"Hypercomplexe Systeme in ihren Beziehungen zur kommutativen Algebra und Zahlentheorie," Verhandl. Int. Math. Kongress Zürich 1 (1932) pp. 189-194.

The relationship of hypercomplex systems to commutative algebra and number theory

By Emmy Noether, Göttingen

Translated by D. H. Delphenich

1. – In recent years, the theory of hypercomplex systems – viz., *algebras* – has taken a strong upswing; however, it is only in the most recent times that the significance of that theory for questions posed commutatively was made clear. Today, I would like to report on the implications that non-commutative things might have in the context of commutative ones, and indeed, I would like to pursue that in detail in the context of two classical problems that go back to Gauss, namely, the principal genus theorem and the norm theorem that is closed linked with it. The formulation of those problems has changed repeatedly in the course of time. For Gauss, they appeared as the conclusion to his theory of quadratic forms. They played an essential role in the characterization of the relative cyclic and Abelian number fields in terms of class field theory, and ultimately they can be expressed as theorem about automorphisms and the splitting of algebras, and the latter formulation then gives, at the same time, a way of adapting the theorems to arbitrary relative Galois number fields.

With that sketch, which I would like to expand upon later, I would, at the same time, like to explain the application of the non-commutative ideas to commutative ones: *One seeks to arrive at invariant and simple formulations of the known facts regarding quadratic forms or cyclic fields by means of the theory of algebras – i.e., those formulations that depend upon only the structural properties of algebras. Once one has verified those invariant formulations* (and that will be the case in the examples that were given above), *one will have then obtained an adaptation of those facts to arbitrary Galois fields in doing so.*

2. – Before going into a detailed exposition, I would still like to give a general overview of the various methods and further results. First of all, it should be remarked that the main difficulty in obtaining the formulation for general Galois fields lies in the fact that no starting point at all will exist without the hypercomplex method. In the examples cited, the fundamental transition to the non-commutative ideas will be obtained by the *simultaneous consideration of fields and groups* by means of the "reduced product" and its multiplication constants: the "factor system" (cf. § **3**). One will then obtain a simple normal algebra over the base field, and any such algebra can be generated in essentially that way. Such a reduced product was first considered by Dickson ([1]),

([1]) Cf., his book *Algebren und ihre Zahlentheorie*, Zurich, 1927, § 34.

while the theory of factor systems was developed by Speiser, Schur, R. Brauer ([2]) from a completely different standpoint, namely, the question of absolutely-reducible representations. A sufficiently simple and far-reaching structure that will allow to be able to address commutative questions can first be achieved by the fusion of the two theories ([3]).

At the same time, one also gets new and transparent proofs for known facts in that way: Here, I would like to refer to a hypercomplex proof of the reciprocity theorem for cyclic fields that will appear soon in Math. Ann. and was given by H. Hasse ([4]) by means of an invariant formulation of his norm residue symbol that was based upon the theory of the reduced product, and further in a hypercomplex foundation of class field theory in the small, which rests upon the same basis, which C. Chevalley recently gave, but in which even newer algebraic theorems on factor systems were developed ([5]). However, at the same time, I must remark, even more restrictively, that the method of the reduced product alone, to all appearances, will *not* yield the whole theory of Galois number fields. That follows from some recent yet-to-be published results of Artin that are connected with the Hasse proof above in the sense of the principle that was given, but only yield equalities of numbers, in place of complete isomorphism theorems.

One already has methods that yield a complete isomorphism (in general, an operator isomorphism) in algebraic form. One deals with the continuation of some Ansätzen of A. Speiser ([6]), and indeed, with the conceptualization of the Galois field as a "Galois module" – i.e., as a module over the base field that admits the substitutions of the Galois group as operators. Operator isomorphisms between fields and group rings (viz., group algebras) exist in the sense that a one-to-one correspondence between the elements exists in such a way that linear forms over the base field will correspond, and the substitutions of the Galois group in the field will be associated with multiplications in the group ring. That theorem, which I proposed ([7]), was proved by M. Deuring ([8]), who used it to construct a basis for Galois theory whereby the operator isomorphism would realize the association of groups and fields. Far-reaching structural theorems (likewise by Duering) run parallel to the formal facts of Artinian L-series and yield a structural access to Artinian leaders (*Führer*). These Artin L-series and leaders ([9]), which are constructed from general group characters, represent the first connection between number theory and representation theory, according to Speiser ([6]), which is a first advance from the Abelian

---

([2]) Cf., say, R. Brauer, "Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearer Substitutionen," Math. Zeit. **28** (1928), and the literature that is given there in rem. 2.

([3]) I first developed that structure in a lecture in Winter 1929/30, and repeated it in Chap. 2 of H. Hasse, *Theory of cyclic algebras*, Trans. **134** (1932). A report of M. Duering on hypercomplex numbers and number-theoretic applications, which is to appear in the collection *Ergebnisse der Mathematik*, was oriented completely within the scope of the lecture.

([4]) H. Hasse, "Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper (insbesondere Normenrestsymbol und Reziprozitätsgesetz)," Math. Ann. **107** (1932/33).

([5]) C. Chevalley, "Sur la théorie du symbole de restes normiques," *to appear* in Jour. f. Math. **169**.

([6]) A. Speiser, "Gruppendeterminante und Körperdiskriminante," Math. Ann. **77** (1916).

([7]) E. Noether, "Normalbasis bei Körpern ohne höhere Verzweigung, Satz 3," Jour. f. Math. **167** (1932) (there is a gap in the proof).

([8]) M. Deuring, "Galoissche Theorie und Darstellungstheorie," Math. Ann. **107** (1932).

([9]) E. Artin, "Über eine neue Art von L-Reihen," Math. Sem. Hamburg **3** (1924); "Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren," *ibid*. **8** (1931); "Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper," Jour. f. Math. **164** (1931).

fields. It has given a strong impetus to the entire development; in particular, the theory of Galois modules has been oriented in that way.

3. – I would now like to pursue in detail the problems of the norm theorem and the principal genus theorem that were placed at the focus. First, let us *define the reduced product:* Let K/k be a Galois field of degree n, and let $\mathfrak{G}$ be its group. The reduced product means a simultaneous embedding of K and $\mathfrak{G}$ in an algebra A in such a way that the automorphisms of K will become inner ones. The symbols u_{S_1}, …, u_{S_n} might correspond to the n group elements. One then first assumes that A is a module of linear forms of rank n over K:

1. $A = u_{S_1} K + \ldots + u_{S_n} K$ (i.e., A consists of all linear forms $u_{S_1} a_1 + \ldots + u_{S_n} a_n$ with a_i arbitrary elements of K).

A will become a ring [which is generated by the u_S, and more generally, by the $u_S K^*$ ([10])] by means of this requirement of being an inner isomorphism, and thus, an algebra of rank n^2 over k. Namely, that requirement is expressed by:

2. $u_S^{-1} z\, u_S = z^S$ ([11]) or $z u_S = u_S\, z^S$ for every z in K.

3. $u_S\, u_T = u_{ST}\, a_{S,T}$ with $a_{S,T}$ in K^*.

4. $a_{S,T}\ a_{S,T}^R = a_{S,TR}\, a_{T,R}$ (associativity law from $[u_S\, u_T]\, u_R = u_S\, [u_T\, u_R]$).

A is called the reduced product of K with $\mathfrak{G}$ for the factor system $a_{S,T}$. One can prove that A is a simple normal algebra over k, and thus, a matrix ring D_r of degree r over the associated division algebra, and that K is a maximal commutative subfield, and therefore a splitting field. (That is, the extension of the coefficient domain k by a field that is isomorphic to K will yield a *split* algebra, viz., a complete matrix ring over the center.) Conversely, for a given division algebra D, there is always a matrix ring D_r that can be generated as a reduced product in the manner that was given.

If one goes from u_S to $v_S = u_S\, c_S$, with c_S in K^*, which will generate the same automorphism, then the "associated" factor system will arise.

5. $\overline{a}_{S,T} = a_{S,T}\, c_S^T\, c_T / c_{ST}$.

Associated factor systems will be combined into a class (a), and one likewise combines all algebras that are similar to A (i.e., all D_r with $r = 1, 2, \ldots$) into another class $\mathfrak{A}$. *The classes* $\mathfrak{A}$ *and* (a) *are in one-to-one correspondence: The classes with a fixed*

([10]) K^* arises from K by omitting the zero; this notation will be employed in general.
([11]) As usual, z^S means the element that is produced from z by the substitution S.

splitting field K define an Abelian group under direct product that is isomorphic to the term-wise product of the classes of the factor systems. The unity element is the class of splitting algebras (the system of all transformation quantities $c_S^T c_T / c_{ST}$*, resp.).* One is then dealing with the group of algebra classes that R. Brauer commented on.

4. – I would now like to come to the connection with the *concept of norm* by *specializing to cyclic splitting fields*, and in that way, to the formulation of the generalized *norm theorem* in terms of the principle that was put forth in the beginning. If *Z* is cyclic, and *S* is a generating substitution of its group (the associated algebra will then be called cyclic) then one can let the powers of *S* correspond to the powers of *u*, so:

1′. $A = Z + uZ + \ldots + u^{n-1} Z$.
2′. $zu = u z^S$.
3′. $u^n = a$.
4′. a lies in the base field k^*.
5′. $\overline{a} = a \cdot N(c)$ when one sets $v = uc$.

Any factor system here consists of a single element α that lies in the base field, which will be denoted by $A = (\alpha, Z)$. The identity class of the factor system is given by the *norms on* Z^*, so the group of algebra classes will be isomorphic to the factor group $k^* / N(Z^*)$. A cyclic algebra (α, Z) will split iff α is a norm of an element in *Z*. This connection between norm and splitting gives the formulation of the "norm theorem," namely, the *theorem on splitting algebra: If an algebra splits at any place then it will split per se.* In this, the "place" is defined as it usually is in number theory in such a way that the base field *k* is replaced by its $\mathfrak{p}$-adic extension *k*, where $\mathfrak{p}$ is a prime ideal in *k* (the finite number of infinite places at which *k* and its conjugates are extended to the field of real numbers, resp.).

In fact, the norm theorem for cyclic fields is included in that. From what was said above, for cyclic algebras (α, Z), the theorem is equivalent to the statement: If α is a $\mathfrak{p}$-adic norm at any (finite or infinite) point then α will be the norm of a number in *Z*, or without the transition to $\mathfrak{p}$-adics: *If* α *is a normal residue (Normenrest) from each prime ideal* $\mathfrak{p}$ *in k (and satisfies certain conditions on its sign) then* α *will be the norm of a number in Z.* The latter notion is, however, the norm theorem that is proved in class field theory with the use of known analytic tools, and the proof of the general theorem on splitting algebras can be obtained from this cyclic special case by purely algebraic-arithmetic considerations ([12]). Hasse pointed to a first important consequence: *Any simple normal algebra over an algebraic number field is cyclic.* The general formulation came about as a result of the search for a proof of this long-suspected fact.

([12]) R. Brauer, H. Hasse, E. Noether, "Beweis eines Haputsatzes in der Theorie der Algebren," Jour. f. Math. **167** (1932).

5. – A second consequence of the theorem on splitting algebras (which once more can be established in a purely algebraic-arithmetic way) is the *principal genus theorem* ([13]), which is at the forefront. Its invariant formulation rests upon the fact that the relations (2) to (5) that define the reduced product are purely multiplicative, and will therefore remain meaningful when K^* is replaced with an Abelian group $\mathfrak{J}$ that satisfies only the condition that its automorphism group must contain a subgroup that is isomorphic to $\mathfrak{G}$. The "extension of $\mathfrak{G}$ by $\mathfrak{J}$," in the sense of group theory, will enter in place of (1). If one takes $\mathfrak{J}$ to be the group of all ideals in K then the factor system will become a system of ideals; a classification by classes in $\mathfrak{J}$ will induce a classification by classes for the factor system, and indeed it will generally be a finer classification of ideals that the original one. The demand that the multiplication of the u_S by (absolute) ideal classes must be unique says only that the transformation quantities $c_S^T c_T / c_{ST}$ (viz., the identity class of the element factor system) must lie in the identity class of the ideal factor system. However, as the specialization to the known cases will show, it does, in fact, satisfy a somewhat less fine classification. I define: *In the identity class of factor systems, one will find those elements $a_{S,T}$ that generate splitting algebras at all (finite and infinite) branching places of K.* The extension of $\mathfrak{G}$ that arises in that way will be denoted by $\mathfrak{G}^*$; $(\mathfrak{c})$ means the absolute ideal class of $\mathfrak{c}$. One will then have the:

Invariant formulation of the principal genus theorem: If an automorphism of $\mathfrak{G}^*$ arises from the classification thus-defined by the substitution $v_S = u_S\,(\mathfrak{c}_S)$ [all of those $(\mathfrak{c}_S)$ define the principal genus] then the automorphism will be inner, and it will be generated by an ideal class $(\mathfrak{b})$.

The known special cases follow from an equivalent, but somewhat more explicit, formulation: *If the transformation quantities $(\mathfrak{c}_S^T)(\mathfrak{c}_T)/(\mathfrak{c}_{ST})$ that are defined by the ideal classes $(\mathfrak{c}_S)$ belong to the identity ideal class of the factor system then there will be an ideal class* $(\mathfrak{b})$ *such that the* $(\mathfrak{c}_S)$ *will become symbolic* $(1 - S)^{\text{th}}$ *powers:* $(\mathfrak{c}_S) = (\mathfrak{b}) / (\mathfrak{b}^S)$ *for all S in* $\mathfrak{G}$. The assumption then expresses precisely the automorphism property; the fact that it is inner is expressed by saying that $v_S = (\mathfrak{b})^{-1}\, u_S\,(\mathfrak{b}) = u_S\,(\mathfrak{b})^{1-S} = u_S\,(\mathfrak{c}_S)$.

The specialization to the cyclic case (while observing the normalization) then yields: If N $([\mathfrak{c}])$ lies in the identity ideal class of the factor system the $(\mathfrak{c})$ will become the symbolic $(1-S)^{\text{th}}$ power: $(\mathfrak{c}) = (\mathfrak{b})^{1-S}$.

6. – In order to arrive at the known concepts for cyclic fields and quadratic forms from here, I will first point out that the theorem for the complete ideal classes is expressed, but its content will remain the same when one restricts oneself to the branching places of prime ideals, as usual.

([13]) The proof will appear in Math. Ann.

However, with that, the principal genus for quadratic fields that was defined here will go to the Gaussian one; the ideal classes then correspond to the quadratic forms, and the norms to the classes of the numbers will that can be represented by forms. The fact that the identity class generates the algebras that split at the branching places of K then means that those representable numbers will be quadratic residues at the branching places. The associated forms then possess the total character of the principal form, and thus define Gauss's principal genus. The fact that $(1-S)^{th}$ symbolic power goes to duplication is known.

For cyclic fields, the concept goes to the following one: The principal genus consists of all ideal classes whose norms will be norm residues at the (finite and infinite) branching places. However, that is known to be equivalent to the "norm residue from the leader," and thus the usual theorem will come about as a specialization of that.

Moreover, one can also introduce a leader that is composed of only the branching places in the general case of an arbitrary Galois field, such that when one normalizes the factor system for each of those places, the ray will include only elements of the identity class.

The question then arises of the connection with the Artinian leaders that were mentioned in the overview (§ **2**), which are indeed composed of the same prime ideals, and therefore the question of the connection with the theory of Galois modules, namely, the second hypercomplex method. Only the future can say how far these two methods will reach.
