Nakayama, T.
Osaka Math. J.
15 (1963), 11–23.

ON A GENERALIZED NOTION OF GALOIS EXTENSIONS OF A RING

To Kenjiro Shoda on the occasion of his 60th birthday

By

TADASI NAKAYAMA

Galois theory of non-commutative rings was first developed by K. Shoda [25] as a generalization and refinement of the R. Brauer–E. Noether theory of commutants, or (to express in an almost, if not completely, equivalent terminology), of inner transformation groups. The "outer" respect was introduced by N. Jacobson [12], by whom, in [13], and by H. Cartan [6] were developed "composite" theories too. Further developements in the Galois theory of rings, in various directions, were given in J. Dieudonné [8], [9], Jacobson [14], G. Hochschild [10], [11], G. Azumaya [3], T. Nakayama [18], [19], [20], [21], [22], A. Resenberg–D. Zelinsky [24], F. Kasch [15], N. Nobusawa [23], T. Nagahara–H. Tominaga [17], Tominaga [26], and so forth. In some of these works (e.g. the writer's note [22]) a much broad interpretation was given to the theory. All these papers consider mostly (if not exclusively) those (Galois) extension rings which are, either by assumption or by nature of circumstances, (right, say) free over the ground ring. On the other hand, the recent trend of algebra, influenced by the development of homological algebra, strongly points at the replacement of "free" by "projective". Indeed, by M. Auslander–O. Goldman [2] are studied separable algebras, which turn out, at least in a very important special case, to be a such generalization of maximally central algebras of Azumaya–Nakayama [5], Azumaya [4]. In the present note we wish to introduce a similar generalization of (generalized) Galois extensions studied in [22], to examine the characterizing conditions, and to observe some of its elementary features.

§ 1. Generalized Galois extensions.

Let A be an (associative and not necessarily commutative) ring (with unit element 1). Let $\mathfrak{A}_0 = \mathrm{Hom}\,(A,A)$ be the (absolute) endomorphism ring of A (as a module), which we consider as a *right* operator domain of A. For any subset X of A. we denote by X_R (resp. X_L) the set of right (resp. left) multiplications, on A, by the elements of X. For a subring S of A, S_R (resp. S_L) is a subring of $\mathfrak{A}_0$ isomorphic (resp. inverse-isomorphic) to S.

Now, let $\mathfrak{B}$ be a (right) operator-ring (with unit element operating identically) of A (as a module). There is a (unique) epimorphism σ of $\mathfrak{B}$ to a subring $\mathfrak{B}_0$ of $\mathfrak{A}_0$ such that if $\sigma:\beta\to\beta_0$ ($\beta\in\mathfrak{B}$, $\beta_0\in\mathfrak{B}_0$) then $a^{\beta}=a^{\beta_0}$ for every $a\in A$. Adopting the notation of Auslander-Goldman [1][1], we denote by $\mathfrak{T}_{\mathfrak{B}}=\mathfrak{T}_{\mathfrak{B}}^{(A)}$ the submodule of $\mathfrak{A}$ generated by the images of the elements of A by $\mathfrak{B}$-homomorphisms of A into the $\mathfrak{B}$-right-module $\mathfrak{B}$;

$$\mathfrak{T}_{\mathfrak{B}} = A^{\mathrm{Hom}_{\mathfrak{B}}(A,\mathfrak{B})}$$

It is readily seen that $\mathfrak{T}_{\mathfrak{B}}$ is a two-sided ideal of $\mathfrak{B}$; to see that $\mathfrak{T}_{\mathfrak{B}}$ is a left ideal of $\mathfrak{B}$, observe that if $\varphi\in\mathrm{Hom}_{\mathfrak{B}}(A,\mathfrak{B})$ then the map $a\to\beta a^{\varphi}$ is also in $\mathrm{Hom}_{\mathfrak{B}}(A,\mathfrak{B})$ for every $\beta\in\mathfrak{B}$.

REMARK 1. If $\mathfrak{B}$ is such that $\mathfrak{B}_0$ contains the left multiplication ring A_L of A;

$$\mathfrak{B}_0\supset A_L\,,$$

then $\mathfrak{T}_{\mathfrak{B}}$ may also be defined by

$$\mathfrak{T}_{\mathfrak{B}} = \mathrm{Hom}_{\mathfrak{B}}(A,\mathfrak{B})\mathfrak{B}$$

where each element of $\mathrm{Hom}_{\mathfrak{B}}(A,\mathfrak{B})$ is identified with the image of $1\in A$ by it. For, if $\varphi\in\mathrm{Hom}_{\mathfrak{B}}(A,\mathfrak{B})$, $\beta\in\mathfrak{B}$ then $1^{\varphi}\beta=(1^{\beta})^{\varphi}\in A^{\mathrm{Hom}_{\mathfrak{B}}(A,\mathfrak{B})}$, while if $a\in A$, $\varphi\in\mathrm{Hom}_{\mathfrak{B}}(A,\mathfrak{B})$ and if β is an element of $\mathfrak{B}$ which is mapped by σ on the left multiplication (on A) a_L of a then $a^{\varphi}=(1^{\beta})^{\varphi}=1^{\varphi}\beta\in\mathrm{Hom}_{\mathfrak{B}}(A,\mathfrak{B})\mathfrak{B}$.

Let, on the other hand, B be a subring of A (containing the unit element 1 of A). We set also

$$\mathfrak{T}_{B_R} = A^{\mathrm{Hom}_{\mathfrak{B}_R}(A,B_R)}\,,$$

which is a two-sided ideal of B_R.

Now consider the following conditions on the relationship of $\mathfrak{B}$, B, and A:

i) $\mathrm{Hom}_{\mathfrak{B}}(A,A)=B_R$,

ii) $\sigma:\mathfrak{B}\to\mathfrak{B}_0$ is monomorphic (whence isomorphic) and $\mathrm{Hom}_B(A_B,A_B)=\mathfrak{B}_0$; by identification we express this situation simply by writing

1) Our notations for operators are, however, left-right symmetric to those in [1].

$$\mathrm{Hom}_B(A_B, A_B) = \mathfrak{B},$$

iii) A is $\mathfrak{B}$-finitely generated ($f.g.$) projective,
iv) A is B_R-$f.g.$ projective,
v) $\mathfrak{T}_{\mathfrak{B}} = \mathfrak{B}$,
vi) $\mathfrak{T}_{B_R} = B_R$,
vii) the B_R-module A has B as a direct summand.

The condition v) is equivalent to "$\mathfrak{T}_{\mathfrak{B}} \ni$ unit element of $\mathfrak{B}$" and may be re-formulated "the $\mathfrak{B}$-right-module $\mathfrak{B}$ is isomorphic to a direct summand of a direct sum of copies of A". Similarly with vi). Now, we have the following implications:

i) + iii) $\Rightarrow$ vi)
i) + v) $\Rightarrow$ ii)
i) + v) $\Rightarrow$ iv)
ii) + iv) $\Rightarrow$ v)
ii) + vi) $\Rightarrow$ iii)
ii) + vi) $\Rightarrow$ i)
vii) $\Rightarrow$ vi)
i) + ii) + iii) $\Rightarrow$ vii).

Except the last one, these implications can readily be derived from the general theory of projective modules and their endomorphism rings, which has been studied by many authors in different aspects and different generalities, and is indeed discussed fully in Curtis [7], Morita [16] and Auslander-Goldman [1]. Refering to the appendix of this last paper, which is already refered to above and where the theory is very nicely summarized, we thus obtain the 1st of the above implications directly from [1], Prop. A. 3 (E, Γ and Ω there being replaced by A, $\mathfrak{B}$ and B_R). The 2nd implication is derived from [1], Th. A. 2 (g). The 3rd follows from [1], Th. A. 2 (c), while the 4th follows from [1], Prop. A. 3. The 5th is derived from [1], Th. A. 2 (c) (E, Γ, Ω there being replaced by A, B_R, $\mathfrak{B}$ here). Further, the 6th follows from [1], Th. A. 2 (g). The 7th is rather evident.

As for the last implication, i) + ii) + iii) $\Rightarrow$ vii), we postpone its verification till § 5 below. Assuming it here, however, we see that the following combinations of conditions are all equivalent:

(0): i) + ii) + iii) + iv),
(I): i) + iii) + v),
(II): i) + v) + vi),
(III): ii) + iv) + vi),

(IV): ii)+iv)+vii),
(V): ii)+v)+vi),
(VI): i)+v)+vii),
(VII): ii)+v)+vii).

Indeed, these are all equivalent to the wholesale combination i)+ii)+iii)+iv)+v)+vi)+vii).

In case this wholesale combination is fulfilled, which is thus equivalent to that any one of the combinations (0)$\sim$(VII) is satisfied, we propose to say that A is $\mathfrak{B}$-*Galois* over B, or, simply, A is $\mathfrak{B}$-Galois, or, A is Galois over B, or, A is a ($\mathfrak{B}$)-Galois extension of B.

As typical ones among the eight characterizations (0)$\sim$(VII), we state the first five in explicit terms:

(0) $\mathrm{Hom}_{\mathfrak{B}}(A, A)=B_R$, $\mathrm{Hom}_B(A_B, A_B)=\mathfrak{B}$, and A is both $\mathfrak{B}$-*f. g.* projective and B_R-*f. g.* projective,

(I) A is $\mathfrak{B}$-*f. g.* projective, $\mathfrak{T}_{\mathfrak{B}}$ $(=A^{\mathrm{Hom}_{\mathfrak{B}}(A, \mathfrak{B})})=\mathfrak{B}$, and $\mathrm{Hom}_{\mathfrak{B}}(A, A)=B_R$,

(II) $\mathfrak{T}_{\mathfrak{B}}$ $(=A^{\mathrm{Hom}_{\mathfrak{B}}(A, \mathfrak{B})})=\mathfrak{B}$, $\mathrm{Hom}_{\mathfrak{B}}(A, A)=B_R$, and $\mathfrak{T}_{B_R}$ $(=A^{\mathrm{Hom}_{B_R}(A, B_R)})=B_R$,

(III) A is B_R-*f. g.* projective, $\mathfrak{T}_{B_R}$ $(=A^{\mathrm{Hom}_{B_R}(A, B_R)})=B_R$, and $\mathrm{Hom}_B(A_B, A_B)=\mathfrak{B}$,

(IV) $\mathrm{Hom}_B(A_B, A_B)=\mathfrak{B}$ and the B_R-module A is *f. g.* projective and has B as a direct summand,

where the relation $\mathrm{Hom}_B(A_B, A_B)=\mathfrak{B}$ in (0), (III), (IV) is to be interpreted in the sense explained in ii) above.

Perhaps (0) is most natural, while the others are often more convenient than (0) to verify in various concrete cases. Anyway, the property of the $\mathfrak{B}$-B-module A thus we require is the one fully studied e. g. in Morita [16], and our concern lies in the present special situation where A is a ring which contains B as a subring.

§ 2. Digression

We wish to study the independency of some of the above conditions, in particular those appearing in the characterization (0). Thus:

EXAMPLE 1. i)+ii)+iii)+non-iv): Let K be a commutative ring (e. g. a field) and let A be the subalgebra of the complete matrix algebra of degree 2 over K generated by

$$1=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad e=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix},\quad b=\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}.$$

Let B be the subalgebra of A generated by 1 and b. A is directly decomposed into the direct sum

$$A = B \oplus eK$$

of B-right submodules B and eK. Thus the condition vii) holds for our A, B. Hence vi) holds too. Let $\mathfrak{B}$ be the B_R-endomorphism ring of A; $\mathfrak{B}=\mathrm{Hom}_B(A_B, A_B)$. Then ii) is satisfied trivially. By the 5th and 6th of the implications in the preceding § we see that the conditions i), iii) are satisfied too.

On the other hand, A is not B_R-projective, as we readily see from the above direct decomposition of A (and the Krull-Remak-Schmidt theorem).

We remark that our example gives actually the situation i)+ii)+iii)+vi)+vii)+non-iv)+non-v); observe that v) could not be the case since i) is the case and iv) is not.

EXAMPLE 2. i)+iii)+iv)+non-ii): Let K be a commutative ring (e. g. a field) and let A be the algebra over K having a (linearly independent) basis (e_1, e_2) whose (associative and commutative) multiplication table is given by

$$e_1^2 = e_1, \quad e_2^2 = e_2, \quad e_1e_2 = e_2e_1 = 0\,.$$

The (K-) endomorphism ring $\mathrm{Hom}_K(A, A)$ of A is the complete matrix algebra of degree 2 over K, operating on the vector $\begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$ from left. Let $\mathfrak{B}$ be its subring consisting of all matrices of form $\begin{pmatrix} \xi & 0 \\ \zeta & \eta \end{pmatrix}$. $\mathfrak{B}$ is thus generated by the multiplication ring $A_R=A_L$ and the K-linear map

$$\gamma: \quad e_1 \to e_2, \qquad e_2 \to 0\,,$$

and is indeed spanned over K by $(e_1)_L$, $(e_2)_L$ and γ; $\mathfrak{B}=(e_1)_LK\oplus(e_2)_LK\oplus\gamma K$. Here $(e_1)_LK\oplus\gamma K=(e_1)_L\mathfrak{B}$, $(e_2)_LK=(e_2)_L\mathfrak{B}$ and we have

$$\mathfrak{B} = (e_1)_L\mathfrak{B} \oplus (e_2)_L\mathfrak{B}\,.$$

Further the $\mathfrak{B}$-right-module A is isomorphic to the right-ideal $(e_1)_L\mathfrak{B}$, generated by the idempotent $(e_1)_L$, by the isomorphism $e_1 \to (e_1)_L$, $e_2 \to \gamma$. Hence A is $\mathfrak{B}$-($f.g.$ and) projective, i. e. iii).

Now, $\mathrm{Hom}_{\mathfrak{B}}(A, A)=K$. So we set $B=K$ $(=1K=(e_1+e_2)K)$ to have i). Evidently A is B_R-$f.g.$ projective, i. e. iv). On the other hand, $\mathrm{Hom}_{B_R}(A, A)=\mathrm{Hom}_K(A, A)$ is not $\mathfrak{B}$, i. e. non-ii).

In fact our example gives a situation i)+iii)+iv)+vi)+vii)+non-ii)+

non–v); v) could not be the case since i) is the case and ii) is not.

EXAMPLE 3. ii)+iii)+iv)+non–i): Let K be a commutative ring (e. g. a field) and A be the complete matrix algebra of degree 2 over K;

$$A = c_{11}K \oplus c_{12}K \oplus c_{21}K \oplus c_{22}K,$$

c_{ij} being matrix units. Let B be its subalgebra

$$B = c_{11}K + c_{21}K + c_{12}K.$$

We have $c_{22}B = c_{21}K + c_{22}K$ and A is the direct sum of $c_{22}B$ and its isomorphic copy $c_{12}B = c_{11}K + c_{12}K$. Hence A is B-$f.g.$ projective, i. e. iv). $\mathrm{Hom}_K(A, A)$ is the complete matrix algebra of degree 4 over K, operating on the vector $\begin{pmatrix} c_{11} \\ c_{12} \\ c_{21} \\ c_{22} \end{pmatrix}$ from left, and the right multiplication B_R of B (on A) consists of all matrices of form

$$\begin{pmatrix} \xi_{11} & 0 & 0 & 0 \\ \xi_{21} & \xi_{22} & 0 & 0 \\ 0 & 0 & \xi_{11} & 0 \\ 0 & 0 & \xi_{21} & \xi_{22} \end{pmatrix}.$$

Setting $\mathfrak{B} = \mathrm{Hom}_B(A_B, A_B)$ (i. e. ii)) we see that $\mathfrak{B}$ consists of all matrices of form

$$\begin{pmatrix} \gamma_{11} & 0 & \gamma_{12} & 0 \\ 0 & \gamma_{11} & 0 & \gamma_{12} \\ \gamma_{21} & 0 & \gamma_{22} & 0 \\ 0 & \gamma_{21} & 0 & \gamma_{22} \end{pmatrix},$$

and thus coincides with the left multiplication ring A_L of A. Hence A is $\mathfrak{B}$-$f.g.$ projective, i. e. iii). Moreover, $\mathrm{Hom}_{\mathfrak{B}}(A, A) = \mathrm{Hom}_A({}_AA, {}_AA) = A_R$ and this is properly larger than B_R, i. e. non–i).

Our example gives indeed ii)+iii)+iv)+v) non–i)+non–vi)+non–vii); that v) is the case is evident from $\mathfrak{B} = A_L$ while non–vi) follows from non-i) (and ii)) and non–vii) follows from non–vi).

REMARK 2. In the above examples K was assumed to be commutative merely for simplicity of expression. The constructions go as well for a non-commutative K.

REMARK 3. The existence of an example for i)+ii)+iv)+non–iii) seems promising. On the other hand, it is hoped too that under certain rather weak restrictions the conditions i), ii) and iv) together imply iii).

§ 3. Comparison with separable extensions

In [2] Auslander and Goldman studied the notion of separable algebras over a commutative ring; an algebra A over a commutative ring B is called separable when A is projective over $A^e = A \otimes_B A^*$, A^* being the opposite of A. They studied especially the case of A central over B. Thus, let A be a ring and B be its center. They showed in particular that A is separable over B if and only if any one of the following conditions is satisfied:

(α) $\mathrm{Hom}_{A^e}(A, A^e) A^e = A^e$,

(β) $A^e \to \mathrm{Hom}_B(A_B, A_B)$ is an isomorphism and A is B_R-$f.g.$ projective,

(γ) $A^e \to \mathrm{Hom}_B(A_B, A_B)$ is an isomorphism and the B_R-module A has B as a direct summand.

Set $\mathfrak{B} = A_R \otimes_B A_L \doteq A \otimes_B A^* = A^e$, and let $\mathfrak{B}_0$ be its natural image in $\mathrm{Hom}(A, A)$; $\mathfrak{B}_0$ is the subring of $\mathrm{Hom}(A, A)$ generated by A_R and A_L. Since $\mathfrak{B}_0 \supset A_L$, $\mathfrak{T}_{\mathfrak{B}} = A^{\mathrm{Hom}_{\mathfrak{B}}(A, \mathfrak{B})}$ coincides with $\mathrm{Hom}_{\mathfrak{B}}(A, \mathfrak{B})\mathfrak{B}$ as was observed in a Remark in § 1. Hence the condition (α) is nothing else as the condition v) in § 1 (for the present situation). Further, (β) is ii)+iv), and (γ) is ii)+vii). Needless to say that the definition of A being separable over B is the condition iii), in § 1, and the condition i) is evidently implied by that A is central over B. In view of the criterion (0) in § 1, for instance, we see that, in case B is the center of A, "A is separable over B" coincides with "A is $\mathfrak{B}$-Galois over B (where $\mathfrak{B} = A_R \otimes_B A_L = A \otimes_B A^* = A^e$)".

The above criteria of Auslander-Goldman [2] tell that under the condition that B is the center of A these equivalent notions are realized if any of the (combined) conditions iii), v), ii)+iv), ii)+vii) holds. These are much simpler than our (0)$\sim$(VII) for the general case, even when we count that i) is trivially satisfied. The simplication is naturally brought about by the assumption that A is central over B and particularly by that B is commutative (which makes the second part of [1], Prop. A. 3 applicable).

The notion of separable algebras is a generalization of the notion of maximally central algebras in Azumaya-Nakayama [5], Azumaya [4]. Indeed, this latter is the combination of "separable" and "free-Galois" which we consider in the next section.

§4. Comparison with free-Galois extensions

In [22] the writer considered the relationship of a ring A, a subring B of A such that A is right $f.g.$ free over B, and the B_R-endomorphism ring $\mathrm{Hom}_B(A_B, A_B)$ of A (in order to prepare for a study of special cases as weakly normal. innerly weakly normal and maximally central extensions). Setting $\mathfrak{B}=\mathrm{Hom}_B(A_B, A_B)$ we have ii) of §1 trivially, while iii) and vi) (and vii) too) follow immediately from "A is B_R-$f.g.$ free". Thus, in the above situation (i.e. if A is B_R-$f.g.$ free), A is $\mathfrak{B}$-Galois over B with $\mathfrak{B}=\mathrm{Hom}_B(A_B, A_B)$, as our criterion (III) (or (IV)) shows. Indeed, under the assumption that A is B_R-$f.g.$ free, the mere condition ii), i.e. $\mathfrak{B}=\mathrm{Hom}_B(A_B, A_B)$, (entails and) is equivalent to that A is $\mathfrak{B}$-Galois over B (i.e. i)+ii)+iii)+iv)+v)+vi)+vii)). Let us thus express the situation "A is right $f.g.$ free over a subring B" by "A is free-($\mathfrak{B}$-) Galois over B ($\mathfrak{B}=\mathrm{Hom}_B(A_B, A_B)$)".

§5. $\mathfrak{B}$-projectivity

We now wish to prove the implication i)+ii)+iii)$\Rightarrow$vii) presumed in §1; the argument will be a generalization of that in Auslander-Goldman [2]. We consider, for this purpose, again an operator ring $\mathfrak{B}$ of a ring A. The map

$$\varphi : \beta(\in \mathfrak{B}) \to 1^{\beta} \quad (\in A),$$

1 denoting the unit element of A, is evidently a $\mathfrak{B}$-homomorphism of $\mathfrak{B}$ into A. *We assume that this $\mathfrak{B}$-homomorphism φ is epimorphic*:

$$\mathrm{Im}\,\varphi = 1^{\mathfrak{B}} = A$$

(which is certainly the case when the natural image $\mathfrak{B}_0$ of $\mathfrak{B}$ in $\mathfrak{A}_0$ contains the left multiplication ring A_L of A, $A_L \subset \mathfrak{B}_0$, as in Remark in §1). Denoting the $\mathrm{Ker}\,\varphi$ by $\mathfrak{k}$ (which is a right-ideal of $\mathfrak{B}$) we obtain an exact sequence

$$0 \to \mathfrak{k} \to \mathfrak{B} \xrightarrow{\varphi} A \to 0\,.$$

Lemma 1. A is $\mathfrak{B}$-projective if and only if this sequence splits, i.e. if and only if there is a $\mathfrak{B}$-homomorphism λ: $A \to \mathfrak{B}$ such that the composite $\lambda\varphi$: $A \xrightarrow{\lambda} \mathfrak{B} \xrightarrow{\varphi} A$ is identical on A. The condition is in turn equivalent to that the map φ^*: $\mathrm{Hom}_{\mathfrak{B}}(A, \mathfrak{B}) \to \mathrm{Hom}_{\mathfrak{B}}(A, A)$ induced by φ: $\mathfrak{B} \to A$ is epimorphic.

Proof is evident for the first half. The second follows immediately if we observe that the map φ^* is $\mathrm{Hom}_{\mathfrak{B}}(A, A)$-left-homomorphic.

We now assume $A_L \subset \mathfrak{B}_0$. Then we have

$$\mathrm{Hom}_{\mathfrak{B}}(A, A) = B_R$$

with a subring B of A.

Lemma 2. For any element λ of $\mathrm{Hom}_{\mathfrak{B}}(A, \mathfrak{B})$ 1^λ $(\in \mathfrak{B})$ is a B-right-homomorphism of A into B.

Proof. Let β be an arbitrary element of $\mathfrak{B}$. For $x \in A$ we have

$$x^\lambda \beta = x^{\beta\lambda} = 1^{(x^\beta)_L\lambda} = 1^\lambda (x^\beta)_L\,,$$

since λ is $\mathfrak{B}$-(whence $\mathfrak{B}_0$-) homomorphic (and β (naturally) $\in \mathfrak{B}$ and $(x^\beta)_L$ $(\in A_L) \in \mathfrak{B}_0$). Hence, for any $y \in A$,

$$y^{x^\lambda \beta} = y^{1^\lambda (x^\beta)_L} = x^\beta y^{1^\lambda}\,.$$

Here $y^{x^\lambda} = xy^{1^\lambda}$ as we see by taking the unit element of $\mathfrak{B}$ as β in this relation. So we obtain

$$(xy^{1^\lambda})^\beta = x^\beta y^{1^\lambda}\,.$$

As β is an arbitrary element of $\mathfrak{B}$ and x is an arbitrary element of A, we have $(y^{1^\lambda})_R \in \mathrm{Hom}_{\mathfrak{B}}(A, A) = B_R$ and $y^{1^\lambda} \in B$. This proves that 1^λ maps A into B. 1^λ is B_R-homomorphic since $1^\lambda \in \mathfrak{B}$ and $\mathfrak{B}_0 \subset \mathrm{Hom}_B(A_B, A_B)$.

Proposition 1. *Suppose* $A_L \subset \mathfrak{B}_0$ *and* A *is* $\mathfrak{B}$*-projective. Then the* B*-right-module* A *has* B *as a direct summand, where* $\mathrm{Hom}_{\mathfrak{B}}(A, A) = B_R$.

Proof. By Lemma 1 there is an element λ in $\mathrm{Hom}_{\mathfrak{B}}(A, \mathfrak{B})$ such that $\lambda\varphi$ is identical on A. We have in particular $(1^\lambda)^\varphi = 1^{\lambda\varphi} = 1$, and this means, by our definition of φ, $1^{1^\lambda} = 1$. As 1^λ is B-right-homomorphic, we have $b^{1^\lambda} = b$ for all $b \in B$. Thus 1^λ is a B-right-homomorphism of A onto B which is identical on B. Hence

$$A = B \oplus \mathrm{Ker}\, 1^\lambda\,,$$

proving our proposition.

Proposition 1 being thus proved, the implication i)+ii)+iii)$\Rightarrow$vii) is now clear, since ii) implies $A_L \subset \mathfrak{B}_0 = \mathfrak{B}$. In fact, we have

Corollary. *Assume* i) *and* ii) (*i.e.* $\mathrm{Hom}_{\mathfrak{B}}(A, A) = B_R$ *and* $\mathrm{Hom}_B(A_B, A_B) = \mathfrak{B}$). *Then* A *is* $\mathrm{Hom}_B(A_B, A_B)$*-projective if and only if the* B*-right-module* A *has* B *as a direct summand.*

The "if" part is evident, because our condition certainly implies $\mathfrak{T}_{B_R} = B_R$ (i.e. vii)$\Rightarrow$vi), as we obseaved before) and this implies the

$\mathrm{Hom}_B(A_B, A_B)$-($f.g.$-) projectivity of A (i. e. ii)+vi)$\Rightarrow$iii), also observed before).

§6. $\mathfrak{B}$-submodules of A

Proposition 1 may be generalized to

Proposition 2. *Let the notations and assumptions be as in Proposition 1. If M is a $\mathfrak{B}$-submodule of A, then N has $\mathfrak{m}=B\cap M$ as a direct summand; here $\mathfrak{m}$ is a left-ideal of B and satisfies $A\mathfrak{m}\subset M$. If conversely $\mathfrak{m}$ is a left-ideal of B, then $M=A\mathfrak{m}$ is a $\mathfrak{B}$-submodule of A and satisfies $B\cap M=\mathfrak{m}$.*

If M is a $\mathfrak{B}$-submodule of A which is B_R-allowable too, then $\mathfrak{m}=B\cap M$ is a two-sided ideal of B and is a direct summand of M as a B_R-module. For a two-sided ideal $\mathfrak{m}$ of B the $\mathfrak{B}$-submodule $M=A\mathfrak{m}$ of A is evidently B_R-allowable too.

Proof. With the same $\lambda\in\mathrm{Hom}_{\mathfrak{B}}(A, \mathfrak{B})$ as in the proof of Proposition 1, 1^λ ($\in\mathfrak{B}$) maps A B_K-homomorphically onto B and is idempotent; we have $A=B\oplus\mathrm{Ker}\,1^\lambda=A^{1^\lambda}\otimes A^{(I-1^\lambda)}$ where I denotes the unit element of $\mathfrak{B}$ (operating identically on A). For any $\mathfrak{B}$-submodule M of A we have evidently $M=M^{1^\lambda}\oplus M^{(I-1^\lambda)}$. Here $M^{1^\lambda}\subset M$ and indeed$=A^{1^\lambda}\cap M=B\cap M$. Moreover, as $A_L\subset\mathfrak{B}_0$, we have $AM=M$, $A(B\cap M)\subset M$ and $B(B\cap M)\subset B\cap AM=B\cap M$.

Consider conversely a left-ideal $\mathfrak{m}$ in B. For any element β of $\mathfrak{B}$ we have, since β is B_R-whence $\mathfrak{m}_R$-homomorphic,

$$(A\mathfrak{m})^\beta = A^\beta\mathfrak{m}\subset A\mathfrak{m}\,.$$

Hence $A\mathfrak{m}$ is a $\mathfrak{B}$-submodule of A, and we have thus $A\mathfrak{m}=(A\mathfrak{m})^{1^\lambda}\oplus(A\mathfrak{m})^{(I-1^\lambda)}$ with $B\cap A\mathfrak{m}(A\mathfrak{m})^{1^\lambda}=A^{1^\lambda}\mathfrak{m}=B\mathfrak{m}=\mathfrak{m}$.

If M is a B_R-submodule, then both M^{1^λ} and $M^{(I-1^\lambda)}$ are B_R-allowable, since both 1^λ, $I-1^\lambda$ commute with all elements of B_R, and M^{1^λ} is thus a right-ideal in B. So, $M^{1^\lambda}=B\cap M$ is a two-sided ideal of B in case M is $(\mathfrak{B}, B)$-allowable.

In case A is $\mathfrak{B}$-Galois over B, we can sharpen the first part of Proposition 2 so as to have the equality $A\mathfrak{m}=M$. Thus, firstly,

Proposition 3. *If A is $\mathfrak{B}$-Galois over a subring B, then*

$$M\approx A\otimes_R\mathrm{Hom}_{\mathfrak{B}}(A, M)$$

for any $\mathfrak{B}$-right-module M by the natural map $A\otimes_B\mathrm{Hom}_{\mathfrak{B}}(A, M)\to M$. Conversely, if B is a subring of a ring A if $\mathfrak{B}$ is a (right-) operator ring *of the module A such that* $\mathrm{Hom}_{\mathfrak{B}}(A, A) = B_R$ *and A is* $\mathfrak{B}$*-f.g. projective, and if the natural map* $A \otimes_B \mathrm{Hom}_{\mathfrak{B}}(A, M) \to M$ *is epimorphic for every* $\mathfrak{B}$*-module M, then A is* $\mathfrak{B}$*-Galois over B.*

Proof. The first half is merely a special cases of [1], Prop. A. 6 (the second part), e. g.; replace E, Ω, Γ there by our $A, \mathfrak{B}, B_R$ (and observe that our notations are left-light symmetric to those there). To prove the second half of our proposition, take $\mathfrak{B}$ itself as M. The image of the map $A \otimes_B \mathrm{Hom}_{\mathfrak{B}}(A, \mathfrak{B})$ is nothing else as $A^{\mathrm{Hom}_{\mathfrak{B}}(A, \mathfrak{B})} = \mathfrak{T}_{\mathfrak{B}}$. Hence our second assertion follows immediately from our criterion (I) in § 1.

Proposition 4. *Let A be* $\mathfrak{B}$*-Galois over B. If M is a* $\mathfrak{B}$*-submodule of A, then*

$$M = A\mathfrak{m} \quad \textit{with} \quad \mathfrak{m} = B \cap M;$$

(here $\mathfrak{m}$ is a left-ideal of B and M has $\mathfrak{m}$ as a direct summand. If conversely $\mathfrak{m}$ is a left-ideal of B, then $M = A\mathfrak{m}$ is a $\mathfrak{B}$-submodule of A and satisfies $B \cap M = \mathfrak{m}$. If M is a $\mathfrak{B}$-submodule of A which is B_R-allowable too, then (and only then) $\mathfrak{m} = B \cap M$ is a two-sided ideal of B, and is a direct summand of M as a B_R-module).

Proof. In view of Proposition 2 we have merely to prove the first assertion (outside of parentheses). Now, $\mathrm{Hom}_{\mathfrak{B}}(A, M) \subset \mathrm{Hom}_{\mathfrak{B}}(A, A) = B_R$ and we see readily

$$\mathrm{Hom}_{\mathfrak{B}}(A, M) = (B \cap M)_R = \mathfrak{m}_R .$$

The image of $A \otimes_B \mathrm{Hom}_{\mathfrak{B}}(A, M) \to M$ is thus $A^{\mathfrak{m}_R} = A\mathfrak{m}$ and by Proposition 3 it coincides with M as is asserted.

REMARK 4. Proposition 4 establishes in particular a 1-1 correspondence between left-ideals (resp. two-sided ideals) of B and $\mathfrak{B}$-submodules (resp. $\mathfrak{B}B$-submodules) of A. Similarly, on the other hand, left-ideals (resp. two-sided ideals) $\mathfrak{M}$ of $\mathfrak{B}$ correspond 1-1 to B_R-submodules (resp. $\mathfrak{B}B_R$-submodules) M of A, by $\mathfrak{M} \to M = A^{\mathfrak{M}} = A \otimes_{\mathfrak{B}} \mathfrak{M}$ $(\subset A \otimes_{\mathfrak{B}} \mathfrak{B} = A)$, $M \to \mathfrak{M} = \mathrm{Hom}_{B_R}(A, M)$ $(\approx M \otimes_{B_R} \mathrm{Hom}_{B_R}(A, B_R) \approx M \otimes_{B_R} \mathrm{Hom}_{\mathfrak{B}}(A, \mathfrak{B}))$ $(\subset \mathrm{Hom}_{B_R}(A, A) = \mathfrak{B})$. These are naturally special cases of category-isomorphisms discussed in Morita [16], Auslander-Goldmann [1], e. g. In particular, $\mathfrak{m} \leftrightarrow M \leftrightarrow \mathfrak{M}$ establishes a 1-1 correspondence between two-sided ideals in B and those in $\mathfrak{B}$; see [1] Prop. A. 5.

Corollary. *Let A be* $\mathfrak{B}$*-Galois over B. Suppose there are given a module-homomorphism* μ *of A into a second ring A' and a ring-homomor-*

phism ν *of* $\mathfrak{B}$ *into an operator-ring* $\mathfrak{B}'$ *of* A' *such that* $(a^{\beta})^{\mu}=(a^{\mu})^{\beta^{\nu}}$ *for all* $a\in A$, $\beta\in\mathfrak{B}$. *If* μ *is monomorphic on* B, *then* μ *is so on the whole of* A.

Proof. Consider $M=\mathrm{Ker}\,\mu$, which is a $\mathfrak{B}$-submodule of A.

Our Proposition 3 is a generalization of Auslander-Goldman [2], Theorem 3.1 and Nakayama [22], Theorem 2. Proposition 4 generalizes [2], Cor. 3.2 as well as [22], Prop. 2, and our Corollary corresponds to a partial contention of [2], Cor. 3.4. As for the further parts of the papers [2] and [22] we wish to come back in a subsequent work to comprise them into our present general aspect.

NAGOYA UNIVERSITY

(Received March 5, 1963)

References

[1] M. Auslander—O. Goldman: *Maximal orders,* Trans. Amer. Math. Soc. **97** (1960), 1-24.

[2] M. Auslander—O. Goldman: *The Brauer group of a commutative ring,* Trans. Amer. Math. Soc. **97** (1960), 367-409.

[3] G. Azumaya: *Galois theory for uni-serial rings,* J. Math. Soc. Japan **1** (1949-50), 130-146.

[4] G. Azumaya: *On maximally central algebras,* Nagoya J. Math. **2** (1951), 119-150.

[5] G. Azumaya—T. Nakayama: *On absolutely uni-serial algebras,* Jap. J. Math. **19** (1948), 263-273.

[6] H. Cartan: *Théorie de Galois pour les corps non-commutatifs,* Ann. École Norm. Sup. **64** (1947), 59-77.

[7] C. W. Curtis: *On commuting rings of endomorphisms,* Canad. J. Math. **8** (1956), 271-291.

[8] J. Dieudonné: *La théorie de Galois des anneaux simples et semi-simples,* Comm. Math. Helv. **21** (1948), 154-184.

[9] J. Dieudonné: *Progrès et problemes de la théorie de Galois,* Coll. Internat. CNRS Paris **24** (1950), 169-172.

[10] G. Hochschild: *Double vector spaces over division rings,* Amer. J. Math. **71** (1949), 443-460.

[11] G. Hochschild: *Automorphisms of simple algebras,* Trans. Amer. Math. Soc. **69** (1950), 292-301.

[12] N. Jacobson: *The fundamental theorem of Galois theory for quasifields,* Ann. of Math. **41** (1940), 1-7.

[13] N. Jacobson: *Note on division rings,* Amer. J. Math. **66** (1947), 27-36.

[14] N. Jacobson: *An extension of Galois theory to non-normal and non-separable fields,* Amer. J. Math. **66** (1947), 27-36.

[15] F. Kasch: *Über den Endomorphismenring eines Vektorraumes und den Satz von der Normalbasis*, Math. Ann. **126** (1953), 447-463.

[16] K. Morita: *Duality for modules and its applications to rings with minimum condition*, Sci. Rep. Tokyo Kyoiku Univ. **6** (1958), 83-142.

[17] T. Nagahara—H. Tominaga: *Galois theory of division rings*, Math. J. Okayama Univ. **6** (1956), 1-21; II, ibid. **7** (1957), 169-172.

[18] T. Nakayama: *Galois theory for general rings with minimum condition*, J. Math. Soc. Japan **1** (1949-50), 203-216.

[19] T. Nakayama: *Note on double-modules over arbitrary rings*, Amer. J. Math. **74** (1952), 645-655.

[20] T. Nakayama: *Galois theory of simple rings*, Trans. Amer. Math. Soc. **73** (1952), 276-292.

[21] T. Nakayama: *Generalized Galois theory for rings with minimum condition*, Amer. J. Math. **73** (1951), 1-12; II ibid. **77** (1955), 1-16.

[22] T. Nakayama: *Wedderburn's theorem, weakly normal rings, and the semi-group of ring-classes*, J. Math. Soc. Japan **5** (1953), 154-170.

[23] N. Nobusawa: *An extension of Krull*'s *Galois theory to division rings*, Osaka Math. J. **7** (1955), 1-6.

[24] A. Rosenberg-D. Zelinsky: *Galois theory of continuous transformation rings*, Trans. Amer. Math. Soc. **79** (1955), 429-452.

[25] K. Shoda: *Über die Galoissche Theorie der halbeinfachen hyperkomplexen Systemen*, Math. Ann. **107** (1932), 252-258.

[26] H. Tominaga: *Galois theory of simple rings*, Math. J. Okayama Univ. **6** (1956-57), 29-48: II, ibid. **6** (1956-57), 153-170.