119. Normal Basis of a Quasi-field.

By Tadasi NAKAYAMA.

Mathematical Institute, Osaka Imperial Univerity.

(Comm. by T. TAKAGI, M.I.A., Dec. 12, 1940.)

Recently N. Jacobson extended the fundamental theorem of the Galois theory to *quasi-fields* in the following sense[1]: Let P be a quasi-field and there be given a *finite group of outer automorphisms*[2] $\mathfrak{G}=\{E, S, \dots, T\}$, of order, say n. If Φ is the sub-quasifield of invariant elements, then P has the rank n over Φ (at both left and right) and there exists a 1-1 correspondence between subgroups of $\mathfrak{G}$ and sub-quasifields between P and Φ. The purpose of the present note is to show that moreover P possesses a (one-sided) normal basis[3] over Φ, that is, there exists an element b in P such that the n conjugates, so to speak, $b^E, b^S, \dots, b^T$ of b form a (linearly independent) left (say)-basis of P over Φ. The proof is a generalization of M. Deuring's *second* proof to the theorem of commutative normal bases;[4] the proof has been emancipated, by the present writer,[5] from the restriction on the semisimplicity of the group ring. But it involves modifications caused by the non-commutativity and makes use of a generalization of the Hilbert-Speiser theorem in a *refined* form.

Let P, $\mathfrak{G}$, n and Φ be as above. Denote the center[6] of P by Z, and put $K=\Phi \cap Z$. Let further K^* be a finite extension of K, and let

$$P^*=P_{K^*}, \qquad \Phi^*=\Phi_{K^*}$$

be the rings obtained from P and Φ by extending the ground field K to K^*. (They are not, in general, quasi-fields any more). Automorphisms $E, S, \dots, T$ of P can be looked upon, in natural manner, as those of P^* (and in fact Φ^* consists of the totality of invariant elements).

Lemma 1 (Generalized Hilbert-Speiser theorem). *Let to each S in*

---

1) N. Jacobson, The fundamental theorem of Galois theory for quasi-fields, Ann. Math. **41** (1940).

2) We mean that all the automorphisms in $\mathfrak{G}$ except the identity are outer.

3) For the theorem of normal basis of a commutative field see: E. Noether, Normalbasis bei Körpern ohne höhere Verzweigung, Crelle, **167** (1931); M. Deuring, Galoissche Theorie und Darstellungstheorie, Math. Ann. **107** (1932); H. Hasse, Klassenkörpertheorie, Marburg (1932); R. Brauer, Über die Kleinsche Theorie der algebraischen Gleichungen, Matn. Ann. **110** (1934); M. Deuring, Anwendungen der Darstellungen von Gruppen durch linearen Substitutionen auf die Galoissche Theorie, Math. Ann. **113** (1936); R. Stauffer, The construction of a normal basis in a separable normal extension field, American J. Math, **58** (1936). There is also an unpublished proof by E. Artin.

4) M. Deuring, Math. Ann. **110**, l. c.

5) T. Nakayama, On Frobeniusean algebras, II (forthcoming in Math. Ann.), § 3. Appendix.

6) We are interested only in the case where P has an *infinite rank* over its center. For, otherwise the theorem can readily be reduced to the commutative case, because of Jacobson's result.

$\mathfrak{G}$ *correspond a regular matrix C_S in P^*, of degree (=order), say, r, such that*

$$C_S C_T^S = C_{TS} \quad \textit{for every } S,\ T. \tag{1}$$

Then there exists in P^* a regular matrix A of degree r such that

$$C_S = A^{-1} A^S \quad \textit{for every } S. \tag{2}$$

The case where $K^* = K$ whence $P^* = P$ was treated in Jacobson's paper, l. c. The present case can be manipulated in like manner. Consider namely a crossed product

$$\mathfrak{S}^* = u_E P^* + u_S P^* + \cdots + u_T P^* ,$$

where $u_E, u_S, \dots, u_T$ are abstractly introduced n elements linearly independent over Φ^* and satisfying $\eta u_S = u_S \eta^S (\eta \in P^*)$, $u_S u_T = u_{ST}$. $\mathfrak{S}^*$ contains a subring $\mathfrak{S} = u_E P + u_S P + \cdots + u_T P$, and $\mathfrak{S}^*$ is obtained from $\mathfrak{S}$ by extending the ground field K to K^*. $\mathfrak{S}$ is a simple ring with the center K, as was shown in Jacobson, l. c. Hence[1] $\mathfrak{S}^*$ is a simple ring with the center K^*.

Consider, on the other hand, an r-dimensional (right-) vector space

$$V = v_1 P^* + v_2 P^* + \cdots + v_r P^*$$

over P^*. That a system of matrices C_S satisfies (1) means that if we associate with u_S the semi-linear transformation $\sigma = (C_S, S)$:

$$(v_1, \dots, v_r)^\sigma = (v_1, \dots, v_r) C_S , \qquad (v\eta)^\sigma = v^\sigma \eta^S (v \in V,\ \eta \in P^*)$$

and with $\xi \in P^*$ the transformation $v \rightarrow v\xi$ then V becomes a right-module of $\mathfrak{S}^*$; we denote the $\mathfrak{S}^*$-module V thus obtained by V_1. Further, if we use the system $\{E_S = E$ (unit matrix of degree r)$\}$ instead of $\{C_S\}$ then we get a second $\mathfrak{S}^*$-right-module V_0 from V. But (finite) moduli of a simple ring $\mathfrak{S}^*$ are characterized, up to isomorphism, by their behaviors with respect to the center K^*. Therefore, the two moduli V_0 and V_1 are operator-isomorphic, and if A is the matrix of the isomorphic transformation, which is certainly regular, then $C_S = A^{-1} E A^S = A^{-1} A^S$ as desired.

On taking reduction into account we show further

Lemma 2 (Refinement of the Hilbert-Speiser theorem). *Let C_S in Lemma 1 be of the form*

$$C_S = \begin{pmatrix} D_S & H_S \\ 0 & F_S \end{pmatrix}. \tag{3}$$

Then we can take the regular matrix A, satisfying (2), in the similarly reduced form

$$A = \begin{pmatrix} A_1 & A_3 \\ 0 & A_2 \end{pmatrix}. \tag{4}$$

---

1) See E. Noether, Nichtkommutative Algebra, Math. Zeitschr. **37** (1933).

Furthermore, if there are given already specified regular matrices A_1 and A_2 satisfying $D_S = A_1^{-1}A_1^S$ and $F_S = A_2^{-1}A_2^S$ then we can take a suitable A_3 so that A given by (4) fulfills (2).[1]

Let for the proof g be the degree of D_S, and consider the subspace $W = v_1P^* + \cdots + v_gP^*$ of V. If we look upon V as V_1, defined above, W is an allowable submodule, as the form (3) shows; in this interpretation we write W_1 for W. Similarly the same space W is an allowable submodule of V_0, which we shall denote by W_0. The $\mathfrak{S}^*$-right-moduli W_0 and W_1 are operator-isomorphic, and such an isomorphism can be extended to that of the over-moduli V_0 and V_1, because they are completely reducible. But the matrix A of such an extended isomorphism has the form (4). This proves the first half of the lemma. As for the second half, we have simply to observe that to specify A_1 and A_2 means to specify the isomorphisms $W_0 \cong W_1$ and $V_0/W_0 \cong V_1/W_1$, and we can, because of the complete reducibility, combine them into an isomorphism between V_0 and V_1.

Now we come to

Theorem (Existence of normal bases). *Let P, $\mathfrak{G}$ and Φ be as before. Then there exists in P an element b such that its conjugates b^E, $b^S, \dots, b^T (\mathfrak{G} = \{E, S, \dots, T\})$ form a (linearly independent) left-basis*[2] *of P over Φ. In other words, the Φ-$\mathfrak{G}$-module P is operator-isomorphic to the group ring $G(\Phi)$ of $\mathfrak{G}$ over Φ.*

Let the above field K^* be sufficiently large so that all the absolutely irredicible representations of $\mathfrak{G}$ lie in it. Let $S \to G_S$ be one of them, and let U_S be the directly indecomposable component of the regular representation of $\mathfrak{G}$ belonging, in the sense of R. Brauer-C. Nesbitt,[3] to G_S. We suppose that U_S lie in K^* too and be reduced in the form that the right upper part is zero; the first largest completely reducible part (as well as the last) of U_S is G_S;

$$(5) \qquad U_S = \begin{pmatrix} G_S & 0 \\ * & * \end{pmatrix}.$$

Let r and g be the degrees of U_S and G_S respectively. From $U_SU_T = U_{ST}$ follows $U'_TU'_S = U'_{ST}$, and so we see, on observing the reduced form of U'_S, the existence of a regular matrix $A = (a_{ij})$ of the reduced form $\begin{pmatrix} A_1 & * \\ 0 & * \end{pmatrix}$ in P^* such that

$$(6) \qquad U'_S = A^{-1}A^S, \quad \text{that is,} \quad A^S = AU'_S \quad \text{for every} \quad S \in \mathfrak{G}.$$

The submatrix A_1 is *regular* too and satisfies

$$(7) \qquad A_1^S = A_1G'_S.$$

---

1) In case of a commutative field Speiser's construction gives, as a matter of fact, the first part of the lemma; his construction, however, does not apply to our non-commutative case. As for the second part, it seems to the writer necessary to employ a structural argument as below even in the commutative case.

2) Similarly P has a normal right-basis over Φ.

3) R. Brauer-C. Nesbitt, On regular representations, Proc. Nat. Acad. Sci. **23** (1937).

We want to prove that the g^2 elements $a_{ij}(i, j=1, 2, \dots, g)$ in A_1 are *left*-linearly independent over Φ^*. To do so, let

$$(8) \qquad \sum_{i=j}^{g}\sum_{j=1}^{g} \varphi_{ij} a_{ij} = 0, \qquad \varphi_{ij} \in \Phi^* .$$

Now, there exists a linear combination $L(G'_S)$ of G'_S with coefficients in K^* equal to the matrix unit ε_{11}. The corresponding linear combination $L(S)$ of S effects, according to (7), the transformation: $a_{i1} \rightarrow a_{i1}$, $a_{ij} \rightarrow 0 (j=2, 3, \dots, g)$. Hence we get from (8)

$$(9) \qquad \sum_{i=1}^{g} \varphi_{i1} a_{i1} = 0 .$$

But there exists for each $k=1, 2, \dots, g$ also a linear combination $L_k(S)$ of S whose corresponding matrix $L_k(G'_S)$ is the matrix unit ε_{k1}. By $L_k(S)$ $a_{i1} \rightarrow a_{ik}$, $a_{ij} \rightarrow 0 (j=2, 3, \dots, g)$, again according to (7). Thus we obtain from (9)

$$(10) \quad \sum_{i=1}^{g} \varphi_{i1} a_{ik} = 0 \ (k=1, 2, \dots, g), \quad \text{that is,} \quad (\varphi_{11}, \dots, \varphi_{g1}) A_1 = 0 .$$

Therefore, since A_1 is regular, $\varphi_{11} = \cdots = \varphi_{g1} = 0$. Similarly all the φ_{ij} are 0. So the g^2 elements in A_1 are left-linearly independent over Φ^*.

Now, write (6) in the form

$$(11) \qquad (A')^S = U_S A' .$$

(Observe that the coefficients in U_S are in K^*). This shows that a Φ^*-left-module $\mathfrak{M}_i (\leqq P^*)$ generated by the r elements $a_{i1}, a_{i2}, \dots, a_{ir}$ forming a column in A' (that is, a row in A) is a Φ^*-$\mathfrak{G}$-double-module and is operator-homomorphic to the *representation* Φ^*-$\mathfrak{G}$-*module* $\mathfrak{U}$ belonging to U_S. This is the case for every $i=1, 2, \dots, r$. But we take only the first g of them: $\mathfrak{M}_1, \mathfrak{M}_2, \dots, \mathfrak{M}_g$, and consider their sum

$$\mathfrak{M} = (\mathfrak{M}_1, \mathfrak{M}_2, \dots, \mathfrak{M}_g)$$

in P^*. Evidently $\mathfrak{M}$ is operator-homomorphic to a direct sum

$$\mathfrak{B} = \mathfrak{U}_1 + \mathfrak{U}_2 + \cdots + \mathfrak{U}_g$$

of g moduli $\mathfrak{U}_i$ isomorphic with $\mathfrak{U}$. Let $\mathfrak{W}$ be the submodule (of dimension g over Φ^*) in $\mathfrak{U}$ corresponding to the first largest completely reducible part G_S of U_S, and $\mathfrak{W}_i$ be the corresponding submodule in $\mathfrak{U}_i$. Then the (direct) sum $\mathfrak{Y} = \mathfrak{W}_1 + \mathfrak{W}_2 + \cdots + \mathfrak{W}_g (\leqq \mathfrak{B})$ is mapped by this homomorphism onto the submodule $\mathfrak{N}$ of $\mathfrak{M}$ generated by the g^2 elements in the submatrix A_1. Since these g^2 elements are (left-) linearly independent over Φ^*, this homomorphism between $\mathfrak{N}$ and $\mathfrak{Y}$ must be an isomorphism. But $\mathfrak{Y}$ contains[1] the largest completely reducible sub-

1) If Φ^* is semi-simple then $\mathfrak{Y}$ is actually the largest completely reducible submodule of $\mathfrak{B}$. And, Φ^* is certainly semi-simple if K^*/K is separable. As a matter of fact, we could assume without loss of generality that this be the case.

module of $\mathfrak{B}$, and therefore, the whole homomorphism between $\mathfrak{M}$ and $\mathfrak{B}$ is necessarily an isomorphism too (or, the gr elements $a_{ij}(i=1, 2, \dots, g; j=1, 2, \dots, r)$ are left-linearly independent over Φ^*).

This is the case for every irreducible representation G_S of $\mathfrak{G}$. So we get $\mathfrak{M}$ for each G_S, and we consider the sum $\mathfrak{N}$ (in P^*) of the $\mathfrak{M}$'s corresponding to all the different G_S's. This sum is direct, since the summands have no isomorphic submoduli. Hence $\mathfrak{N}$ is the whole P^* because both $\mathfrak{N}$ and P^* have the same rank $n(K^*:K)$ over Φ. But $\mathfrak{B}$ is, by its construction, operator-isomorphic to the group ring $\mathfrak{G}(\Phi^*)$,[1] and so is $\mathfrak{N}$. That is, the Φ^*-$\mathfrak{G}$-module P^* is operator-isomorphic to the group ring $\mathfrak{G}(\Phi^*)$. It follows then that the Φ-$\mathfrak{G}$-moduli P and $\mathfrak{G}(\Phi)$ are also operator-isomorphic to each other, as one easily sees from the Krull-Remak-Schmidt theorem asserting the up-to-isomorphism uniqueness of the direct decomposition of a group (with chain conditions).

Remark. In case the group ring $\mathfrak{G}(\Phi)$ is semi-simple[2] U_S and G_S coincide and so we do not need Lemma 2. Even when $\mathfrak{G}(\Phi)$ is non-semisimple we could evade the same lemma if P^* were a quasi-field. In this case we take namely an arbitrary regular A satisfying (7) and consider its first g columns. There exist, since A is regular and P^* is assumed to be a quasi-field, g indices $i_1, i_2, \dots, i_g$ such that the submatrix

$$(12) \qquad (a_{ij} \quad \text{with} \quad i=i_1, i_2, \dots, i_g; \quad j=1, 2 \dots, g)$$

is regular, and we use this submatrix instead of A_1. Furthermore, the same would be the case if all the PZ_ν^* were quasi-fields, where $Z^* = Z_1^* + Z_2^* + \dots + Z_m^*$ is a decomposition of Z^* into a direct sum of mutually conjugate fields.[3] For, we consider the component of the matrix A with respect to PZ_1^*, for instance, and look for g indices i_μ such that the component of (12) is regular in PZ_1^*. Then the components of (12) for the other PZ_ν^* are automatically regular (in the corresponding quasi-fields PZ_ν^*), as one easily sees, on observing that Z_ν^* are mutually conjugate under $\mathfrak{G}$, from (7). The case of a commutative P, treated in Nakayama, l. c., can be classed into this last category.

1) The regular representation of $\mathfrak{G}$ contains U_s exactly g times.

2) This is the case if and only if n is not divisible by the characteristic of Φ (or, of K).

3) Observe that Z is separable and normal over K. Its Galois group is homomorphic to $\mathfrak{G}$.