. They are, indeed, not even semi-invariants; for, with the substitution (2.1 2), according to (3.1), (3.2),

$$\left(\frac{\bar{\alpha}, Z}{\mathfrak{p}}\right) = \left(\frac{\alpha^{\mu} \mathrm{N}(c), Z}{\mathfrak{p}}\right) = \left(\frac{\alpha^{\mu}, Z}{\mathfrak{p}}\right)\left(\frac{\mathrm{N}(c), Z}{\mathfrak{p}}\right) = \left(\frac{\alpha, Z}{\mathfrak{p}}\right)^{\mu} \tag{4.1}$$

holds.

* See Hasse (13 §8, 15). In (13 §8) I was able to prove this theorem only for a prime degree n. Inspired by the important applications in the theory of cyclic algebras developed in this paper, I succeeded recently, in (15), in proving (3.11) for general degree n. It may be explicitly noticed, that (3.11), in distinction to (3.1)–(3.10), does not hold for every general abelian corps Z, but does hold in the cyclic case.

It is, however, easy to form total-invariants, namely by inweaving the automorphism S, coupled with α in the cyclic generation according to (1.1), (1.2). As a matter of fact, $((\alpha, Z)/\mathfrak{p})$ may be represented as a power of the generating automorphism S:

$$\left(\frac{\alpha, Z}{\mathfrak{p}}\right) = S^{\nu_{\mathfrak{p}}}. \tag{4.2}$$

Now, the exponents $\nu_{\mathfrak{p}}$, uniquely determined mod n, claim the interest. For dealing with them, I write likewise as a substitute for (4.2), by preliminarily introducing a new set of symbols,

$$\left[\frac{\alpha, Z, S}{\mathfrak{p}}\right] = [(\alpha, Z, S)/\mathfrak{p}]^* \equiv \nu_{\mathfrak{p}} \pmod{n}. \tag{4.3}$$

Then, the following holds:

(4.4) *The symbols* $[(\alpha, Z, S)/\mathfrak{p}]$ *are semi-invariant, i.e., from*

$$(\alpha, Z, S) = (\bar{\alpha}, \bar{Z}, \bar{S})$$

follows

$$\left[\frac{\alpha, Z, S}{\mathfrak{p}}\right] \equiv \left[\frac{\bar{\alpha}, \bar{Z}, \bar{S}}{\mathfrak{p}}\right] \pmod{n},$$

for each prime spot $\mathfrak{p}$ *of* Ω.

For, by the substitution (2.1 2) connected with the identity (2.1 1), the relation (4.2) changes, according to (4.1), into

$$\left(\frac{\bar{\alpha}, Z}{\mathfrak{p}}\right) = \left(\frac{\alpha, Z}{\mathfrak{p}}\right)^{\mu} = S^{\mu\nu_{\mathfrak{p}}} = \bar{S}^{\nu_{\mathfrak{p}}}.$$

In the following I shall indeed prove

THEOREM A. (i) *The symbols* $[(\alpha, Z, S)/\mathfrak{p}]$ *are total-invariant.*

(ii) *The symbols* $[(\alpha, Z, S)/\mathfrak{p}]$, *together with the degree* n, *are a complete set of total-invariants, i.e.,*

$$(\alpha, Z, S) = (\bar{\alpha}, \bar{Z}, \bar{S})$$

holds, if and only if

$$\left[\frac{\alpha, Z, S}{\mathfrak{p}}\right] \equiv \left[\frac{\bar{\alpha}, \bar{Z}, \bar{S}}{\mathfrak{p}}\right] \pmod{n}$$

for each prime spot $\mathfrak{p}$ *of* Ω.

* This alternative form has been introduced by the editors to simplify typography.

This theorem gives the solution of the above question (i), to characterise cyclic algebras in a total-invariant manner. As a complete set of total-invariants a set of residue classes $\nu_\mathfrak{p} \pmod n$, presents itself, uniquely corresponding to the prime spots $\mathfrak{p}$ of Ω, and different from 0 only for a finite number of $\mathfrak{p}$.*

I shall further give the solution of the above question (ii), to determine all cyclic generations of a given cyclic algebra, by the following theorem:

THEOREM B. *For a cyclic algebra A of degree n with the invariants $\nu_\mathfrak{p}$, a cyclic corps Z of degree n leads to a cyclic generation, if and only if, for each prime spot $\mathfrak{p}$ of Ω, the $\mathfrak{p}$-degree $n_\mathfrak{p}$ of Z is a multiple of the integer*

$$m_\mathfrak{p} = \frac{n}{(\nu_\mathfrak{p}, n)}.$$

Here I denote as the $\mathfrak{p}$-*degree* of Z the order of the decomposition group (Zerlegungsgruppe†) of the prime divisors $\mathfrak{P}$ of $\mathfrak{p}$ in Z, i.e., also the product of the degree and order of the $\mathfrak{P}$, or hence, still more simply expressed, the degree of the corresponding $\mathfrak{P}$-adic corps $Z_\mathfrak{P}$.

As to all of the cyclic generations arising then from Z, full knowledge is already given by (2.1).

In particular, it may be noticed, that for only a finite number of $\mathfrak{p}$'s the integer $m_\mathfrak{p}$ is different from 1. Hence, for only a finite number of $\mathfrak{p}$'s there are really restrictive conditions in Theorem B.

5. **Similar algebras.** Theorems A and B are contained in more general facts arising from considering also the degree n as variable.

As a normal simple algebra every cyclic algebra A, according to the second structure theorem of Wedderburn (1),‡ may be represented as a direct product $A = D \times M$ of a normal division algebra D and a total matrix algebra M. Moreover D and M are uniquely determined apart from an interior automorphism of A (transformation with a regular element of A).§ I shall call two normal simple algebras A and $\overline{A}$ *similar*, $A \sim \overline{A}$, if the division algebras D and $\overline{D}$ contained within them are isomorphic (equivalent). If A

---

* Recording, however, explicitly this finite number of $\mathfrak{p}$'s according to (3.9), and restricting one's self in the theorems to stating the conditions for the corresponding $\nu_\mathfrak{p}$, would yield rather disagreeable complications. Albert (1) does this. He states there a result equivalent to my Theorem A dealing with the special case of rational generalised quaternion algebras.

† See Hasse (7. Erl. 30, 9 §8).

‡ See also Dickson (1 §51, 3 §78), Artin (2).

§ See Wedderburn (1), Artin (2).

and $\overline{A}$ are of the same degree,* this obviously leads back to the isomorphism. In particular, I denote by $A \sim 1$ that A is a total matrix algebra, $A = M$.

If A is similar to a cyclic algebra (α, Z, S), I call A cyclically representable, (α, Z, S) a *cyclic representation* of A, and Z a *cyclic representation corps* for A.

To any class of normal simple algebras similar to each other, there are two corresponding integers, namely the *index* m, and the *exponent* l. The index m is defined as the degree of the division algebra similar to A. The exponent l is defined as the least integer for which $A^l \sim 1$ (the power to be understood in the sense of direct product).†

6. **Enunciation of the theorems.** The invariants

$$\left[\frac{\alpha, Z, S}{\mathfrak{p}}\right] \equiv \nu_{\mathfrak{p}} \pmod{n}$$

of a cyclic algebra $A = (\alpha, Z, S)$ of degree n carry with them, as residue classes mod n, a reference to the degree n of A. Formally it is possible to get rid of that degree by introducing the corresponding quotients $\nu_{\mathfrak{p}}/n$. In accordance with this it is suitable, instead of the symbol set preliminarily introduced in (4.3), to define rather, definitively, a new set of symbols by

$$(6.1) \qquad \left(\frac{\alpha, Z, S}{\mathfrak{p}}\right) = ((\alpha, Z, S)/\mathfrak{p}) \equiv \frac{\nu_{\mathfrak{p}}}{n} \pmod 1, \text{ if } \left(\frac{\alpha, Z}{\mathfrak{p}}\right) = S^{\nu_{\mathfrak{p}}}.$$

The integers $m_{\mathfrak{p}}$, appearing above in Theorem B, are then precisely the denominators in the reduced expression of those fractions:

$$(6.2) \qquad \frac{\nu_{\mathfrak{p}}}{n} \equiv \frac{\mu_{\mathfrak{p}}}{m_{\mathfrak{p}}} \pmod 1, \quad (\mu_{\mathfrak{p}}, m_{\mathfrak{p}}) = 1.$$

For these integers $m_{\mathfrak{p}}$ the following holds obviously, according to (4.2), (6.2):

(6.3) *$m_{\mathfrak{p}}$ is the order of the norm residue symbol* $((\alpha, Z, S)/\mathfrak{p})$.

Now the following theorems may be stated, which include especially the above Theorems A and B:

THEOREM 1. (i) *The symbols* $((\alpha, Z, S)/\mathfrak{p})$ *are total-invariant in the sense of similarity.*

---

* I suggest the use of *degree* instead of the American *rank*. For in Germany *Rang* is usual as a synonym for the American *order*, as seems quite natural considering the meaning of *Rang* (number of linear independent solutions) in the classical linear algebra. There is practically no objection to *degree*, for it is still neutral in both countries. Moreover the thing dealt with is really a "degree" (see the subsequent result (11.3)).

† The existence of such an l was first proved by Brauer (2,3). See also the subsequent proof in §12.

(ii) *The symbols* $((\alpha, Z, S)/\mathfrak{p})$ *are a complete set of total-invariants in the sense of similarity, i.e.,*

$$(\alpha, Z, S) \sim (\bar{\alpha}, \overline{Z}, \bar{S})$$

holds, if and only if

$$\left(\frac{\alpha, Z, S}{\mathfrak{p}}\right) \equiv \left(\frac{\bar{\alpha}, \overline{Z}, \bar{S}}{\mathfrak{p}}\right) \pmod 1$$

for each prime spot $\mathfrak{p}$ *of* Ω.

This theorem gives the solution of the problem to characterise cyclically representable algebras in a total-invariant manner. As a complete set of total-invariants a set of residue classes $\mu_{\mathfrak{p}}/m_{\mathfrak{p}} \pmod 1$ presents itself, uniquely corresponding to the prime spots $\mathfrak{p}$ of Ω, and different from 0 only for a finite number of $\mathfrak{p}$'s.

For placing in evidence the independence of the total-invariant $((\alpha, Z, S)/\mathfrak{p})$ from the casual cyclic representation (α, Z, S) I use the symbol

$$\left(\frac{A}{\mathfrak{p}}\right) \equiv \left(\frac{\alpha, Z, S}{\mathfrak{p}}\right) \pmod 1. \tag{6.4}$$

In particular, I call the reduced denominators $m_{\mathfrak{p}}$ of the total-invariants the $\mathfrak{p}$-*indices* of A.

The following Theorems show then how the theory of cyclically representable algebras may be expressed in terms of the indicated invariants.

THEOREM 2. *For a cyclically representable algebra* A, *a cyclic corps* Z *leads to a cyclic representation, if and only if for each prime spot* $\mathfrak{p}$ *of* Ω *the* $\mathfrak{p}$-*degree* $n_{\mathfrak{p}}$ *of* Z *is a multiple of the* $\mathfrak{p}$-*index* $m_{\mathfrak{p}}$ *of* A.

THEOREM 3. *For a cyclically representable algebra* A, *the relation*

$$A \sim 1$$

holds, if and only if

$$\left(\frac{A}{\mathfrak{p}}\right) \equiv 0 \pmod 1,$$

for each prime spot $\mathfrak{p}$ *of* Ω.

THEOREM 4. *The direct product* $\tilde{A} = A \times \overline{A}$ *of two cyclically representable algebras* A *and* $\overline{A}$ *is again cyclically representable. Moreover, for the corresponding invariants,*

$$\left(\frac{\tilde{A}}{\mathfrak{p}}\right) \equiv \left(\frac{A}{\mathfrak{p}}\right) + \left(\frac{\overline{A}}{\mathfrak{p}}\right) \pmod 1$$

holds.

THEOREM 5. *The index* m *of a cyclically representable algebra is equal to its exponent. They are both the least common multiple of all its* $\mathfrak{p}$-*indices* $m_{\mathfrak{p}}$.

According to (6.3) and (3.11) the least common multiple of the $m_\mathfrak{p}$ is precisely the exponent of the least power of α which is a norm of an element of Z. Hence Theorem 5 also gives

THEOREM 5'. *Let $A = (\alpha, Z, S)$ be a cyclic algebra of degree n. The degree m of the division algebra similar to A is the least integer, for which α^m is a norm of an element of Z.*

In particular, A itself is a division algebra, if and only if α^n is the least power of α which is a norm of an element of Z.

This theorem rounds off Dickson's above mentioned criterion (1.5).

THEOREM 6. *If an algebra is cyclically representable, it is cyclic.*

This theorem reduces, in particular, the important question, still unanswered, whether *every* normal division algebra D is cyclic, to the question whether there is even one cyclic algebra A similar to D.

It may be once more explicitly noticed that all these theorems depend essentially on the presupposition that the reference field Ω is an algebraic number field of finite degree. This also holds for those statements whose formulation is independent of the special nature of Ω, such as Theorem 6 and the first statement in Theorem 5.*

II. EMMY NOETHER'S THEORY OF CROSSED PRODUCTS

7. **Definition of a crossed product.** The proofs of the above theorems may be obtained in the simplest and most lucid manner by subordinating the theory of cyclic algebras or cyclically representable algebras to the theory of *crossed products* (*verschränkte Produkte*) developed recently by Emmy Noether.† I have been permitted by the author to give here an account of this very important new theory. The publication by the author herself which will start from a larger base, namely the general theory of representations by matrices (linear substitutions),‡ is likely to appear in the near future.§ For the present purpose, I have arranged the proofs for the convenience of a reader who does not care to go back to the theorems of the general theory of representations. I shall go into details only as far as it is needed for a person who knows the general theory of algebras as presented for example in Dickson (1, 3).‖

* As to the latter, see the contrary statement in Brauer (4 §5), due to a reference field containing indeterminate variables.

† In a lecture at the University of Göttingen, 1929.

‡ For this see the extensive paper Noether (2).

§ In a separate paper and also in van der Waerden (1).

‖ The norm residue theory and the theory of $\mathfrak{p}$-adic corps, very important in I and III, is in no way supposed to be known in II. Hence, if the reader perhaps should be deterred by the extensive

In II, the reference field Ω is allowed to be any abstract field with only the restriction to be perfect (vollkommen).* By such a generality algebraic number fields as well as their $\mathfrak{p}$-adic extensions are covered.

Like the conception of a cyclic algebra, the conception of a crossed product has its origin in constructions of Dickson (2, 3 Kap. III, 4). It may be briefly characterised by the fact that the cyclic corps Z is now replaced by a general Galois corps Z of degree n over Ω. Let G be the group of automorphisms of Z, the so-called Galois group of Z.

A *crossed product* of Z (by G) is defined as an algebra A of the following type:

A possesses a Z-basis u_S, uniquely corresponding to the n elements S of G, for which the relations

$$zu_S = u_S z^S, \tag{7.1}$$

$$u_S u_T = u_{ST} a_{S,T}, \tag{7.2}$$

where $a_{S,T} \neq 0$ in Z, hold. The set (a) of the coefficients $a_{S,T}$ is called the *factor set* (*Factorensystem*) of A.

A is an algebra of order n^2 with the basis $u_S z_k$ (S in G, $k = 1, \cdots, n$), where the z_k form a basis of Z. I shall denote the generation of A in (7.1), (7.2) by

$$A = (a, Z).$$

8. **Elementary properties of a crossed product.** I begin by stating some elementary facts concerning crossed products $A = (a, Z)$.

From the associativity of A the restrictive condition

$$a_{S,T}^{U} = \frac{a_{T,U} a_{S,TU}}{a_{ST,U}} \tag{8.1}$$

for the factor set (a) follows at once. This associative condition presents itself as a rule for the application of the automorphisms U from G to the factors $a_{S,T}$.

Conversely, every set of elements $a_{S,T} \neq 0$ in Z, satisfying the restrictive condition (8.1), obviously leads, by fixing (7.1), (7.2) (and trivial associative relations), to an algebra A of order n^2 with the crossed product representation $A = (a, Z)$.

A contains the modulus (unit)

---

knowledge required in I, he may nevertheless go on studying II. I hope he will not be disappointed or discouraged before getting through II.

* In the sense of Steinitz (1 §11). See also Hasse (8 §4). This assumption aims to guarantee the validity of Galois theory in its full extension.

(8.2) $$e = u_E a_{E,E}^{-1},$$

where E denotes the unit in G. This may be easily verified, since, by (7.1), e is commutative with the elements of Z and, by (8.1), in particular

(8.3) $$a_{E,E}^{S} = a_{E,S}, \quad a_{S,E} = a_{E,E}$$

hold.

No misunderstanding arises in identifying the modulus e and the unit of Z, i.e., the sub-corps $Ze = Zu_E$, isomorphic to Z, and the corps Z itself. Then (8.2) becomes

(8.4) $$u_E = a_{E,E}.$$

Furthermore the following is true:

(8.5) *Z is a maximal sub-corps of A, i.e., the elements of Z are the only elements of A commutative with every element of Z.*

Let

$$a = \sum_S u_S z_S, \quad z_S \text{ in } Z,$$

be an element of A with its representation by the Z-basis u_S, and z an element in Z. From $az = za$ follows by (7.1)

$$\sum_S u_S z_S z = \sum_S u_S z^S z_S,$$

whence, by equating Z-coördinates,

$$(z - z^S) z_S = 0,$$

for each S of G. Taking here z as a primitive element in Z, one has $z^S \neq z$, if $S \neq E$, whence

$$z_S = 0, \text{ if } S \neq E.$$

Thus, with regard to (8.4), a is of the simple form

$$a = u_E z_E = a_{E,E} z_E.$$

This means that a belongs to Z.

Further, we have

(8.6) *The elements u_S are regular (not divisors of zero).*

From (7.2), (8.4),

$$u_S u_{S^{-1}} = a_{E,E} a_{S,S^{-1}}$$

follows, i.e.,

$$u_S^{-1} = u_{S^{-1}} a_{S,S^{-1}}^{-1} a_{E,E}^{-1}. \tag{8.6 1}$$

The theory of invariants of the crossed product representations with a fixed Z, or, as I shall call it again, the theory of *semi-invariants*, is given by the following theorem:

(8.7) *For the identity*

$$(a, Z) = (\bar{a}, Z) \tag{8.7 1}$$

it is necessary and sufficient that the factor sets (a) *and* $(\bar{a})$ *be connected by a relation*

$$\bar{a}_{S,T} = a_{S,T} \frac{c_T c_S{}^T}{c_{ST}}, \tag{8.7 2}$$

with elements $c_S \neq 0$ *in* Z.

This relation reverts to the connection

$$\bar{u}_S = u_S c_S \tag{8.7 3}$$

between the Z-bases u_S *and* $\bar{u}_S$ *in the two crossed product representations* (8.7 1).

(a) If (8.7 1) holds, $u_S{}^{-1}\bar{u}_S$ is, by (7.1), commutative with every element of Z. Hence, by (8.5), (8.6), $u_S{}^{-1}\bar{u}_S$ itself is an element $c_S \neq 0$ in Z, i.e., (8.7 3) holds. (8.7 2) follows from this by the elementary calculation

$$\bar{u}_S \bar{u}_T = u_S c_S u_T c_T = u_S u_T c_S{}^T c_T = u_{ST} a_{S,T} c_S{}^T c_T$$
$$= \bar{u}_{ST} a_{S,T} \frac{c_S{}^T c_T}{c_{ST}}.$$

(b) If (8.7 2) holds and a new Z-basis $\bar{u}_S$ is introduced by (8.7 3), according to the calculation just outlined $(\bar{a})$ is found to be the corresponding factor set. Hence (a, Z) is also of the type $(\bar{a}, Z)$, i.e., (8.7 1) holds.

Factor sets (a) and $(\bar{a})$, connected as in (8.7 2), are called *associated*, and one writes for brevity

$$(\bar{a}) \sim (a).$$

The characteristic semi-invariant for a crossed product is then, according to (8.7), the corresponding class of associated factor sets.

9. Structure of a crossed product. I develop now the deeper lying structural properties of crossed products.

For this purpose it is suitable to use the concept of a *splitting field* (*Zerfällungskörper*), introduced by Brauer (1) and Noether (1). A field Z over Ω is called a splitting field for a normal simple algebra A, if the normal simple algebra A_Z, determined by A over Z, i.e., the direct product $A \times Z$, is ~ 1.

It is known that this holds in any case for the field Ω' of all algebraic elements over Ω, and indeed also for fields Z of finite degree over Ω (e.g., for a field which arises from Ω by adjunction of all Ω'-coördinates of a complete set of matrix units in $A_{\Omega'}$, representing these matrix units by an Ω-basis of $A_{\Omega'}$, which belongs to the sub-algebra A).* In what follows a *splitting field* is implicitly always meant to be one of finite degree.

Of course, every splitting field of A belongs at once to the whole class of all algebras similar to A, in particular to the division algebra D within this class.

(9.1) *Every crossed product $A=(a, Z)$ is a normal simple algebra.*

(9.2) *The field Z, isomorphic to Z, is a splitting field for A.*

(i) I show first that A is normal, i.e., has the centrum Ω. This follows easily from (8.5). (8.5) means, in fact, that the centrum of A is contained in Z. Now, by (7.1), only those elements of Z are commutative also with each u_S that are invariant under each automorphism S from G. This condition is satisfied only by the elements of the reference field Ω.

I pass now to the proof that A is simple, i.e., has no proper invariant sub-algebra. Let B be a proper invariant sub-algebra of A, not zero. Let, further,

$$b = \sum_S u_S y_S, \quad y_S \text{ in } Z,$$

be the Z-basis representation of an element b of B, not zero. Let here $S=R, \cdots, T, U$ be exactly those subscripts to which non-zero Z-coördinates y_S correspond. Because of the invariance of B, then

$$zb = \sum_S z u_S y_S = \sum_S u_S z^S y_S \text{ and } b\bar{z} = \sum_S u_S y_S \bar{z}$$

also belong to B, for arbitrary z, $\bar{z}$ in Z. Hence, so does

$$b_1 = zb - b\bar{z} = \sum_S u_S y_S (z^S - \bar{z}).$$

Now z may be taken as a primitive element in Z, and $\bar{z}=z^U$. Then b_1 becomes an element in B in whose representation by the Z-basis u_S non-zero Z-coördinates correspond exactly to the subscripts $S=R, \cdots, T$ (without U). Proceeding in this way one is finally led to an element in B of the type $u_R y_R a_R$ with $a_R \neq 0$ in Z. Because of the invariance of B, u_R itself belongs to B, and therefore, further, *each*

$$u_S = u_R u_{R^{-1}S}^{-1} a_{R,R^{-1}S},$$

and with them every

* See Dickson (3 §86).

$$a = \sum_S u_S z_S$$

in A. This means $B = A$.

(ii) Let $\mathfrak{u} = (u_T)$ be the one-rowed matrix formed by the Z-basis u_S of A. By taking the Z-basis representations of the products au_T there results, for every a in A, a system of linear equations

$$a\mathfrak{u} = \mathfrak{u}A_a, \tag{9.3}$$

where A_a is a matrix in Z. These matrices A_a form, according to (9.3), an isomorphic *representation* $\mathfrak{A}$ of A in Z. Their degree (number of rows) is the degree n of Z.

Interesting, by the way, is the explicit expression of the matrices A_a, which may be deduced without difficulty by (7.1), (7.2),

$$A_a = (a_{ST^{-1},T}^{\ T} z_{ST^{-1}}) \quad (S \text{ rows, } T \text{ columns}), \tag{9.4}$$

when

$$a = \sum_S u_S z_S, \quad z_S \text{ in } Z.$$

In what follows, however, (9.4) is not needed.

From the representation $\mathfrak{A}$ in Z an isomorphic representation A in Z may be derived by passing through an isomorphism from Z to Z.

Now the change from A to A_Z means also for A that one must add all linear composita with arbitrary coefficients in Z. For, by this process, certainly a *homeomorphic* matrix algebra A_Z results. The latter must even be *isomorphic*. For, those elements of A_Z, to which the zero-matrix in A_Z corresponds, form an invariant sub-algebra B_Z of A_Z, which cannot be identical with A, because no element of A (except 0) belongs to it. Since A_Z is simple, as was shown in (i), $B_Z = 0$ follows. This means indeed the isomorphism between A_Z and A_Z.

Since A_Z has the order n^2 and consists of matrices of degree n, it follows further that $\mathrm{A}_Z \sim 1$. Hence also $A_Z \sim 1$, i.e., Z is a splitting field for A.

10. General normal simple algebras as crossed products. Of the results (9.1) and (9.2) also the converse, in a sense, is true. There hold, indeed, the following theorems, which illuminate the fundamental importance of the theory of crossed products for the general theory of algebras:

(10.1) *Every normal division algebra D (and therefore every normal simple algebra) is similar to crossed products $A = (a, Z)$.*

More precisely:

(10.2) *To every Galois splitting field* Z of D there corresponds a crossed product representation $A = (a, Z)$ of an algebra A, similar to D, with a corps Z, isomorphic to* Z.

* Of course, an arbitrary splitting field may always be extended to a Galois splitting field.

(a) I show, first, that the degree n of Z is a multiple $n=rm$ of the degree m of D.

The presupposition concerning Z means $D_Z \sim 1$. Let e_{ik} be a set of m^2 matrix units in D_Z. I consider, then, the right-invariant sub-algebra $R=e_{11}D_Z$ of D_Z, which consists of the first rows of this matrix representation.

Let r be the D-order of R. Since D has order m^2, the order of R is then rm^2. Otherwise, this order of R may also be calculated as the product of the Z-order of R, which is the number m of terms in the rows of R, by the order of Z, which is the degree n of Z; thus mn results as the order of R. Comparison yields

$$n = rm.$$

(b) I show, further, that the algebra A of degree $n=rm$, similar to D, contains a maximal sub-corps Z, isomorphic to Z.

Let $\mathfrak{r}$ be a D-basis of R, considered as a one-rowed matrix. By taking the D-basis representations of the products $\zeta\mathfrak{r}$ there results, for every ζ in Z, a system of linear equations.

$$\zeta\mathfrak{r} = \mathfrak{r}z_\zeta, \tag{10.3}$$

where z_ζ is a matrix in D. These matrices z_ζ form, according to (10.3), an isomorphic representation Z of Z by matrices in D. Their degree is the D-order r of R. Hence, Z is a sub-corps, isomorphic to Z, of the algebra A of degree $n=rm$, similar to D, for the latter may be regarded as the algebra of all matrices of degree r in D.

Moreover, Z is a maximal sub-corps of A, for A, as an algebra of degree n, contains no element, and therefore also no sub-corps, of a higher degree than n.

Hitherto no use has been made of the assumption that Z be Galois.

(c) Now I make use of this assumption, developing the influence of the automorphisms of Z on the representation Z furnished by (10.3).

The Galois group Γ of Z corresponds isomorphically to the Galois group G of Z by fixing

$$z_\zeta{}^S = z_{\zeta\Sigma} \quad (\Sigma \text{ in } \Gamma,\ S \text{ in } G). \tag{10.4}$$

Now, Γ may be made an automorphism group of $D_Z = D \times Z$ by fixing the elements of D to be invariant under Γ. Then, under an automorphism from Γ, the set of matrix units e_{ik} changes to another such set e_{ik}^Σ, the right invariant sub-algebra $R=e_{11}D_Z$ to the analogously formed $R^\Sigma = e_{11}^\Sigma D_Z$ and the D-basis $\mathfrak{r}$ of R to a D-basis $\mathfrak{r}^\Sigma$ of R^Σ.

Since Wedderburn's matrix representation is unique apart from an in-

terior automorphism of A, there is a regular element q_Σ in D_Z for which $e_{ik}^\Sigma = q_\Sigma e_{ik} q_\Sigma^{-1}$, and

$$R^\Sigma = q_\Sigma e_{11} q_\Sigma^{-1} D_Z = q_\Sigma e_{11} D_Z = q_\Sigma R.$$

Consequently, besides $\mathfrak{r}^\Sigma$, $q_\Sigma \mathfrak{r}$ also is a D-basis of R^Σ. Hence, one has a system of linear equations

$$q_\Sigma \mathfrak{r} = \mathfrak{r}^\Sigma u_S, \tag{10.5}$$

where u_S is a regular matrix in D, i.e., a regular element of A.

Now, by applying the automorphism Σ to (10.3), there results, with respect to the fixed invariance of the elements of D under Σ,

$$\zeta^\Sigma \mathfrak{r}^\Sigma = \mathfrak{r}^\Sigma z_\zeta.$$

Retransforming this, by the help of (10.5), to the D-basis $\mathfrak{r}$ of R, it follows that

$$\zeta^\Sigma \mathfrak{r} = \mathfrak{r} u_S^{-1} z_\zeta u_S.$$

This means, with regard to (10.3),

$$z_\zeta \Sigma = u_S^{-1} z_\zeta u_S.$$

According to (10.4), therefore,

$$z^S = u_S^{-1} z u_S, \text{ for every } z \text{ in } Z, \tag{10.6}$$

holds.

From (10.6), it follows further that the elements $u_{ST}^{-1} u_S u_T$ are commutative with all elements of Z. Since Z has been shown to be a maximal subcorps of A, it follows from this that these elements belong to Z. Because of the regularity of the u_S these elements are also different from zero. Hence

$$u_S u_T = u_{ST} a_{S,T}, \text{ with } a_{S,T} \neq 0 \text{ in } Z. \tag{10.7}$$

(d) I show, lastly, that $A = (a, Z)$.

For this purpose, with regard to the relations (10.6), (10.7) just stated, it is sufficient to adjoin the proof that the u_S form a Z-basis of A.

Now from a linear relation

$$\sum_S u_S y_S = 0, \quad y_S \text{ in } Z,$$

by a procedure like that in the proof of (9.1), using (10.6), a set of relations of the type

$$u_R y_R a_R = 0, \text{ with } a_R \neq 0 \text{ in } Z,$$

for each R from G may be deduced. These relations mean indeed $y_R \neq 0$ for

each R from G. Consequently, the u_S are linearly independent with respect to Z.

This implies that the sub-algebra $\Sigma_S u_S Z$ of A has the same order n^2 as A. Hence it is identical with A. It follows that the u_S really form a Z-basis of A.

11. **General splitting fields.** With regard to the results (9.1), (9.2) and (10.1), (10.2), the theory of crossed products may also be designated as the theory of Galois splitting fields of a normal division algebra D.

Parenthetically, for reasons of completeness, I adjoin here the theorems of Brauer (1,3) and Noether (1), which determine all splitting fields, both Galois and not Galois, of D.

As already noted, in (a) and (b) of the proof of (10.1), (10.2), independently of the assumption that Z be Galois, the following facts have been stated:

(11.1) *If* Z *is a splitting field for the normal division algebra* D, *the degree* n *of* Z *is a multiple* $n=rm$ *of the degree* m *of* D.

(11.2) *The algebra* A *of degree* n, *similar to* D, *contains a maximal sub-corps* Z, *isomorphic to* Z.

Of these results also the converse, in a sense, is true, at any rate for the special case where the reference field Ω is an algebraic number field of finite degree:

(11.3) *If* Z *is a maximal sub-corps of the normal simple algebra* A, *the degree of* Z *equals the degree* n *of* A.

(11.4) *Every field* Z, *isomorphic to* Z, *is a splitting field for* A.

(11.3) may be proved in a known manner by means of Hilbert's irreducibility theorem.*

(11.4) follows by considering the isomorphic matrix representation of A in Z furnished by a Z-basis of A. According to (11.3), its degree is n. Now the

---

* For division algebras see Dickson (3 §132). For general normal simple algebras analogous conclusions are valid; for this, see Artin (3 §4). For this proof the special assumption concerning the reference field Ω is essential.

For division algebras Albert (2) gave a very short proof of (11.3), which does not use Hilbert's irreducibility theorem and, consequently, is independent of that assumption. This proof is akin to the proofs of Brauer (3) for (11.3) and (11.4). The latter's proofs place in evidence the limits of the validity of these theorems with respect to varying the reference field Ω:

(11.4) holds for every perfect Ω.

(11.3), in the special case of division algebras, also holds for every perfect Ω.

(11.3), in the general case, holds, if and only if Ω is *regular*, i.e., if Ω has to each algebraic extension of finite degree algebraic extensions of every fixed relative degree.

For reasons of prolixity I must forego developing here the just mentioned proofs of Brauer, and also the proofs of Noether for the same theorems, which will appear in her paper previously mentioned.

For the purposes of II, theorems (11.3) and (11.4) are only needed in the case of algebraic number fields of finite degree.

conclusions may be drawn quite analogously to the proof of (9.2) for the Galois special case.

12. **Classes of similar normal simple algebras and classes of associated factor sets.** Next I develop further contributions to the theory of semi-invariants of crossed products given in (8.7), by following up the relations between the classes of associated factor sets pointed out there as semi-invariants on the one hand, and the classes of similar normal simple algebras on the other hand.

(12.1) *If* $(a) \sim (1)$, *then* $(a, Z) \sim 1$.

It may even be assumed without any restriction that $(a) = (1)$, i.e., that each $a_{S,T} = 1$.

I start from the isomorphic matrix representation $\mathfrak{A}$ of $A = (a, Z)$, furnished in (9.3) by the Z-basis $\mathfrak{u} = (u_T)$ of A. Here I transform the Z-basis $\mathfrak{u}$ to the new Z-basis $\mathfrak{u}C$ of A by means of the substitution with the coefficient matrix

$$C = (z_k^S) \quad (S \text{ rows, } k \text{ columns}),$$

formed with the conjugate bases to a basis z_k of Z as rows. This transformation gives, from (9.3),

(12.1 1) $$a(\mathfrak{u}C) = (\mathfrak{u}C)\overline{A}_a, \text{ where } \overline{A}_a = C^{-1}A_aC.$$

The $\overline{A}_a$ form another isomorphic matrix representation $\overline{\mathfrak{A}}$ of A in Z. Its degree is the degree n of A. Now, due to the assumption $(a) = (1)$, $\overline{\mathfrak{A}}$ even belongs to Ω. Now, from (12.1 1), it follows for an arbitrary R from G, since $u_R^{-1}Cu_R = C^R$ and $u_R^{-1}\overline{A}_a u_R = \overline{A}_a{}^R$, that

(12.1 2) $$a(\mathfrak{u}u_RC^R) = (\mathfrak{u}u_RC^R)\overline{A}_a{}^R.$$

Now, since the $a_{S,T} = 1$,

$$\mathfrak{u}u_RC^R = \left(\sum_P u_Pu_Rz_k{}^{PR}\right) = \left(\sum_P u_{PR}z_k{}^{PR}\right)$$

$$= \left(\sum_Q u_Qz_k{}^Q\right) = \mathfrak{u}C.$$

Hence (12.1 2) changes to

$$a(\mathfrak{u}C) = (\mathfrak{u}C)\overline{A}_a{}^R.$$

Now, by comparison with (12.1 1),

$$\overline{A}_a{}^R = \overline{A}_a.$$

Thus the matrices $\bar{a}_\alpha$ of Z are invariant under each automorphism R of Z. Therefore they really belong to Ω.

Since $\overline{\mathfrak{A}}$ is, like A, of order n^2, it follows that $\overline{\mathfrak{A}} \sim 1$, i.e., also $A \sim 1$.

(12.2) *If* $(a, Z) \sim 1$, *then* $(a) \sim (1)$.

More generally,

(12.3) *if* (a, Z) *has the index* m, *then* $(a^m) \sim (1)$.

Let D be the division algebra similar to $A = (a, Z)$. Then m is the degree of D, and the degree n of A is a multiple $n = rm$ of m.

A may be represented as the algebra of all matrices of degree r in D. Let e_{ik}, as in the proof of (10.1), (10.2), be a complete set of matrix units of A, and $R = e_{11}A$ the right-invariant sub-algebra of A consisting of the first rows of that matrix representation.

R is of order kn, where k is the Z-order of R. On the other hand, the order of R is found, passing through the D-order r of R, to be rm^2. Comparison yields the value

$$k = m$$

for the Z-order of R.

Now let $\mathfrak{r}$ be a Z-basis of R as a one-rowed matrix. By taking the Z-basis representations of the products $\mathfrak{r}u_S$, there results, for each S of G, a system of linear equations

(12.3 1) $$\mathfrak{r}u_S = \mathfrak{r}B_S,$$

where B_S is a matrix in Z. Its degree is the Z-order m of R.

From (12.3 1), it follows further that

$$\mathfrak{r}u_S u_T = \mathfrak{r}B_S u_T = \mathfrak{r}u_T B_S{}^T = \mathfrak{r}B_T B_S{}^T,$$

while, according to (12.3 1), also

$$\mathfrak{r}u_S u_T = \mathfrak{r}u_{ST} a_{S,T} = \mathfrak{r}B_{ST} a_{S,T}.$$

Comparison yields

(12.3 2) $$B_T B_S{}^T = B_{ST} a_{S,T}.^*$$

On account of (8.6), the B_S are likewise regular, i.e., their determinants

* According to (12.3 2), the matrices B_S do not exactly form a matrix representation of G in the usual sense, but they do form a *crossed representation* of G in Z, as Noether calls it.

Such crossed representations were first considered by Speiser (1). In a supplementary paper to this, Schur (1) was first led to the conception of a *factor set* which has become so important nowadays.

The theory of factor sets was then further developed by Brauer (2), first without connection with the theory of algebras. Later Brauer (3) and Noether (in a lecture at the University of Göttingen) subordinated it to the theory of algebras.

$$|B_S| = c_S \neq 0.$$

Hence, by taking determinants, in (12.3 2) it follows that

$$c_T c^T = c_{ST} a^m_{S,T},$$

with elements $c_S \neq 0$ in Z. According to (8.7 2), this means indeed that

$$(a^m) \sim (1).$$

(12·4) *The relation* $(a, Z) \times (\bar{a}, Z) \sim (a\bar{a}, Z)$ *holds.*

In order to represent the elements of the direct product $(a, Z) \times (\bar{a}, Z)$, Z in the second factor is to be replaced by an isomorphic corps $\overline{Z}$ whose elements are to be regarded as linearly independent of those of Z. Let then $A = (a, Z)$, with the Z-basis u_S as in (7.1), (7.2), and accordingly $\overline{A} = (\bar{a}, \overline{Z})$, with the $\overline{Z}$-basis $\bar{u}_S$.

(a) $A \times \overline{A}$ contains $Z \times \overline{Z}$. As a semi-simple commutative algebra $Z \times \overline{Z}$ is, on account of the structure theorems of Wedderburn (1),* a direct sum of corps, and this decomposition is unique apart from the arrangement of the components.† Let $\tilde{Z}$ be one of these component corps and e its modulus, hence $\tilde{Z} = e(Z \times \overline{Z})$. $\tilde{Z}$ contains the sub-corps eZ and $e\overline{Z}$ both isomorphic to Z. As isomorphic sub-corps of the same corps Z these two corps are conjugate. Since they are Galois, they are therefore identical. That means

$$\tilde{Z} = e(Z \times \overline{Z}) = eZ = e\overline{Z}. \tag{12.4 1}$$

Hence, $\tilde{Z}$ is isomorphic to Z. Thus, $Z \times \overline{Z}$ is a direct sum of corps isomorphic to Z, whose number then must be equal to the degree n of Z.‡

The moduli of these n components represent a decomposition of the modulus of $A \times \overline{A}$ in n idempotents orthogonal to each other. This decomposition leads, in a familiar manner,§ to a set of n^2 matrix units in $A \times \overline{A}$, and so to a splitting off from $A \times \overline{A}$ of a complete matrix algebra of order n^2 as a direct factor. The remaining normal simple algebra is isomorphically represented by $e(A \times \overline{A})e$, where e denotes any one of the diagonal matrix units, i.e., any one of these moduli. Accordingly there results

$$A \times \overline{A} \sim \tilde{A}, \text{ with } \tilde{A} = e(A \times \overline{A})e. \tag{12.4 2}$$

(b) The Galois group G of Z is made an automorphism group of $Z \times \overline{Z}$ by

* See also Dickson (1 §§40, 51, 3 §§69, 78).

† See Dickson (1 §24, 3 §53).

‡ These facts may be also obtained in a more complicated but elementary way by studying the decomposition of a generating equation for $e\overline{Z}$ in linear factors of eZ.

§ See Dickson (1 §51, 3 §78), Artin (2).

fixing its automorphisms to keep the single elements of $\overline{Z}$ invariant. Then, under the automorphisms R from G, the idempotent e changes to n idempotents e^R, for each of which, according to (12.4 1),

$$Z^R = e^R(Z \times \overline{Z}) = e^R Z = e^R \overline{Z}$$

is a corps isomorphic to Z, which occurs in $Z \times \overline{Z}$ as a direct summand.

The n idempotents e^R and therefore the n corps Z^R are different from each other. For, from $e^R = e$ it follows that the single elements of $e\overline{Z}$, hence, according to (12.4 1), also those of eZ, and with them those of Z, are invariant under R. This, indeed, is satisfied only if $R = E$.

Now, by reason of the uniqueness of the direct decomposition of $Z \times \overline{Z}$, this decomposition is precisely given by

$$Z \times \overline{Z} = \sum_R Z^R = \sum_R e^R Z. \tag{12.4 3}$$

Accordingly, the elements z^* of $Z \times \overline{Z}$ are uniquely represented in the form

$$z^* = \sum_R e^R z_R, \quad z_R \text{ in } Z. \tag{12.4 4}$$

In particular for the elements $\bar{z}$ in $\overline{Z}$, with regard to their invariance under G, comparison of coördinates yields

$$z_R = z_E{}^R,$$

i.e.,

$$\bar{z} = \sum_R e^R z^R, \quad z \text{ in } Z. \tag{12.4 5}$$

Therein $\bar{z}$ runs through the corps $\overline{Z}$ in an isomorphic correspondence J to the elements z of Z; I denote this by $\bar{z} = z^J$.

Now let $\overline{G}$ be the Galois group of $\overline{Z}$, and let, conversely, the single elements of Z be invariant under $\overline{G}$. For each automorphism S from G, I denote† by S' that automorphism from $\overline{G}$ which corresponds to S by means of the isomorphism J, i.e.,

$$\bar{z}^{S'} = z^{SJ}.$$

Then, the representation (12.4 5) for $\bar{z}^{S'}$ is, on the one hand,

$$\bar{z}^{S'} = \sum_R e^R z^{SR} = \sum_R e^{S^{-1}R} z^R,$$

while, on the other hand, this representation may also be found from (12.4 5) itself, by application of S', to be

† To simplify typography in superscripts, S' is used here rather than $\overline{S}$.

$$\bar{z}^{S'} = \sum_R e^{RS'} z^R.$$

The comparison of these two relations for the elements z_k of a basis of Z yields

$$e^{RS'} = e^{S^{-1}R}. \tag{12.4 6}$$

Now, since u_S is commutative with the elements of $\overline{A}$ and therefore, in particular with the elements of $\overline{Z}$, the transformation by u_S has precisely the same effect as the automorphism S of $Z \times \overline{Z}$. Correspondingly, the transformation by $\bar{u}_S$ has the same effect as the automorphism $\overline{S}$ of $Z \times \overline{Z}$. Therefore in particular, with regard to (12.4 6),

$$\begin{aligned} e^R u_S &= u_S e^{RS}, \\ e^R \bar{u}_S &= \bar{u}_S e^{RS'} = \bar{u}_S e^{S^{-1}R} \end{aligned} \tag{12.4 7}$$

hold.

From the first of these two relations it follows, by the way, that

$$e_{S,T} = u_S^{-1} u_T e^T$$

is a set of n^2 matrix units in $A \times \overline{A}$ corresponding to the e^S as $e_{S,S}$. I do not need this, however, in the following.

(c) Now, according to (12.4 2), $\tilde{A} = e(A \times \overline{A})e$ is to be deduced. The elements a^* of $A \times \overline{A}$ are evidently given by

$$a^* = \sum_{S,T} u_S \bar{u}_T z_{S,T}, \quad z_{S,T} \text{ in } Z \times \overline{Z},$$

and so, with regard to (12.4 4), by

$$a^* = \sum_{S,T} u_S \bar{u}_T e^R z_{R,S,T}, \quad z_{R,S,T} \text{ in } Z,$$

in a unique representation. Therefore $\tilde{A}$ consists of the elements

$$\begin{aligned} \tilde{a} = ea^*e &= \sum_{R,S,T} e u_S \bar{u}_T e^R z_{R,S,T} \\ &= \sum_{R,S,T} u_S \bar{u}_T e^{T^{-1}S} e^R e z_{R,S,T} \end{aligned}$$

(according to (12.4 5))

$$= \sum_S u_S \bar{u}_S e z_{E,S,S}$$

(because of the orthogonality of the e^R according to (12.4 3)).

By setting then

$$\tilde{u}_S = u_S \bar{u}_S, \quad \tilde{z}_S = e z_{E,S,S} \text{ in } \tilde{Z} = eZ,$$

$\tilde{A}$ consists of the elements

$$\tilde{a} = \sum_S \tilde{u}_S \tilde{z}_S, \quad \tilde{z}_S \text{ in } \tilde{Z},$$

in a unique representation on account of the order. This means that the $\tilde{u}_S$ form a $\tilde{Z}$-basis of $\tilde{A}$.

As a consequence of (12.4 7), in addition, for every $\tilde{z} = ez$

$$\tilde{z}\tilde{u}_S = ezu_S\tilde{u}_S = eu_S\tilde{u}_S z^S = u_S\tilde{u}_S ez^S = \tilde{u}_S\tilde{z}^{\tilde{S}},$$

holds, where $\tilde{S}$ denotes that automorphism of $\tilde{Z}$ which corresponds to S by means of the isomorphism $\tilde{Z} = ez$ from Z to $\tilde{Z}$.

Further, it follows obviously that

$$\tilde{u}_S\tilde{u}_T = \tilde{u}_{ST}a_{S,T}\tilde{a}_{S,T}.$$

Therefore,

$$\tilde{A} = (a\tilde{a}, \tilde{Z}).$$

This yields, by (12.4 1) and (12.4 2), the assertion (12.4).

13. **The group of classes of similar normal simple algebras.** The foregoing results, derived in §§9–12, may be stated also in the following manner, as is easily seen:

(13.1) *The classes of similar normal simple algebras A which possess a fixed Galois splitting field Z form an abelian group with respect to direct multiplication.*

This group is isomorphic to the group of classes of associated factor sets (a) for a corps Z, isomorphic to Z, *where multiplication is defined termwise.*

(13.2) *Each element A of this group has a finite exponent l. Indeed, $A^m \sim 1$, if m is the index of A; hence, further, l is a divisor of m.*

Accordingly, of course, *all* classes of normal simple algebras form likewise an abelian group with respect to direct multiplication, in which each element is of finite order. For the existence of the reciprocal element is already guaranteed by (13.1): To $A \sim (a, Z)$, $A^{-1} \sim (a^{-1}, Z)$ is reciprocal. From (7.1), (7.2), by the way, it is easy to see, that the reciprocal A^{-1} may be found simply by inverting the succession of factors, i.e., by passing to the *reciprocal algebra* in the sense of Dickson (1 §12, 3 §20).

Theorems (13.1) and (13.2) were first stated by Brauer (3), although on a somewhat different basis.

As Brauer (3) also states, (13.2) may be strengthened as follows:

(13.3) *The exponent l of A is divisible by each prime divisor p of m.*

Let Z be a Galois splitting field for A and $n = rm$ its degree. From a well known theorem of Sylow†, it follows that Z has a sub-field Σ of such a kind

† See Speiser (2 Satz 67).

that the degree of Z over Σ is a power p^ν, while the degree of Σ is prime to p.

By (11.1), Σ is not a splitting field for A, because its degree is not divisible by m. Therefore A_Σ is not similar to 1. Further, since $A_Z \sim 1$, i.e., since A_Σ has the splitting field Z of degree p^ν over Σ, by (11.1), the index of A_Σ is a power p^μ. By (13.2), therefore, the exponent of A_Σ also is a power p^λ, in particular, $p^\lambda \neq 1$ because A_Σ is not similar to 1.

Now, the exponent l of A is a multiple of the exponent p^λ of A_Σ, because, from $A^l \sim 1$, it follows that

$$(A_\Sigma)^l = (A^l)_\Sigma \sim 1.$$

Moreover, Brauer (3) proved the following important theorem:

(13.4) *Every normal division algebra D is a direct product of normal division algebras whose degrees are powers of different primes.*

Let

$$l = \prod_i p_i^{\lambda_i}$$

be the prime decomposition of the exponent l of D, and

$$q_i \equiv 1 \pmod{p_i^{\lambda_i}}, \quad q_i \equiv 0 \pmod{1/p_i^{\lambda_i}}, \quad \text{hence} \quad \Sigma_i q_i \equiv 1 \pmod{l}.$$

Then, by (13.1), (13.2),

$$D \sim D^{\Sigma_i q_i} = \prod_i D^{q_i} \sim \prod_i D_i,$$

where the

$$D_i \sim D^{q_i} \tag{13.4 1}$$

are normal division algebras with the exponents $p_i^{\lambda_i}$. By (13.2), therefore, the degrees of the D_i are powers $p_i^{\mu_i}$.

Let, more precisely,

$$\prod_i D_i = D \times M_r,$$

where M_r denotes the total matrix algebra of degree r. Comparison of degrees leads to

$$\prod_i p_i^{\mu_i} = mr.$$

On the other hand, every splitting field of D is, by (13.4), also a splitting field for the D_i. Since, in particular, D has, by (11.3), (11.4), splitting fields of degree m,† it follows from (11.1) that each $p_i^{\mu_i}$ is a divisor of m. Therefore also $\prod_i p_i^{\mu_i}$ is a divisor of m. This means that $r = 1$, i.e.,

$$D = \prod_i D_i.$$

† See the remarks in footnote on p. 188.

Hence the assertion (13.4) follows. Finally, the following theorem, which, in connection with the foregoing, goes farther, may be noted:

(13.5) *Every normal division algebra is a direct product of normal division algebras which do not properly contain normal division algebras.*

The proof follows easily from a theorem of Wedderburn (2).

14. **Extension of the reference field.** I shall consider now the behavior of a crossed product when one passes from the reference field Ω to an arbitrary perfect extensional field ϕ.

(14) *The relation* $(a, Z)_\phi \sim (a^\phi, Z^\phi)$ *holds.*

Here, Z^ϕ *denotes the composite of* Z *and* ϕ *considered as a corps over* ϕ, *and* (a^ϕ) *that partial set of* (a) *which corresponds to the automorphisms of* Z^ϕ *with respect to* ϕ.

Let† $A=(a, Z)$ and n be the degree of A.

(a) $A_\phi = A \times \phi$ contains $Z_\phi = Z \times \phi$. As a semi-simple commutative algebra, Z_ϕ is a direct sum of corps. Let $\overline{Z}$ be one of these corps and e its unit, hence $\overline{Z} = eZ_\phi = e(Z \times \phi)$. $\overline{Z}$ arises from its sub-field e^ϕ, isomorphic to ϕ, by adjunction of the elements of the corps eZ, isomorphic to Z. As a corps, $\overline{Z}$ is therefore isomorphic to the composite Z^ϕ of Z and ϕ.‡ Thus, Z_ϕ is a direct sum of corps isomorphic to Z^ϕ, whose number, then, must be k, when h is the degree of Z^ϕ over ϕ and k the complementary divisor of $n=hk$.

As in the proof of (12.4), from this the relation

$$A_\phi \sim \overline{A}, \text{ with } \overline{A} = eA_\phi e, \tag{14.1}$$

results.

(b) The Galois group G of Z is made an automorphism group of Z_ϕ by fixing its automorphisms to keep the single elements of ϕ invariant. Then, under the automorphisms S from G, the idempotent e changes to n idempotents e^S, for each of which $\overline{Z}^S = e^S Z_\phi$ is one of the k direct summands of Z_ϕ.

Now, if P is an automorphism from G with $e^P = e$, the single elements of e^ϕ are invariant under P. Let F be that sub-corps of Z for which eF is contained in e^ϕ;§ then F also is invariant under P. This means that P belongs to the sub-group H of G which corresponds to the sub-corps F of Z according to the fundamental theorem of the Galois theory.‖ Conversely, each automorphism P from H has the property $e^P = e$. Consequently, when S runs

† The proof is in extensive parts analogous to the proof of (12.4).

‡ In the sense of Hasse (8 §18). Notice the difference between *composite* and *direct product.*

§ F is the *Durchschnitt* of Z and ϕ in the same abstract sense as in the conception of the *free composite* (freies Kompositum) Z^ϕ according to Hasse (8 §18).

‖ See, for instance, Hasse (8 §17).

through all automorphisms from G, exactly to the automorphisms from any full residue class HS correspond the same $e^{HS}=e^S$ and the same $\overline{Z}^{HS}=\overline{Z}^S$, and to different residue classes with respect to H correspond different e^S and $\overline{Z}^S$.

H itself furnishes an automorphism group of $\overline{Z}$ with respect to e^ϕ as reference field. H is, indeed, the complete Galois group of $\overline{Z}$ with respect to e^ϕ, since each automorphism of $\overline{Z}$ with respect to e^ϕ reduces to the automorphism of eZ with respect to eF, i.e., of Z with respect to F, contained within it. Consequently, the order of H is equal to the degree h of $\overline{Z}$ over e^ϕ (i.e., of Z^ϕ over ϕ), and therefore the index of H is equal to the complementary divisor k of n.

Among the direct summands $\overline{Z}^S$ of Z_ϕ, furnished by means of the automorphisms S from G, there are, therefore, k that are distinct, i.e., exactly sufficient, according to the foregoing, to make up the total number of direct summands of Z_ϕ. Thus, the direct decomposition of Z_ϕ is given by

$$Z_\phi = \sum_{S \bmod H} \overline{Z}^S = \sum_{S \bmod H} e^S Z_\phi. \tag{14.2}$$

Now, in A_ϕ, the transformation by u_S has precisely the same effect as the automorphism S of Z_ϕ. Therefore we have in particular that

$$eu_S = u_S e^S. \tag{14.3}$$

(c) Now, according to (14.1), $\overline{A}=eA_\phi e$ is to be deduced. The elements a^* of A_ϕ are evidently given by

$$a^* = \sum_S u_S z_S^*, \quad z_S^* \text{ in } Z_\phi,$$

in a unique representation. Therefore $\overline{A}$ consists of the elements

$$\bar{a} = ea^*e = \sum_S eu_S z_S^* e = \sum_S u_S e^S e z_S^*$$

(according to (14.3))

$$= \sum_{P \text{ in } H} u_P e z_P^*$$

(because of the orthogonality of the e^S, corresponding to different residue classes with respect to H, according to (14.2)), hence of the elements

$$\bar{a} = \sum_{P \text{ in } H} u_P \bar{z}_P, \quad \bar{z}_P \text{ in } \overline{Z},$$

in a unique representation (on account of the order). This means that the u_P form a $\overline{Z}$-basis of $\overline{A}$.

In addition, for each P, Q from H, the relations

$$\bar{z}u_P = u_P\bar{z}^P, \text{ for every } \bar{z} \text{ in } \overline{Z},$$

$$u_P u_Q = u_{PQ}a_{P,Q}$$

hold. This means that

$$\overline{A} = (\bar{a}, \overline{Z}),$$

where $(\bar{a})$ denotes the partial set of (a) corresponding to the automorphisms from H. With regard to (14.1), this yields the relation (14) on performing, finally, the isomorphism from $\overline{Z}$ to Z^ϕ.

15. **Specialization to the cyclic case.** I develop, finally, the manner in which the general theory of crossed products presents itself in the special case of a cyclic corps Z. This is precisely the case which matters for the proofs of the Theorems in I.

In this special case, without loss of generality, one need only consider factor sets normalized to a particular simple form, by passing according to (8.7) to a suitable associated factor set. Let S be a generating automorphism of Z, $(\bar{a})$ any factor set, and $\bar{u}_S$ the corresponding Z-basis. I set then

$$u_{S^\mu} = u^\mu \ (\mu = 0, \cdots, n-1), \text{ where } u = \bar{u}_S.$$

This means, indeed, as is easily seen, a substitution of the type (8.7 3). Because $S^n = E$, further,

$$u^n = \alpha \neq 0 \text{ in } Z. \dagger \tag{15.1}$$

The factor set (a), corresponding to the new Z-basis u_{S^μ}, may be expressed then by this α alone, namely

$$a_{S^\mu,S^\nu} = \begin{cases} 1, \text{ if } \mu+\nu < n, \\ \alpha, \text{ if } \mu+\nu \geqq n \end{cases} \qquad (0 \leqq \mu < n,\ 0 \leqq \nu < n). \tag{15.2}$$

The associative condition (8.1) is equivalent to the following fact:

(15.3) *α is an element in Ω.*

(a) From (8.1) it follows, according to (15.2), that

$$\alpha^S = a^S_{S,S^{n-1}} = \frac{a_{S^{n-1},S}a_{S,E}}{a_{E,S}} = \frac{\alpha \cdot 1}{1} \doteq \alpha,$$

i.e., (15.3).

† Dickson (2, 3 Kap. III, 4), in his investigations on division algebras which revert, indeed, to the theory of crossed products, always introduces such normalisations. His investigations are then concerned with pointing out the conditions for associativity and division algebras, and with the realisation of these conditions. The conditions, however, turn out rather complicated, by reason of this special normalisation. It is precisely by dropping all normalisation that Noether obtains both the fine simplicity and great generality of her theory.

(b) Conversely, from (15.3), the associativity of (a, Z) follows directly.†

(15.1), (15.3) reduce exactly to the definition of a cyclic algebra $A = (\alpha, Z, S)$ given in §1. Hence, in the first place, the facts (1.3), (1.4) are subordinated to the theorems (9.1), (8.5) of the general theory. Notice that these facts are even proved for arbitrary perfect reference fields Ω, not only for algebraic number fields of finite degree, as was supposed in I.

Furthermore:

(15.4) $(a)\sim(1)$, *i.e.*, $A\sim 1$ *holds, if and only if* α *is a norm from* Z.

(a) $(a)\sim(1)$ means, according to (8.7 2), that

$$(15.4\ 1) \qquad a_{S^\mu, S^\nu} = \frac{c_{S^\nu} c_{S^\mu}^{S^\nu}}{c^{S^{\mu+\nu}}}, \text{ with elements } c_{S^\mu} \neq 0 \text{ in } Z.$$

From this it follows, in particular, by multiplying over ν, while $\mu = 1$ is fixed, and taking (15.2) into account, that

$$(15.4\ 2) \qquad \alpha = \mathrm{N}(c), \text{ with } c = c_S \text{ in } Z.$$

(b) Conversely, from (15.4 2), one deduces easily (15.4 1), by setting

$$c_S = \prod_{\rho=0}^{\mu-1} c^{S^\rho}.$$

By (15.4), as is easily shown, the fact (2.1) is subordinated to the theorem (8.7) of the general theory, and further Dickson's criterion (1.5) to the theorems (12.3), (11.1) of the general theory. Notice again that these facts are are even proved for arbitrary perfect reference fields Ω.

Finally, I note how the general theorem (14) presents itself in the cyclic special case:

(15.5) *For an arbitrary perfect extension field* ϕ *of* Ω

$$(\alpha, Z, S)_\phi = (\alpha, Z^\phi, S_\phi)$$

holds, where S_ϕ *denotes the least power of* S *which represents an automorphism of the composite* Z^ϕ *with respect to* ϕ.

According to (14),

$$(\alpha, Z, S)_\phi = (a, Z)_\phi = (a^\phi, Z^\phi)$$

holds. Here (a^ϕ) denotes that partial set of (a) which corresponds to the automorphisms of Z^ϕ with respect to ϕ. These automorphisms are the powers of S_ϕ. Thus if $S_\phi = S^k$ and $n = hk$, the factor set (a^ϕ), according to (15.2), consists of

† Of course, this may also be proved by calculating (8.1) from (15.2).

$$a_{S_\phi^\mu, S_\phi^\nu} = a_{S^{\mu k}, S^{\nu k}} = \begin{cases} 1, \text{ if } \mu + \nu < h, \\ \alpha, \text{ if } \mu + \nu \geqq h \end{cases} \qquad (0 \leqq \mu < h, 0 \leqq \nu < h).$$

Since h is the degree and S_ϕ a generating automorphism of the Galois group of the cyclic corps Z^ϕ with respect to ϕ, the assertion (15.5) follows from this.

III. Proofs of the theorems in I

16. $\mathfrak{P}$-adic extension of a normal simple algebra. In III again, as in I, the reference field Ω is assumed to be an algebraic number field of finite degree.

The proofs of the Theorems in I depend on passing from Ω to the $\mathfrak{p}$-adic extension fields $\Omega_\mathfrak{p}$ for the prime spots $\mathfrak{p}$ of Ω, and, in accordance with this, from a normal simple algebra A to its $\mathfrak{p}$-adic extensions $A_\mathfrak{p}$ $(= A \times \Omega_\mathfrak{p} = A_{\Omega_\mathfrak{p}})$.

As I have shown in a previous paper,† the division algebra $D_\mathfrak{p}$, similar to $A_\mathfrak{p}$, has an *arithmetically distinguished cyclic generation*, namely one such that its cyclic generation corps is the uniquely determined *unramified* corps $W^\mathfrak{p}$ of degree $m_\mathfrak{p}^*$ over $\Omega_\mathfrak{p}$, where $m_\mathfrak{p}^*$ denotes the index of $A_\mathfrak{p}$, i.e., the degree of $D_\mathfrak{p}$.‡

For characterising the cyclic algebras which arise from $W^\mathfrak{p}$ as cyclic generation corps, I use the generalisation of the norm residue symbol to the $\mathfrak{p}$-adic corps $W^\mathfrak{p}$. In order to define this symbol for a *finite* prime spot (prime ideal) let, analogous to (3.6), $(W^\mathfrak{p}/\mathfrak{p})$ denote that uniquely determined automorphism of $W^\mathfrak{p}$ which satisfies the relation

(16.1) $$w_\mathfrak{p}^{(W^\mathfrak{p}/\mathfrak{p})} \equiv w_\mathfrak{p}^{N(\mathfrak{p})} \pmod{\mathfrak{p}}, \textit{ for every integer } w_\mathfrak{p} \textit{ in } W^\mathfrak{p}.$$

Analogous to (3.7), I define then

(16.2) $$\left(\frac{\beta_\mathfrak{p},\ W^\mathfrak{p}}{\mathfrak{p}}\right) = \left(\frac{W^\mathfrak{p}}{\mathfrak{p}}\right)^{-\rho},$$

where $\beta_\mathfrak{p}$ *is a number in* $\Omega_\mathfrak{p}$ *divisible exactly by* $\mathfrak{p}^\rho$. The symbol so defined has, analogous to (3.1), (3.2), the following properties:

(16.3) $$\left(\frac{\beta_\mathfrak{p},\ W^\mathfrak{p}}{\mathfrak{p}}\right) = E$$

holds, if and only if $\beta_\mathfrak{p}$ *is a norm from* $W^\mathfrak{p}$;

(16.4) $$\left(\frac{\beta_\mathfrak{p},\ W^\mathfrak{p}}{\mathfrak{p}}\right)\left(\frac{\bar{\beta}_\mathfrak{p},\ W^\mathfrak{p}}{\mathfrak{p}}\right) = \left(\frac{\beta_\mathfrak{p}\bar{\beta}_\mathfrak{p},\ W^\mathfrak{p}}{\mathfrak{p}}\right).$$

† Hasse (14 §§2–5).

‡ This is also true for infinite prime spots $\mathfrak{p}$, not yet considered in Hasse (14). $\Omega_\mathfrak{p}$ is then the field of all real numbers, and $W^\mathfrak{p}$ must be interpreted as the single corps of degree $m_\mathfrak{p}^*$ $(= 1$ or $2)$ over $\Omega_\mathfrak{p}$. For, over the field of all real numbers, there is indeed, except this field itself $(m_\mathfrak{p}^* = 1)$, only one division algebra, i.e., the common quaternion algebra $(m_\mathfrak{p}^* = 2)$, and for this algebra the corps of all complex numbers is evidently a cyclic generation corps.

For, $\beta_\mathfrak{p}$ is a norm from $W^\mathfrak{p}$, if and only if ρ is divisible by $m_\mathfrak{p}^*$.† For an *infinite* prime spot $\mathfrak{p}$ the symbol $(\beta_\mathfrak{p}, W^\mathfrak{p}/\mathfrak{p})$ is completely fixed already by imposing the property (16.3) for, because $m_\mathfrak{p}^* = 1$ or 2, no distinction of different non-residue sorts is required.

Further, I define again, analogous to (6.1),

$$\left(\frac{\beta_\mathfrak{p}, W^\mathfrak{p}, R_\mathfrak{p}}{\mathfrak{p}}\right) \equiv \frac{\mu_\mathfrak{p}^*}{m_\mathfrak{p}^*} \pmod 1, \quad \text{if} \quad \left(\frac{\beta_\mathfrak{p}, W^\mathfrak{p}}{\mathfrak{p}}\right) = R_\mathfrak{p}^{\mu_\mathfrak{p}^*}. \tag{16.5}$$

Here $R_\mathfrak{p}$ denotes a generating automorphism of $W^\mathfrak{p}$.

Then, analogous to (2.1) and (4.4) (but exceeding the latter), the following is true:

(16.6) *The identity*

$$(\beta_\mathfrak{p}, W^\mathfrak{p}, R_\mathfrak{p}) = (\bar{\beta}_\mathfrak{p}, W^\mathfrak{p}, \overline{R}_\mathfrak{p}) \tag{16.6 1}$$

holds, if and only if

$$\left(\frac{\beta_\mathfrak{p}, W^\mathfrak{p}, R_\mathfrak{p}}{\mathfrak{p}}\right) \equiv \left(\frac{\bar{\beta}_\mathfrak{p}, W^\mathfrak{p}, \overline{R}_\mathfrak{p}}{\mathfrak{p}}\right) \pmod 1. \tag{16.6 2}$$

(a) From (16.6 1) it follows, by means of (2.1), that

$$\bar{\beta}_\mathfrak{p} \equiv \beta_\mathfrak{p}^\mu \mathrm{N}(c_\mathfrak{p}), \text{ with } c_\mathfrak{p} \text{ in } W^\mathfrak{p}, \text{ where } \overline{R}_\mathfrak{p} = R_\mathfrak{p}^\mu. \tag{16.6 3}$$

This leads, by using (16.3), (16.4), as in the proof of (4.4), to the validity of (16.6 2).

(b) From (16.6 2) by using (16.3), (16.4), first (16.6 3) follows, and thence (16.6 1) by means of (2.1).

If W is a cyclic corps of degree n over Ω in which $\mathfrak{p}$ is unramified and splits into prime divisors $\mathfrak{P}$ of degree $m_\mathfrak{p}^*$, the $\mathfrak{P}$-adic corps corresponding to these $\mathfrak{P}$ are isomorphic to $W^\mathfrak{p}$. Then, there is the following connection between the norm residue symbol for $W^\mathfrak{p}$, defined in (16.2), and the norm residue symbol for W with respect to $\mathfrak{p}$, defined in (3.7):

$$\left(\frac{\beta, W}{\mathfrak{p}}\right) = \left(\frac{\beta, W^\mathfrak{p}}{\mathfrak{p}}\right). \tag{16.7}$$

This follows from (3.10) on the one hand and (16.2) on the other hand, by observing that the automorphism $(W/\mathfrak{p})$ of W, normalised according to (3.6), furnishes the automorphism $(W^\mathfrak{p}/\mathfrak{p})$ of $W^\mathfrak{p}$, normalised according to (16.1).‡

The automorphisms of $W^\mathfrak{p}$ are furnished precisely by the automorphisms

† See for instance Hasse (14 Satz 27).

‡ For infinite prime spots, (16.7) holds already by reason of (16.3).

from the decomposition group of the prime divisors $\mathfrak{P}$.† Since this decomposition group has as its order the degree $m_{\mathfrak{p}}^*$ of the prime divisors $\mathfrak{P}$, it is generated by $R_{\mathfrak{p}}^{n/m_{\mathfrak{p}}^*}$, where R is a generating automorphism of W. Hence it follows from (16.7), by (16.5), that

$$\left(\frac{\beta, W, R}{\mathfrak{p}}\right) \equiv \left(\frac{\beta, W^{\mathfrak{p}}, R^{n/m_{\mathfrak{p}}^*}}{\mathfrak{p}}\right) \pmod 1. \tag{16.8}$$

17. **Proof of Theorem 1, (i).** Let

$$A = (\alpha, Z, S) \tag{17.1}$$

be a cyclic algebra of degree n, and

$$\left(\frac{\alpha, Z, S}{\mathfrak{p}}\right) \equiv \frac{\nu_{\mathfrak{p}}}{n} \equiv \frac{\mu_{\mathfrak{p}}}{m_{\mathfrak{p}}} \pmod 1, \quad (\mu_{\mathfrak{p}}, m_{\mathfrak{p}}) = 1, \tag{17.2}$$

the corresponding symbols, according to (6.1), (6.2), which are semi-invariant, as has been shown in (4.4).

Further, let for a prime spot $\mathfrak{p}$ of Ω, according to the references given in §16,

$$A_{\mathfrak{p}} \sim D_{\mathfrak{p}} = (\beta_{\mathfrak{p}}, W^{\mathfrak{p}}, R_{\mathfrak{p}}) \tag{17.3}$$

be‡ an arithmetically distinguished cyclic generation of the division algebra $D_{\mathfrak{p}}$, similar to $A_{\mathfrak{p}}$, and

$$\left(\frac{\beta_{\mathfrak{p}}, W^{\mathfrak{p}}, R_{\mathfrak{p}}}{\mathfrak{p}}\right) \equiv \frac{\mu_{\mathfrak{p}}^*}{m_{\mathfrak{p}}^*} \pmod 1 \tag{17.4}$$

the corresponding symbol, according to (16.5), which is semi-invariant, as has been shown in (16.6). With this, moreover,

$$(\mu_{\mathfrak{p}}^*, m_{\mathfrak{p}}^*) = 1\S \tag{17.4 1}$$

holds.

I shall, then, prove the fundamental fact

$$\left(\frac{\alpha, Z, S}{\mathfrak{p}}\right) \equiv \left(\frac{\beta_{\mathfrak{p}}, W^{\mathfrak{p}}, R_{\mathfrak{p}}}{\mathfrak{p}}\right) \pmod 1. \tag{17.5}$$

in particular

† See Hasse (11, 13 §7).

‡ More exactly "the uniquely determined," namely in the sense of semi-invariance, i.e., apart from substitutions of type (2.1 2).

§ See Hasse (14 §4). By means of (16.1), (16.2), (16.4), indeed, $\mu_{\mathfrak{p}}^*$ turns out to be the negative reciprocal to the residue class r there. For infinite prime spots $\mathfrak{p}$, (17.4 1) is again already true by (16.3).

(17.5 1) $$m_\mathfrak{p} = m_\mathfrak{p}^*.$$

This fact furnishes at once the proof of the assertion (i) in Theorem 1. For, it reduces the semi-invariant symbol (17.2), belonging to A and $\mathfrak{p}$ in the cyclic generation (17.1), to the semi-invariant symbol (17.4), belonging to $A_\mathfrak{p}$ in its arithmetically distinguished cyclic representation (17.3), and so places in evidence the total-invariance of the former symbol.

Moreover, (17.5) gives a formation rule and an interpretation for the invariants $((\alpha, Z, S)/\mathfrak{p})$ which do not refer to a casual cyclic generation, as their definition does.

Proof of (17.5). A. The proof of (17.5 1) which must first be given depends upon the comparison of the arithmetically distinguished cyclic representation (17.3) of $A_\mathfrak{p}$ with the cyclic representation

(17.6) $$A_\mathfrak{p} \sim (\alpha, Z^\mathfrak{p}, S_\mathfrak{p})$$

of $A_\mathfrak{p}$ which follows from (17.1) according to (15.5). Here $Z^\mathfrak{p} = Z^{\Omega_\mathfrak{p}}$ denotes the composite of Z and $\Omega_\mathfrak{p}$. It is isomorphic to the $\mathfrak{P}$-adic corps $Z_\mathfrak{P}$ corresponding to the prime divisors $\mathfrak{P}$ of $\mathfrak{p}$ in Z. Further, $S_\mathfrak{p}$ denotes the least power of S effecting an automorphism of $Z^\mathfrak{p}$. Since the Galois group of $Z^\mathfrak{p}$ with respect to $\Omega_\mathfrak{p}$ is given precisely by the decomposition group of the prime divisors $\mathfrak{P}$, $S_\mathfrak{p}$ is the least power of S which is a (generating) element of this decomposition group.

I now calculate the exponent of $A_\mathfrak{p}$, first from (17.6) on the one hand, and then from (17.3) on the other hand, by means of (12.1), (12.2), (12.4).

As the order of the factor set belonging to (17.6), this exponent is, by (15.4), the exponent of the least power of α which is a norm from $Z^\mathfrak{p}$, hence, by (3.1), the order of $((\alpha, Z)/\mathfrak{p})$, and so, by (17.2) (as already by (6.3)), equal to $m_\mathfrak{p}$.

As the order of the factor set belonging to (17.3), that exponent is, by (15.4), the exponent of the least power of $\beta_\mathfrak{p}$ which is a norm from $W^\mathfrak{p}$, hence, by (16.3), the order of $((\beta_\mathfrak{p}, W^\mathfrak{p})/\mathfrak{p})$, and so, by (17.4), (17.4 1), equal to $m_\mathfrak{p}^*$.

Comparison yields, indeed, (17.5 1).

Notice that the last conclusion implies the following:

(17.7) *The index $m_\mathfrak{p}^*$ of $A_\mathfrak{p}$ is the same as the exponent of $A_\mathfrak{p}$ and equal to the order $m_\mathfrak{p}$ of* $((\alpha, Z)/\mathfrak{p})$.

From this, in particular, one obtains the following fact, which will be repeatedly applied in the sequel:

(17.7 1) $A_\mathfrak{p} \sim 1$ *holds, if and only if* $((\alpha, Z)/\mathfrak{p}) = E$. The latter may also be derived immediately from (3.1) and (15.4).

B. (a) In order to give the full proof of (17.5), I must take a round-about way, for the reasons already mentioned after (3.1), (3.2).

Let α_0 and $\mathfrak{q}$ be determined according to (3.3)–(3.5). I consider, then, instead of (17.1) the modified algebra

$$A^0 = (\alpha_0, Z, S). \tag{17.8}$$

By (3.7), (3.9), (3.10), for the corresponding norm residue symbols we have that

$$\left(\frac{\alpha, Z}{\mathfrak{p}}\right) = \left(\frac{\alpha_0, Z}{\mathfrak{p}}\right) = \left(\frac{Z}{\mathfrak{q}}\right) = \left(\frac{\alpha_0, Z}{\mathfrak{q}}\right)^{-1}, \tag{17.9}$$

in particular, that

$$\left(\frac{\alpha, Z, S}{\mathfrak{p}}\right) \equiv -\left(\frac{\alpha_0, Z, S}{\mathfrak{p}}\right) \pmod 1, \tag{17.10}$$

$$\left(\frac{\alpha_0, Z}{\mathfrak{r}}\right) = E, \tag{17.11}$$

for each prime spot $\mathfrak{r} \neq \mathfrak{p}, \mathfrak{q}$ of Ω.

I develop next several consequences from these relations.

(i) From (17.8), by (15.5),

$$A_{\mathfrak{p}}^0 \sim (\alpha_0, Z^{\mathfrak{p}}, S_{\mathfrak{p}}) \tag{17.12}$$

follows, where $S_{\mathfrak{p}}$ is defined as in (17.6). Now, because of the first relation in (17.9) and by (3.1), (3.2), α_0 differs from α only by a norm from $Z^{\mathfrak{p}}$. Hence it follows, by (2.1) from (17.6) and (17.12), that

$$A_{\mathfrak{p}}^0 = A_{\mathfrak{p}}. \tag{17.13}$$

This means that the modification performed on A does not imply any modification on $A_{\mathfrak{p}}$.

(ii) According to (3.3)–(3.5), $\mathfrak{q}$ is not a divisor of the conductor $\mathfrak{f}$ of Z. Hence $\mathfrak{q}$ is unramified in Z. On account of (17.9), further, the order of the generating element $(Z/\mathfrak{q})$ of the decomposition group of the prime divisors $\mathfrak{Q}$ of $\mathfrak{q}$ in Z, i.e., the degree of the prime divisors $\mathfrak{Q}$, is equal to the order $m_{\mathfrak{p}}$ of $((\alpha, Z)/\mathfrak{p})$. Hence $Z^{\mathfrak{q}} = W^{\mathfrak{q}}$ is the unramified corps of degree $m_{\mathfrak{p}}$ over $\Omega_{\mathfrak{q}}$. The analogue to (17.6) for A^0 and $\mathfrak{q}$ instead of A and $\mathfrak{p}$ is therefore

$$A_{\mathfrak{q}}^0 \sim (\alpha_0, W^{\mathfrak{q}}, S^{n/m_{\mathfrak{p}}}). \tag{17.14}$$

Further, by (16.6),

$$\left(\frac{\alpha_0, Z, S}{\mathfrak{q}}\right) \equiv \left(\frac{\alpha_0, W^{\mathfrak{q}}, S^{n/m_{\mathfrak{p}}}}{\mathfrak{q}}\right) \pmod 1 \tag{17.15}$$

holds.

(iii) From (17.11), it follows by (17.7 1) that

$$A_{\mathfrak{r}}^{0} \sim 1. \tag{17.16}$$

From (17.10), (17.15), it follows for the symbol $((\alpha, Z, S)/\mathfrak{p})$ to be investigated that

$$\left(\frac{\alpha, Z, S}{\mathfrak{p}}\right) \equiv -\left(\frac{\alpha_0, W^{\mathfrak{q}}, S^{n/m_{\mathfrak{p}}}}{\mathfrak{q}}\right) \pmod 1. \tag{17.17}$$

(b) Now, let ϕ be a cyclic extension field of degree $m_{\mathfrak{p}}$ with the property that $\mathfrak{p}$ and $\mathfrak{q}$ remain prime in ϕ, and therefore become of degree $m_{\mathfrak{p}}$.† I show, then, that ϕ is a splitting field for A^0.

For this purpose, I must consider A^0. According to (15.5),

$$A_{\phi}^{0} \sim (\alpha_0, Z^{\phi}, S_{\phi}). \tag{17.18}$$

(i) On account of the choice of ϕ, $\phi_{\mathfrak{p}}$ is the uniquely determined unramified field of degree $m_{\mathfrak{p}}$ over $\Omega_{\mathfrak{p}}$, hence isomorphic to the corps $W^{\mathfrak{p}}$ in (17.3); this is seen from the fact that, by (17.5 1), $m_{\mathfrak{p}} = m_{\mathfrak{p}}^{*}$, as has already been stated in A. According to (9.2), therefore, $\phi_{\mathfrak{p}}$ is a splitting field for $A_{\mathfrak{p}}$, hence, by (17.13), for $A_{\mathfrak{p}}^{0}$. From this it follows that

$$(A_{\phi}^{0})_{\mathfrak{p}} = (A^0 \times \phi)_{\mathfrak{p}} = A_{\mathfrak{p}}^{0} \times \phi_{\mathfrak{p}} \sim 1.$$

Hence, by (17.7 1), it holds for the cyclic representation (17.18) that

$$\left(\frac{\alpha_0, Z^{\phi}}{\mathfrak{p}}\right) = E. \tag{17.19}$$

(ii) For the prime spots $\mathfrak{r}' \neq \mathfrak{p}, \mathfrak{q}$ of ϕ it is also true, on account of (17.16), that

$$(A_{\phi}^{0})_{\mathfrak{r}'} = (A^0 \times \phi)_{\mathfrak{r}'} = A_{\mathfrak{r}}^{0} \times \phi_{\mathfrak{r}'} \sim 1.$$

This yields, by (17.7 1),

$$\left(\frac{\alpha_0, Z^{\phi}}{\mathfrak{r}'}\right) = E, \tag{17.20}$$

for each prime spot $\mathfrak{r}' \neq \mathfrak{p}, \mathfrak{q}$ of ϕ.

(iii) From (17.19), (17.20) it follows, by means of the law of reciprocity (3.8), for the only remaining prime ideal $\mathfrak{q}$ of ϕ that

$$\left(\frac{\alpha_0, Z^{\phi}}{\mathfrak{q}}\right) = E. \tag{17.21}$$

† The existence of such a field will be proved at another place in addition to the existence theorems in Hasse (5, 6, 10).

Now, from (17.19)–(17.21), it follows by (3.11) that α_0 is a norm from Z^{ϕ}. This means then, by (15.4), that $A_{\phi}^{0} \sim 1$. Thus ϕ is, indeed, a splitting field for A^0.

According to (10.2), there is therefore a cyclic representation

$$A^0 \sim (\beta, W, R), \tag{17.22}$$

where W is a corps isomorphic to ϕ and R a generating automorphism of W. Here we have, on account of (17.16), by (17.7 1), that

$$\left(\frac{\beta, W}{\mathfrak{r}}\right) = E,$$

for each prime spot $\mathfrak{r} \neq \mathfrak{p}, \mathfrak{q}$ of Ω. Consequently, by the law of reciprocity (3.8),

$$\left(\frac{\beta, W}{\mathfrak{p}}\right) = \left(\frac{\beta, W}{\mathfrak{q}}\right)^{-1},$$

i.e.,

$$\left(\frac{\beta, W, R}{\mathfrak{p}}\right) \equiv -\left(\frac{\beta, W, R}{\mathfrak{q}}\right) \pmod 1. \tag{17.23}$$

Now, since $\mathfrak{p}$ and $\mathfrak{q}$ according to the choice of ϕ remain prime also in W and so the corresponding decomposition groups coincide with the full Galois group of W, (17.22) implies, analogous to (17.6),

$$A_{\mathfrak{p}}^{0} \sim (\beta, W^{\mathfrak{p}}, R), \quad A_{\mathfrak{q}}^{0} \sim (\beta, W^{\mathfrak{q}}, R), \tag{17.24}$$

where $W^{\mathfrak{p}}$, $W^{\mathfrak{q}}$ signify as above the unramified corps of degree $m_{\mathfrak{p}}$ over $\Omega_{\mathfrak{p}}$, $\Omega_{\mathfrak{q}}$. Also, by (16.8),

$$\left(\frac{\beta, W, R}{\mathfrak{p}}\right) \equiv \left(\frac{\beta, W^{\mathfrak{p}}, R}{\mathfrak{p}}\right), \quad \left(\frac{\beta, W, R}{\mathfrak{q}}\right) \equiv \left(\frac{\beta, W^{\mathfrak{q}}, R}{\mathfrak{q}}\right) \pmod 1. \tag{17.25}$$

(17.24), (17.13), (17.3) on the one hand, and (17.24), (17.14) on the other hand imply the identities

$$(\beta, W^{\mathfrak{p}}, R) = (\beta_{\mathfrak{p}}, W^{\mathfrak{p}}, R_{\mathfrak{p}}), \quad (\beta, W^{\mathfrak{q}}, R) = (\alpha_0, W^{\mathfrak{q}}, S^{n/m_{\mathfrak{p}}}).$$

Now, these identities imply, by (16.6),

$$\left(\frac{\beta, W^{\mathfrak{p}}, R}{\mathfrak{p}}\right) \equiv \left(\frac{\beta_{\mathfrak{p}}, W^{\mathfrak{p}}, R_{\mathfrak{p}}}{\mathfrak{p}}\right), \quad \left(\frac{\beta, W^{\mathfrak{q}}, R}{\mathfrak{q}}\right) \equiv \left(\frac{\alpha_0, W^{\mathfrak{q}}, S^{n/m_{\mathfrak{p}}}}{\mathfrak{q}}\right) \pmod 1. \tag{17.26}$$

From (17.23), (17.25), and (17.26) together,

$$\left(\frac{\beta_{\mathfrak{p}}, W^{\mathfrak{p}}, R_{\mathfrak{p}}}{\mathfrak{p}}\right) \equiv -\left(\frac{\alpha_0, W^{\mathfrak{q}}, S^{n/m_{\mathfrak{p}}}}{\mathfrak{q}}\right) \pmod 1 \tag{17.27}$$

follows. Now, comparison of (17.17) with (17.27) proves the assertion (17.5).

18. **Proof of Theorem 2.** Before I pass to the proof of the assertion (ii) in Theorem 1, I shall prove first Theorem 2.

The proof depends on the following analogous fact for $\mathfrak{p}$-adic algebras:

(18.1) *For a normal simple algebra $A_\mathfrak{p}$ over $\Omega_\mathfrak{p}$, a cyclic corps $Z^\mathfrak{p}$ is a cyclic representation corps, if and only if the degree $n_\mathfrak{p}$ of $Z^\mathfrak{p}$ is a multiple of the index $m_\mathfrak{p}$ of $A_\mathfrak{p}$.*

(a) The necessity of this condition follows immediately from the fact that the field, isomorphic to the cyclic representation corps $Z^\mathfrak{p}$ of $A^\mathfrak{p}$, is, by (9.2), a splitting field for $A_\mathfrak{p}$, and therefore its degree $n_\mathfrak{p}$ is, by (11.1), a multiple of the index $m_\mathfrak{p}$ of $A_\mathfrak{p}$.

(b) Now I show that the condition is sufficient.

For the sub-group of the norms from $Z^\mathfrak{p}$ in $\Omega_\mathfrak{p}$, the quotient-group is isomorphic to the Galois group of $Z^\mathfrak{p}$ with respect to $\Omega_\mathfrak{p}$,† hence cyclic of order $n_\mathfrak{p}$. Therefore, if $n_\mathfrak{p}$ is a multiple of $m_\mathfrak{p}$, there exists a number $\alpha_\mathfrak{p}$ in $\Omega_\mathfrak{p}$ whose order with respect to that norm group is precisely $m_\mathfrak{p}$ and hence for which precisely $\alpha_\mathfrak{p}^{m_\mathfrak{p}}$ is, as the least power, a norm from $Z^\mathfrak{p}$. Hence, by (13.1) and (15.4), the cyclic algebra

$$\overline{A}_\mathfrak{p} = (\alpha_\mathfrak{p}, Z^\mathfrak{p}, S_\mathfrak{p}), \tag{18.1 1}$$

where $S_\mathfrak{p}$ denotes a generating automorphism of $Z^\mathfrak{p}$, has the exponent $m_\mathfrak{p}$. According to (17.7), its index is also $m_\mathfrak{p}$. Consequently, in the arithmetically distinguished cyclic representation

$$\overline{A}_\mathfrak{p} \sim (\bar{\beta}_\mathfrak{p}, W^\mathfrak{p}, R_\mathfrak{p}) \tag{18.1 2}$$

of $\overline{A}_\mathfrak{p}$, there occurs the same unramified corps $W^\mathfrak{p}$, as in the arithmetically distinguished cyclic representation

$$A_\mathfrak{p} \sim (\beta_\mathfrak{p}, W^\mathfrak{p}, R_\mathfrak{p}) \tag{18.1 3}$$

of $A_\mathfrak{p}$. Then, for the semi-invariant symbols corresponding to the cyclic representations (18.1 2), (18.1 3), a relation

$$\left(\frac{\beta_\mathfrak{p}, W^\mathfrak{p}, R_\mathfrak{p}}{\mathfrak{p}}\right) \equiv \kappa\left(\frac{\bar{\beta}_\mathfrak{p}, W^\mathfrak{p}, R_\mathfrak{p}}{\mathfrak{p}}\right) \equiv \left(\frac{\bar{\beta}_\mathfrak{p}^\kappa, W^\mathfrak{p}, R_\mathfrak{p}}{\mathfrak{p}}\right) \pmod 1 \tag{18.1 4}$$

holds, with a κ prime to $m_\mathfrak{p}$.

Now, (18.1 1), (18.1 2) imply, by (13.1) and (15.4),

$$(\bar{\beta}_\mathfrak{p}^\kappa, W^\mathfrak{p}, R_\mathfrak{p}) \sim \overline{A}_\mathfrak{p}^\kappa \sim (\alpha_\mathfrak{p}^\kappa, Z^\mathfrak{p}, S_\mathfrak{p}). \tag{18.1 5}$$

On the other hand it follows, from (18.1 4) by (16.6), that

† See Hasse (12).

(18.1 6) $$(\beta_\mathfrak{p}, W^\mathfrak{p}, R_\mathfrak{p}) = (\bar{\beta}_\mathfrak{p}^\kappa, W^\mathfrak{p}, R_\mathfrak{p}).$$

From (18.1 3), (18.1 5), (18.1 6) together,

$$A_\mathfrak{p} \sim (\alpha_\mathfrak{p}^\kappa, Z^\mathfrak{p}, S_\mathfrak{p})$$

follows. Hence $Z^\mathfrak{p}$ is indeed a cyclic representation corps for $A_\mathfrak{p}$.

I pass now to the proof of Theorem 2.

(a) If Z is a cyclic representation corps for A, then for each $\mathfrak{p}$, by (17.6), $Z^\mathfrak{p}$ is a cyclic representation corps for $A_\mathfrak{p}$. Hence, by (18.1), the degree of $Z^\mathfrak{p}$ over $\Omega_\mathfrak{p}$, i.e., the $\mathfrak{p}$-degree $n_\mathfrak{p}$ of Z, is a multiple of the index of $A_\mathfrak{p}$, i.e., by (17.7), of the $\mathfrak{p}$-index $m_\mathfrak{p}$ of A. Thus the necessity of the condition in Theorem 2 follows.

(b) In order to prove also the sufficiency of that condition, it need, with regard to (10.2), only be shown that a cyclic field Z' of degree n' is a splitting field for the cyclically representable algebra

$$A = (\alpha, Z, S),$$

if for each $\mathfrak{p}$ the $\mathfrak{p}$-degree $n_\mathfrak{p}$ of Z' is a multiple of the $\mathfrak{p}$-index $m_\mathfrak{p}$ of A, hence, if the degree $n_\mathfrak{p}$ of the $\mathfrak{P}'$-adic extension fields $Z'_{\mathfrak{P}'}$, corresponding to the prime divisors $\mathfrak{P}'$ of $\mathfrak{p}$ in Z', is a multiple of the index $m_\mathfrak{p}$ of $A_\mathfrak{p}$.

Now, let Z' be a cyclic field with this property. I must, then, consider $A_{Z'}$. By (15.4),

(18.2) $$A_{Z'} \sim (\alpha, Z^{Z'}, S_{Z'}).$$

The assumption concerning Z' implies, by (18.1), that for each $\mathfrak{p}$ a corps, isomorphic to Z', is a cyclic representation corps for $A_\mathfrak{p}$. Hence, according to (9.2), $Z'_{\mathfrak{P}'}$ itself is a splitting field for $A_\mathfrak{p}$.

Now it follows, quite analogously to the above dealing with (17.18), that

$$(A_{Z'})_{\mathfrak{P}'} = (A \times Z')_{\mathfrak{P}'} = A_\mathfrak{p} \times Z'_{\mathfrak{P}'} \sim 1.$$

Hence, by (17.7 1), for the cyclic representation (18.2), we have

$$\left(\frac{\alpha, Z^{Z'}}{\mathfrak{P}'}\right) = E, \text{ for each prime spot } \mathfrak{P}' \text{ of } Z'.$$

From this it follows just as above, due to (3.11), and (15.4), that

$$A \sim 1.$$

Thus Z' is indeed a splitting field for A.

19. **Proof of Theorem 1, (ii).** Let

(19.1) $$A = (\alpha, Z, S),$$

(19.2) $$\overline{A} = (\bar{\alpha}, \overline{Z}, \bar{S})$$

be two cyclic algebras of degrees n, $\bar{n}$, and $\mathfrak{p}$-indices $m_\mathfrak{p}$, $\bar{m}_\mathfrak{p}$. Further suppose

$$\left(\frac{\alpha, Z, S}{\mathfrak{p}}\right) \equiv \left(\frac{\bar{\alpha}, \overline{Z}, \bar{S}}{\mathfrak{p}}\right) \pmod 1 \text{ for each } \mathfrak{p}, \tag{19.3}$$

hence, in particular,

$$m_\mathfrak{p} = \bar{m}_\mathfrak{p} \text{ for each } \mathfrak{p}. \tag{19.3 1}$$

Since, according to (19.1), Z is a cyclic representation corps for A, for each $\mathfrak{p}$ the $\mathfrak{p}$-degree of Z is, by Theorem 2, a multiple of the $\mathfrak{p}$-index $m_\mathfrak{p}$ of A, hence, by (19.3 1), also of the $\mathfrak{p}$-index $\bar{m}_\mathfrak{p}$ of $\overline{A}$, and therefore, again by Theorem 2, Z is a cyclic representation corps also for $\overline{A}$.

Let accordingly

$$\overline{A} \sim (\beta, Z, S). \tag{19.4}$$

Then, by comparing the cyclic representations (19.2) and (19.4), it follows, on account of Theorem 1, (i), that

$$\left(\frac{\bar{\alpha}, \overline{Z}, \bar{S}}{\mathfrak{p}}\right) \equiv \left(\frac{\beta, Z, S}{\mathfrak{p}}\right) \pmod 1 \text{ for each } \mathfrak{p}.$$

Together with (19.3), this yields

$$\left(\frac{\alpha, Z, S}{\mathfrak{p}}\right) \equiv \left(\frac{\beta, Z, S}{\mathfrak{p}}\right) \pmod 1 \text{ for each } \mathfrak{p},$$

i.e., from the definition of these symbols,

$$\left(\frac{\alpha, Z}{\mathfrak{p}}\right) = \left(\frac{\beta, Z}{\mathfrak{p}}\right) \text{ for each } \mathfrak{p}.$$

Hence, on account of (3.2), (3.11), β differs from α only by a norm from Z as a factor. Thus, the comparison of the cyclic representations (19.1) and (19.4) yields, by (2.1), indeed

$$A \sim \overline{A}.$$

20. **Proof of Theorem 3.** According to (15.4), $(\alpha, Z, S) \sim 1$ holds, if and only if α is a norm from Z. This again, by (3.11), holds, if and only if each $((\alpha, Z)/\mathfrak{p}) = E$, i.e., if each $((\alpha, Z, S)/\mathfrak{p}) \equiv 0 \pmod 1$.

21. **Proof of Theorem 4.** Let

$$A \sim (\alpha, Z, S), \quad \overline{A} \sim (\bar{\alpha}, \overline{Z}, \bar{S}) \tag{21.1}$$

be two cyclically representable algebras. Then, let Z be any common cyclic

representation corps for both A and $\overline{A}$. The existence of such a corps Z may be derived from Theorem 2.† Let, accordingly,

$$A \sim (\beta, Z, S), \quad \overline{A} \sim (\bar{\beta}, Z, S). \tag{21.2}$$

Then, by (13.1),

$$A \times \overline{A} = \tilde{A} \sim (\beta\bar{\beta}, Z, S) = (\alpha, Z, S).$$

Hence also $\tilde{A}$ is cyclically representable.

Here we have, for the corresponding semi-invariant symbols, that

$$\left(\frac{\alpha, Z, S}{\mathfrak{p}}\right) \equiv \left(\frac{\beta, Z, S}{\mathfrak{p}}\right) + \left(\frac{\bar{\beta}, Z, S}{\mathfrak{p}}\right) \equiv \left(\frac{\alpha, Z, S}{\mathfrak{p}}\right) + \left(\frac{\bar{\alpha}, \overline{Z}, \overline{S}}{\mathfrak{p}}\right) \pmod 1,$$

the former on account of the definition of these symbols and by (3.2), the latter, according to Theorem 1, (i), by comparing the cyclic representations (21.1) and (21.2).

22. **Proof of Theorem 5.** Let

$$A \sim (\alpha, Z, S)$$

be a cyclic representable algebra. Then, by (13.1),

$$A^k \sim (\alpha^k, Z, S).$$

By (15.4), $A^k \sim 1$ holds, if and only if α is a norm from Z, hence, by (3.11), if and only if

$$\left(\frac{\alpha^k, Z}{\mathfrak{p}}\right) = E \text{ for each } \mathfrak{p},$$

and further, by (3.2), if and only if

$$\left(\frac{\alpha, Z}{\mathfrak{p}}\right)^k = E \text{ for each } \mathfrak{p}.$$

From this it follows that the exponent l of A is equal to the least common multiple of the orders $m_{\mathfrak{p}}$ of the symbols $((\alpha, Z)/\mathfrak{p})$.

In particular, in accordance with Theorem 2, there is a cyclic representation corps Z_0, whose degree n_0 is equal to that least common multiple of the $m_{\mathfrak{p}}$.‡ Thus, the index m of A, as a multiple of l according to (13.2), and as a divisor of n_0, according to (11.3), must be the same as l and that least common multiple.

23. **Proof of Theorem 6.** Let A be a cyclically representable algebra of de-

† See the footnote on p. 205.

‡ See again the footnote on p. 205.

gree n. On account of Theorem 2 there are cyclic representation corps whose degree is precisely n.† They lead to cyclic generations of A.

24. **Conclusion.** Let me note once more the analogy between the foregoing theory of cyclic representable algebras and my theory of general quadratic forms which I have developed in some previous papers,‡ and which I have already mentioned in §3 as one of the starting points for my present work.

Let me point out, in particular, the *Fundamentalprinzip*, dominating all my work referred to:

In order that a representation or equivalence relation hold in Ω, it is necessary and sufficient that this relation hold in each $\mathfrak{p}$-adic extension field $\Omega_\mathfrak{p}$ of Ω.

In harmony with this, there hold here the following *fundamental principles*:

In order that two cyclic representable algebras A, $\bar{A}$ be similar, it is necessary and sufficient that for each $\mathfrak{p}$ their $\mathfrak{p}$-adic extensions $A_\mathfrak{p}$, $\bar{A}_\mathfrak{p}$ be similar.

In order that a cyclic representable algebra A be a total matrix algebra, it is necessary and sufficient that for each $\mathfrak{p}$ the $\mathfrak{p}$-adic extension $A_\mathfrak{p}$ be a total matrix algebra.

In order that a cyclic corps Z be a cyclic representation corps for a cyclically representable algebra, it is necessary and sufficient that for each $\mathfrak{p}$ the $\mathfrak{p}$-adic extension corps $Z^\mathfrak{p}$ be a cyclic representation corps for the $\mathfrak{p}$-adic extension $A_\mathfrak{p}$.

The validity of these principles may be easily derived from the foregoing proofs, especially from Theorems 1–3, and (17.5), (17.7), (18.1).

These principles, for their own part, illuminate the methodical scheme of my proofs. The facts to be proved are each time first derived for the $\mathfrak{p}$-adic extensions $A_\mathfrak{p}$; this may be done without great difficulty. Then, by means of the *composition principle* (3.11), borrowed from the class field theory, the transition to the algebra A itself is performed.

I was not, however, able to give a methodically pure performance of this scheme. For, by the reasons mentioned after (3.1), (3.2), for proving the total-invariance of the symbol $((\alpha, Z)/\mathfrak{p})$ (Theorem 1, (ii)) I had to go beyond the $\mathfrak{p}$-adic extension $A_\mathfrak{p}$ of A, and had to consider also the behavior of A for another prime ideal $\mathfrak{q}$.

Nevertheless, even if the theory of the norm residue symbol should, at some time, be carried far enough to avoid that round-about way, the proof of Theorem 1, (i), in the manner here developed will be preferable, I am sure, for reasons of brevity and simplicity.

† See again the footnote on p. 205.

‡ Hasse (1–4).

TABLE OF LITERATURE

A. A. ALBERT

1. *A necessary and sufficient condition for the non-equivalence of any two generalized quaternion division algebras.* Bulletin of the American Mathematical Society, August, 1930.

2. *A note on an important theorem on normal division algebras.* Bulletin of the American Mathematical Society, October, 1930.

E. ARTIN

1. *Beweis des allgemeinen Reziprozitätsgesetzes.* Abhandlungen aus dem Mathematischen Seminar der Hamburger Universität, vol. 5 (1927).

2. *Zur Theorie der hyperkomplexen Zahlen.* Abhandlungen aus dem Mathematischen Seminar der Hamburger Universität, vol. 5 (1927).

3. *Zur Arithmetik der hyperkomplexen Zahlen.* Abhandlungen aus dem Mathematischen Seminar der Hamburger Universität, vol. 5 (1927).

R. BRAUER

1. *Über minimale Zerfällungskörper irreduzibler Darstellungen.* (Gemeinsam mit E. Noether.) Sitzungsberichte der Preussischen Akademie der Wissenschaften, Mathematisch-Physikalische Klasse, Berlin, 1927.

2. *Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearer Substitutionen,* I. Mathematische Zeitschrift, vol. 28 (1928).

3. *Zur Theorie der hyperkomplexen Zahlen.* Mathematische Zeitschrift, vol. 30 (1929).

4. *Untersuchungen über die Eigenschaften von Gruppen linearer Substitutionen,* II. Mathematische Zeitschrift, vol. 31 (1930).

L. E. DICKSON

1. *Algebras and their Arithmetics.* Chicago, 1923.

2. *New division algebras.* Transactions of the American Mathematical Society, vol. 28 (1926).

3. *Algebren und ihre Zahlentheorie.* Zürich, 1927.

4. *New division algebras.* Bulletin of the American Mathematical Society, September–October, 1928.

H. HASSE

1. *Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen.* Journal für die reine und angewandte Mathematik, vol. 152 (1923).

2. *Über die Äquivalenz quadratischer Formen im Körper der rationalen Zahlen.* Journal für die reine und angewandte Mathematik, vol. 152 (1923).

3. *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper.* Journal für die reine und angewandte Mathematik, vol. 153 (1924).

4. *Äquivalenz quadratischer Formen in einem beliebigen algebraischen Zahlkörper.* Journal für die reine und angewandte Mathematik, vol. 153 (1924).

5. *Zwei Existenztheoreme über algebraische Zahlkörper.* Mathematische Annalen, vol. 95 (1926).

6. *Ein weiteres Existenztheorem in der Theorie der algebraischen Zahlkörper.* Mathematische Zeitschrift, vol. 24 (1926).

7. *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, I. Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 35 (1926).

8. *Höhere Algebra*, II. Sammlung Göschen, Berlin, 1927.

9. *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Ia. Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 36 (1927).

10. *Existenz gewisser algebraischer Zahlkörper.* Sitzungsberichte der Preussischen Akademie der Wissenschaften, Mathematisch-Physikalische Klasse, Berlin, 1927.

11. *Neue Begründung und Verallgemeinerung der Theorie des Normenrestsymbols.* Journal für die reine und angewandte Mathematik, vol. 162 (1930).

12. *Die Normenresttheorie relativ-Abelscher Zahlkörper als Klassenkörpertheorie im Kleinen.* Journal für die reine und angewandte Mathematik, vol. 162 (1930).

13. *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, II. Jahresbericht der Deutschen Mathematiker-Vereinigung, Ergänzungsband, vol. 6 (1930).

14. *Über $\wp$-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme.* Mathematische Annalen, vol. 104 (1931).

E. NOETHER

1. *Über minimale Zerfällungskörper irreduzibler Darstellungen.* (Gemeinsam mit R. Brauer.) Sitzungsberichte der Preussischen Akademie der Wissenschaften, Mathematisch-Physikalische Klasse, Berlin, 1927.

2. *Hyperkomplexe Grössen und Darstellungstheorie.* Mathematische Zeitschrift, vol. 30 (1929).

I. SCHUR

1. *Einige Bemerkungen zu der vorstehenden Arbeit des Herrn A. Speiser.* Mathematische Zeitschrift, vol. 5 (1919).

A. SPEISER

1. *Zahlentheoretische Sätze aus der Gruppentheorie.* Mathematische Zeitschrift, vol. 5 (1919).

2. *Theorie der Gruppen von endlicher Ordnung.* 2. Auflage, Berlin, 1927.

E. STEINITZ

1. *Algebraische Theorie der Körper.* Journal für die reine und angewandte Mathematik, vol. 137 (1910). (Neu herausgegeben von R. Baer und H. Hasse, Berlin-Leipzig, 1930.)

B. L. VAN DER WAERDEN

1. *Moderne Algebra*, II. Berlin, 1931.

J. H. M. WEDDERBURN

1. *On hypercomplex numbers.* Proceedings of the London Mathematical Society, vol. 6 (1909).

2. *On division algebras.* Transactions of the American Mathematical Society, vol. 22 (1921).

UNIVERSITY OF MARBURG,
MARBURG, GERMANY