NON-NORMAL GALOIS THEORY FOR NON-COMMUTATIVE AND NON-SEMISIMPLE RINGS

TADASI NAKAYAMA

THE purpose of the present work is to give, as a continuation of the writer's study of Galois theory for general rings ([8], [9], [10]), a kind of Galois theory for general, non-commutative and non-semisimple rings, which includes, at least in its main features, the Kaloujnine-Jacobson Galois theory of non-normal fields ([3]; cf. [4], [5]). To deal with the non-commutativity we bring to the fore certain double-moduli rather than self-composites, while the non-semisimplicity is manipulated by the method and idea used in the writer's above mentioned study on (normal) Galois theory and commuter systems of non-semisimple rings. (For the normal Galois theory of rings cf. [1], [2], [6], [7], [11], besides the above.) Some of our arguments may even serve to make some simplification in Jacobson's treatment of ordinary fields.

1. Galois ring and Galois system of module-endomorphisms of a ring. Throughout this paper a ring means a ring with unit element and its module, right or left, one for which the unit element is the identity operator.

Let A be a semiprimary ring. An A-right-, say, module $\mathfrak{m}$ is called regular when a direct sum of a certain (finite) number, say v, of its copies is (A-) isomorphic to the direct sum of a certain number, say u, of copies of the A-right-module A. The A-endomorphism ring A^* of $\mathfrak{m}$ is nothing but the commuter ring of A in the absolute endomorphism ring of $\mathfrak{m}$. We have

LEMMA. *The number u/v,* called the (A-) rank of the regular module $\mathfrak{m}$, *is determined uniquely and characterizes the structure of* $\mathfrak{m}$. *A^* is semiprimary and* $\mathfrak{m}$ *is also regular with respect to A^*. The A^*-rank of* $\mathfrak{m}$ *is inverse to the A-rank. The A^*-endomorphism ring of* $\mathfrak{m}$ *coincides with A.*

If $\mathfrak{m}$ is also regular with respect to a (semiprimary) subring B, then any other regular A-right-module $\mathfrak{n}$ is regular with respect to B too and the ratio of the A-ranks of $\mathfrak{m}$, $\mathfrak{n}$ is equal to that of their B-ranks.

We note further that if A satisfies the minimum condition for right-ideals then A^* satisfies the same for left-ideals.

Throughout this paper, R will denote a ring satisfying the minimum con-

Received December 1, 1949, revised March 17, 1950. *Addendum in revision.* After the submission of the present paper to the Journal, the writer had access to a paper by G. Hochschild, entitled "Double vector spaces over division rings" (Amer. Jour. Math., vol. 71 (1949)), closely related to the present one. The idea of considering in the non-commutative case certain double-moduli, rather than self-composites, has been exploited there already. However, in the present work we dealt with non-division rings, in fact with general non-semisimple rings.

dition for left-ideals.[1] Let **A** be its absolute endomorphism ring, that is, the endomorphism ring of R as module without operator domain. Denote by R_l, R_r, or generally X_l, X_r with a subset X of R, the set of left-, right-multiplications of R, or X, upon R. Let **B** be a subring of **A**, i.e. a certain ring of (module-)endomorphisms of R, which contains R_l. When further the direct sum of a certain number, say s, of copies of R is (**B**-) isomorphic to the **B**-right-module **B** itself, i.e., when R is **B**-regular with s^{-1} as rank, we call **B** a *Galois ring* of module-endomorphisms of R. Here **B** satisfies the minimum condition for R_l-right-submoduli, whence certainly that for its right-ideals. The commuter ring $V(\mathbf{B})$ of **B** in **A**, i.e. the **B**-endomorphism ring of R, is contained in $V(R_l) = R_r$, and so has a form S_r with a subring S of R. R is S_r-regular with rank s, that is, R has an independent S-right-basis of s terms. Moreover, $V(S_r) = \mathbf{B}$.

If conversely S is a subring of R such that R possesses an independent (finite) S-right-basis, of s terms, say, then S certainly satisfies, together with R, the minimum condition for left-ideals[2] and $V(S_r) = \mathbf{B}$ is a Galois ring in the above sense. And $S_r = V(\mathbf{B})$. Thus

THEOREM 1. *Galois rings* **B** *of module-endomorphisms and subrings S such that R has independent right-basis over S are in* 1-1 *dual correspondence, by* $V(\mathbf{B}) = S_r$, $\mathbf{B} = V(S_r)$. *The* **B**-*rank of R is inverse to the S_r- (that is, S-right-) of R.*

Further, by the Lemma, applied to the **B**-, and R_l-module **B**, instead of A-, and B-module $\mathfrak{n}$, we see that **B** is R_l (right-) regular and the R_l-rank of **B** is equal to the S-rank s of R. Hence

THEOREM 2. *The Galois ring* **B** *has an independent right-basis of s terms over its subring R_l, where $1/s$ is the* **B**-*rank of R (that is, s is the S_r-rank of R):*

$$\mathbf{B} = \beta_1 R_l \oplus \beta_2 R_l \oplus \ldots \oplus \beta s R_l.$$

We call such an independent right-basis of a Galois ring over R a *Galois system* of module-endomorphisms of R. Our next task will then be the construction of such a Galois system.

2. Construction of Galois system. Let $\mathfrak{m}$ be a right-module of R and $\mathfrak{n}$ be a left-module of R. By their direct product $\mathfrak{m} \times \mathfrak{n} = \mathfrak{m} \times_R \mathfrak{n}$ we mean, as usual, a module generated (freely) by symbols uv ($u \in \mathfrak{m}$, $v \in \mathfrak{n}$) with relations

$$(u_1 + u_2)v = u_1 v + u_2 v, \qquad u(v_1 + v_2) = uv_1 + uv_2,$$
$$(uz)v = u(zv) \quad (z \in R).$$

[1]We can develop our whole theory also under the assumpton that R, $\boldsymbol{B}$, S (see below) are semiprimary rings, or even under a much weaker assumption as G. Azumaya has kindly pointed out. However, the writer prefers to present the theory in the form below where R (and then S) satisfies the minimum condition, since the assumption does not spoil the essential feature of the theory.

[2]Consider $R\mathfrak{l}$ with left-ideals $\mathfrak{l}$ of S.

https://doi.org/10.4153/CJM-1951-025-5 Published online by Cambridge University Press

If $\mathfrak{n}$ is an R-double-module the product $\mathfrak{m} \times \mathfrak{n}$ is, in a natural manner, an R-right-module, and if both $\mathfrak{m}$, $\mathfrak{n}$ are R-double-modules then $\mathfrak{m} \times \mathfrak{n}$ becomes an R-double-module. In case $\mathfrak{m}$ possesses an independent R-right-basis $(u_1, u_2, \ldots, u_m)$ we have $\mathfrak{m} \times \mathfrak{n} = u_1\mathfrak{n} \oplus u_2\mathfrak{n} \oplus \ldots \oplus u_m\mathfrak{n}$. If also $\mathfrak{n}$ possesses an independent R-left-basis $(v_1, v_2, \ldots, v_n)$, then $\mathfrak{m} \times \mathfrak{n} = \sum^0{}_{ij} u_i R v_j$.

Now, let S be a subring of R such that R has an independent S-right-basis of s, say, terms. We consider R as S-right-, and S-left-module, and we want to construct the direct self-product $R \times R$ over S. However, to avoid ambiguity in notation, we introduce two (ring-) isomorphisms σ, τ of R. Putting $zx^\sigma = (zx)^\sigma, x^\sigma z = (xz)^\sigma, x^\tau z = (xz)^\tau, zx^\tau = (zx)^\tau$ $(x, z \in R)$ we consider R^σ, R^τ as R-double-moduli. We then construct

$$(1) \qquad R^\sigma \times R^\tau = R^\sigma \times_S R^\tau = x_1{}^\sigma R^\tau \oplus x_2{}^\sigma R^\tau \oplus \ldots \oplus x_s{}^\sigma R^\tau,$$

where $(x_1, x_2, \ldots, x_s)$ is an independent S-right-basis of R.

According to (1) we have, for each $z \in R$,

$$(2) \qquad z^\sigma 1^\tau = x_1{}^\sigma \beta_1(z)^\tau + x_2{}^\sigma \beta_2(z)^\tau + \ldots + x_s{}^\sigma \beta_s(z)^\tau, \qquad \beta_h(z) \in R.$$

$\beta_h(z)$ are determined uniquely by z, and β_h: $z \to \beta_h(z)$ $(h = 1, 2, \ldots, s)$ are module-endomorphisms of R. Moreover, for $a \in S$ we have $(za)^\sigma 1^\tau = z^\sigma a^\tau = \sum_h x_h{}^\sigma (\beta_h(z)a)^\tau$. Thus $\beta_h(z)a = \beta_h(za)$, or $\beta_h a_r = a_r \beta_h$, and so β_h are S_r-endomorphisms of R, and $\beta_h \in V(S_r) = \mathbf{B}$. We assert that they form a Galois system belonging to S. Observe first that

$$x_i{}^\sigma 1^\tau = x_1{}^\sigma \beta_1(x_i)^\tau + x_2{}^\sigma \beta_2(x_i) + \ldots + x_s{}^\sigma \beta_s(x_i)$$

and so
$$\beta_h(x_i) = \delta_{hi} \qquad \text{(Kronecker } \delta\text{)}.$$

Therefore $\beta_h y_l$, with $y \in R$, maps x_i upon $y\delta_{hi}$, and $\sum_h \beta_h y_{hl}$ $(y_h \in R)$ maps x_i upon y_i. It follows that $\beta_1, \beta_2, \ldots, \beta_s$ are R_l-right-independent. Moreover, since y_h may be taken arbitrarily, the totality of $\sum_h \beta_h y_{hl}$ coincides with the whole $V(S_r) = \mathbf{B}$;

$$(3) \qquad V(S_r) = \mathbf{B} = \beta_1 R_l \oplus \beta_2 R_l \oplus \ldots \oplus \beta_s R_l.$$

If $z = \sum_h x_h a_h$ $(a_h \in S)$ then $\beta_h(z) = a_h$. Thus

THEOREM 3. *The s (module-)endomorphisms β_h of R defined in* (2) *form a Galois system belonging to the subring S. Here $\beta_h(R) = S$ for each h. Moreover $\beta_h(z) = 0$ $(h = 1, 2, \ldots, s)$ (that is, $z^\sigma 1^\tau = 0$) implies $z = 0$.*

3. Double-moduli and their relation moduli. Although Theorems 1, 2, 3 already give the main features of our Galois theory, it is useful as well as important to extend the above construction of a Galois system to the case of general double-moduli of a certain type and thus obtain a characterization of a Galois ring (Theorem 7). It is our purpose to generalize Jacobson's theory of self-composites of (commutative) fields, but we have to adopt a somewhat different formulation and method, because of the non-commutativity and the non-semisimplicity of R.

Let $\mathfrak{M}$ be a double-module of R having an independent R-right-basis, and let u_0 be an element of $\mathfrak{M}$. Let $(u_1, u_2, \ldots, u_m)$ be an independent R-right-basis of $\mathfrak{M}$, and put

$$zu_0 = u_1\mu_1(z) + u_2\mu_2(z) + \ldots + u_m\mu_m(z) \tag{4}$$

for $z \in R$; $\mu_1, \mu_2, \ldots, \mu_m$ are module-endomorphisms of R.

Consider further a second R-double-module $\mathfrak{N}$ with an independent R-right-basis $(v_1, v_2, \ldots, v_n)$, and its element v_0. Introduce module-endomorphisms $\nu_1, \nu_2, \ldots, \nu_n$ of R correspondingly by

$$zv_0 = v_1\nu_1(z) + v_2\nu_2(z) + \ldots + v_n\nu_n(z). \tag{5}$$

Suppose that there exists an (R-two-sided) homomorphic mapping φ of $\mathfrak{M}$ in $\mathfrak{N}$ which maps u_0 on v_0; $u_0^\varphi = v_0$. Put

$$u_h^\varphi = \sum_k v_k x_{kh} \qquad (x_{kh} \in R) \tag{6}$$

Then φ maps $zu_0 = \sum u_h\mu_h(z)$ on $\sum v_k x_{kh}\mu_h(z)$, while $(zu_0)^\varphi = zu_0^\varphi = zv_0$ $= \sum v_k\nu_k(z)$ too. So $\nu_k(z) = \sum x_{kh}\mu_h(z)$, or

$$\nu_k = \sum_h \mu_h x_{khl}. \tag{7}$$

Thus

$$\nu_1R_l + \nu_2R_l + \ldots + \nu_nR_l \subseteq \mu_1R_l + \mu_2R_l + \ldots + \mu_mR_l. \tag{8}$$

If we consider, firstly, the case that $\mathfrak{M} = \mathfrak{N}$ and φ is the identity mapping, our observation shows that the module

$$\sum_h \mu_hR_l = \mu_1R_l + \mu_2R_l + \ldots + \mu_mR_l \tag{9}$$

does not depend on the special choice of the independent basis $(u_1, u_2, \ldots, u_m)$. We call the module (9) the *relation module* of u_0 in $\mathfrak{M}$.

If we consider secondly the case that $\mathfrak{M} \subseteq \mathfrak{N}$ and φ is again the identity mapping, we find that the relation module of u_0 in a module $\mathfrak{N}$ containing $\mathfrak{M}$ (and having an independent R-right-basis) is contained in that of u_0 in $\mathfrak{M}$. If here $\mathfrak{M}$ is a direct summand in $\mathfrak{N}$ as R-right-module, then the relation moduli of u_0 in $\mathfrak{M}$ and $\mathfrak{N}$ coincide. This last remark, which is rather useful, we see readily by observing that $\mathfrak{N}/\mathfrak{M}$ is regular with integral rank and so $\mathfrak{N}$ has an independent R-right-basis which contains a basis for $\mathfrak{M}$; in fact, every independent R-right-basis of $\mathfrak{M}$ may be extended to one of $\mathfrak{N}$.

Now, if in particular Ru_0 contains an independent R-right-basis of $\mathfrak{M}$, then the m module-endomorphisms $\mu_1, \mu_2, \ldots, \mu_m$ of R are R_l-right-independent, and moreover any independent R_l-right-basis of the relation module is obtained from suitable choice of independent R-right-basis of $\mathfrak{M}$. Let namely

$$u_i = t_iu_0 \qquad (t_i \in R). \tag{10}$$

https://doi.org/10.4153/CJM-1951-025-5 Published online by Cambridge University Press

Then

$$(11) \qquad \mu_h(t_i) = \delta_{hi}$$

and t_i is mapped on y_i by $\sum \mu_h y_{hl}$, which implies the right-independence of $\mu_1, \mu_2, \ldots, \mu_m$ over R_l.

Further, under the same assumption also the converse of the above relationship between the inclusion (8) and homomorphism is valid. Assuming (8), where μ and ν are given in (4), (5), and also (7), we define φ as R-right-homomorphic mapping of $\mathfrak{M}$ into $\mathfrak{N}$ by virtue of (6). Then

$$u_0^\varphi = (\sum u_h \mu_h(1))^\varphi = \sum v_k x_{kh} \mu_h(1) = \sum v_k \nu_k(1) = v_0.$$

More generally

$$(zu_0)^\varphi = (\sum u_h \mu_h(z))^\varphi = \sum v_k x_{kh} \mu_h(z) = \sum v_k \nu_k(z) = zv_0.$$

Our purpose is to show that φ is also R-left-homomorphic, and we may, for that purpose, assume $u_1, u_2, \ldots, u_m \in Ru_0$. On putting $u_h = t_h u_0$ $(t_h \in R)$, as in (10), we have

$$u_h^\varphi = (t_h u_0)^\varphi = t_h v_0 = \sum v_k \nu_k(t_h).$$

Comparing this with (6) we obtain

$$x_{kh} = \nu_k(t_h).$$

Therefore

$$\begin{aligned}(zu_h)^\varphi = (zt_h u_0)^\varphi &= (\sum u_i \mu_i(zt_h))^\varphi = \sum v_k x_{ki} \mu_i(zt_h) \\ &= \sum v_k \nu_k(zt_h) = zt_h v_0 = z(\sum v_k \nu_k(t_h)) = z(\sum v_k x_{kh}) = zu_h^\varphi.\end{aligned}$$

This shows that the mapping is R-left-homomorphic, as is desired.

On returning to the case of general u_0 which may not, necessarily, even generate $\mathfrak{M}$, we show further that its relation module $\sum \mu_h R_l$ in $\mathfrak{M}$ is R_l-left-allowable too. For, if we put

$$(12) \qquad zu_h = \sum u_j \rho_{jh}(z)$$

then $\sum u_j \mu_j(zy) = zyu_0 = z \sum u_h \mu_h(y) = \sum u_j \rho_{jh}(z) \mu_h(y)$ and

$$(13) \qquad z_l \mu_j = \mu_h(\rho_{jh}(z))_l,$$

which proves our assertion.

Here

$$(14) \qquad z \to (\rho_{jh}(z))$$

is a self-representation of R, i.e. a (matric) representation of R in R. Consider the relation module of a basis element, say $u_0 = u_i$. Then $\mu_h = \rho_{hi}$, and the relation module $\sum \mu_h R_l$ is nothing but the R_l-right-module generated by $\rho_{1i}, \rho_{2i}, \ldots, \rho_{mi}$; this module may thus be called the *i-column module* of the representation (14).

THEOREM 4. *Let $\mathfrak{M}$ be an R-double-module possessing an independent R-right-basis. The relation module $\sum \mu_h R_l$ in* (9) *of an element u_0 in $\mathfrak{M}$, with μ_i given as in* (4), *is independent of the special choice of the independent R-right-basis (u_h) of $\mathfrak{M}$, and is a double-module of R_l. If in particular Ru_0 contains an independent R-right-basis, then $\mu_1, \mu_2, \ldots, \mu_m$ are R_l-right-independent. Let $\mathfrak{N}$ be a second R-double-module with an independent R-right-basis. If φ is an R-two-sided homomorphic mapping of $\mathfrak{M}$ into $\mathfrak{N}$, then the relation module $\sum \nu_k R_l$ of $v_0 = u_0^{\varphi}$ in $\mathfrak{N}$ is contained in the relation module $\sum \mu_h R_l$ of u_0 in $\mathfrak{M}$ (see* (8)). *In particular, if $\mathfrak{M} \subseteq \mathfrak{N}$ then the relation module of u_0 in $\mathfrak{N}$ is contained in that of u_0 in $\mathfrak{M}$. If $\mathfrak{M}$ is direct summand in $\mathfrak{N}$ as R-right-module, then these relation moduli coincide. In case Ru_0 contains an independent R-right-basis of $\mathfrak{M}$ the inclusion $\sum \nu_k R_l \subseteq \sum \mu_h R_l$ is also sufficient in order that there exist an R-two-sided homomorphic mapping of $\mathfrak{M}$ into $\mathfrak{N}$ which maps u_0 upon v_0. Thus the structure of an R-double-module which has an independent R-right-basis contained in Ru_0, with an element u_0 of the module, is uniquely determined by its relation module of the element u_0.*

The last statement means that, if two self-representations of R are defined by R-double-moduli possessing independent R-right-bases contained in the R-left-moduli generated, respectively, by their first, say, basis elements and if their 1-column moduli coincide, then the representations are equivalent (in the usual sense of equivalence of representations).

Further we obtain readily

THEOREM 5. *Let $\mathfrak{M}$, $\mathfrak{N}$ be R-double-moduli, with independent R-right-bases, and let $u_0 \in \mathfrak{M}$, $v_0 \in \mathfrak{N}$. Consider the direct sum $\mathfrak{M} \oplus \mathfrak{N}$ and its element $w_0 = u_0 + v_0$. Then the relation module of w_0 in $\mathfrak{M} \oplus \mathfrak{N}$ is the sum, not necessarily direct, $\sum \mu_h R_l + \sum \nu_k R_l$ of the relation moduli $\sum \mu_h R_l$, $\sum \nu_k R_l$ of u_0, v_0 in $\mathfrak{M}$, $\mathfrak{N}$.*

We next consider the direct product $\mathfrak{M} \times \mathfrak{N} = \mathfrak{M} \times_R \mathfrak{N}$ of $\mathfrak{M}$, $\mathfrak{N}$ and its element $w_0 = u_0 v_0$. We have

THEOREM 6. *The relation module of $w_0 = u_0 v_0$ in $\mathfrak{M} \times \mathfrak{N} = \mathfrak{M} \times_R \mathfrak{N}$ coincides with the product module $(\sum \mu_h R_l)(\sum \nu_k R_l) = \sum \mu_h \nu_k R_l$ of the relation moduli $\sum \mu_h R_l$, $\sum \nu_k R_l$ of u_0, v_0 in $\mathfrak{M}$, $\mathfrak{N}$.*

For, $\mathfrak{M} \times \mathfrak{N} = u_1 \mathfrak{N} \oplus u_2 \mathfrak{N} \oplus \ldots \oplus u_m \mathfrak{N} = u_1 v_1 R \oplus u_1 v_2 R \oplus \ldots \oplus u_m v_n R$, and $u_1 v_1, u_1 v_2, \ldots, u_m v_n$ are R-right-independent. And

$$z w_0 = z u_0 v_0 = \sum u_h \mu_k(z) v_0 = \sum u_h v_k \nu_k(\mu_h(z)).$$

This shows that the relation module of w_0 in $\mathfrak{M} \times \mathfrak{N}$ is really $\sum \mu_h \nu_k R_l$. But this is the product module $(\sum \mu_h R_l)(\sum \nu_k R_l)$, since $\sum \nu_k R_l$ is R_l-left-allowable too.

Now, let S be the totality of elements a in R such that $a u_0 = u_0 a$. S is a subring of R. If $a \in S$ then

$$z a u_0 = z u_0 a = u_1 \mu_1(z) a + u_2 \mu_2(z) a + \ldots + u_m \mu_m(z) a,$$

https://doi.org/10.4153/CJM-1951-025-5 Published online by Cambridge University Press

whence $\mu_h(za) = \mu_h(z)a$, or $a_r\mu_h = \mu_k a_r$. Thus the relation module $\sum\mu_h R_l$ is contained in $V(S_r)$. If conversely a is an element of R such that μ_h are a_r-endomorphisms, then

$$zau_0 = \sum u_h\mu_h(za) = \sum u_h\mu_h(z)a = zu_0a \qquad (z \in R),$$

in particular $au_0 = u_0a$, and so $a \in S$. Thus

$$(15) \qquad S = \{a \in R;\ au_0 = u_0a\} = \{a \in R;\ \mu_h a_r = a_r\mu_h (h = 1, 2, \ldots, m)\}.$$

Suppose now that Ru_0 contains an independent R-right-basis of $\mathfrak{M}$ and that our relation module $\sum\mu_h R_l$ forms a ring. If $\mathfrak{N} = Rv_0R$ is a second R-double-module which is isomorphic to $\mathfrak{M}$ by $u_0 \leftrightarrow v_0$, then the ring assumption of $\sum\mu_h R_l$ means, by Theorems 4, 6, that $u_0 \to u_0v_0$ gives an (R-two-sided) homomorphic mapping of $\mathfrak{M}$ into the direct product $\mathfrak{M} \times_R \mathfrak{N}$. Let our basis (u_h) of $\mathfrak{M}$ be taken from Ru_0; put $u_h = t_hu_0$ $(t_h \in R)$, as in (10). Let (v_h) be the corresponding basis of $\mathfrak{N}$. By our mapping of $\mathfrak{M}$ into $\mathfrak{M} \times \mathfrak{N}$ zu_0 should be mapped upon

$$zu_0v_0 = \sum u_h\mu_h(z)v_0 = \sum u_hv_k\mu_k(\mu_h(z)),$$

while $zu_0 = \sum u_h\mu_h(z) = \sum t_hu_0\mu_h(z)$ and this should be mapped on

$$\sum t_hu_0v_0\mu_h(z) = \sum u_hv_0\mu_h(z) = \sum u_hv_k\mu_k(1)\mu_h(z).$$

We have, since u_hv_k are R-right-independent, $\mu_k(\mu_h(z)) = \mu_k(1)\mu_h(z)$. Then

$$\mu_h(z)u_0 = \sum u_k\mu_k(\mu_h(z)) = \sum u_k\mu_k(1)\mu_h(z) = u_0\mu_h(z),$$

hence $\mu_h(z) \in S$. Let (u'_h) be a second independent R-right-basis of $\mathfrak{M}$ and let μ'_h be the corresponding endomorphisms. Put $u_h = \sum u'_kx_{kh}$. Then $\mu'_h(z) = \sum x_{hk}\mu_k(z)$ and in particular $\mu'_h(t_i) = \sum x_{hk}\delta_{ki} = x_{hi}$. Thus $\mu'_h(R) \subseteq S$ $(h = 1, 2, \ldots, m)$ if and only if $x_{hk} \in S$. This last means that $y_{hk} \in S$ for the inverse matrix (y_{hk}) of (x_{hk}). Thus the condition amounts to

$$u'_h \in u_1S \oplus u_2S \oplus \ldots \oplus u_mS = Ru_0S.$$

Here we have, as a matter of fact, $\mu'_h(R) = S$, since the S-right-module generated by x_{hi} $(i = 1, 2, \ldots, m)$ certainly exhausts S.

Conversely, if every μ_h maps R in S, then

$$\mu_k(\mu_h(z)) = \mu_k(1\mu_h(z)) = \mu_k(1)\mu_h(z),$$

whence $\mu_h\mu_k \in \mu_hR_l$, and $\sum\mu_hR_l$ forms a ring.

Further, again under the assumption that $\sum\mu_hR_l$ is a ring and $u_h = t_hu_0 \in Ru_0$, we have

$$\sum t_h\mu_h(z)u_0 = \sum t_hu_0\mu_h(z) = \sum u_h\mu_h(z) = zu_0$$

and $z - \sum t_h\mu_h(z)$ is, for every $z \in R$, in the left-ideal $\mathfrak{l} = \{z \in R,\ zu_0 = 0\}$. Here $t_h (h = 1, 2, \ldots, m)$ are S-right-independent mod $\mathfrak{l}$, as we see readily from $\mu_i(t_h) = \delta_{ih}$. Thus (t_h) forms an independent S-right-basis of R mod $\mathfrak{l}$. If in particular $\mathfrak{l} = 0$, that is, if (the single element) u_0 is R-left-independent, then (t_h) forms an independent S-right-basis of R. Since the R_l-rank m is in that case equal to the S_r-rank of R, our relation module $\sum \mu_h R_l$ must then exhaust the whole Galois ring $V(S_r)$, here we may also argue as in §2 without appealing to the rank relation. So we have

THEOREM 7. *Let $\mathfrak{M} = Ru_0R$ have an independent R-right-basis contained in Ru_0. The relation module of u_0 in $\mathfrak{M}$ forms a ring if*[3] *and only if we may choose such a basis (u_h) so that $\mu_h(R) \subseteq S$ for every h, where S is the subring* (15) *of R; as matter of fact $\mu_h(R) = S$ then. This last is the case, under the ring assumption of the relation module, if and only if $\{u_h\} \subseteq Ru_0S$. Provided that zu_0 $(z \in R)$ vanishes only when $z = 0$, our ring assumption implies also that R has an independent S-right-basis; in fact (t_h) $(h = 1, 2, \ldots, m)$ forms such a basis when (t_hu_0) forms an independent R-right-basis of $\mathfrak{M}$, and moreover the homomorphic mapping $1^\sigma 1^\tau \rightarrow u_0$ of the self-product $R \times_S R = R^\sigma \times_S R^\tau$ of R over S* (§2) *upon $\mathfrak{M}$ becomes an isomorphism. In short, our relation module is a Galois ring if and only if it is a ring and $zu_0 = 0$ implies $z = 0$.*

4. Relationship between relation moduli over R and its subring. Let S be a subring of R and let R possess an independent S-right-basis; $R = x_1S \oplus x_2S \oplus \ldots \oplus x_sS$. Then an R-double-module $\mathfrak{M}$ with an independent R-right-basis $(u_1, u_2, \ldots, u_m)$ is certainly an S-double-module with independent S-right-basis (u_hx_i). Let u_0 be an element of $\mathfrak{M}$ and let its relation module in $\mathfrak{M}$, as R-module, be given by $\sum \mu_h R_l$. We now consider the relation module of u_0 in $\mathfrak{M}$ as S-module. On putting

(16) $$z = x_1\pi_1(z) + x_2\pi_2(z) + \ldots + x_s\pi_s(z) \qquad (\pi_i(z) \in S),$$

we have $zu_0 = \sum u_h\mu_h(z) = \sum_h u\pi_i(\mu_h(z))$. Thus the relation module of u_0 in the S-module $\mathfrak{M}$ is given by

(17) $$\sum_{h,i} \mu_h \pi_i S_l$$

(where μ_h are considered as homomorphisms of S into R).

In case u_0 is one of the basis elements, say u_1, the situation may be described also in terms of representation. Namely, on assuming $x_1 = 1$, without loss of generality, we consider the regular representation $(\lambda_{ij}(z))$ of R in S, with respect to our basis (x_i):

(18) $$zx_j = \sum x_i\lambda_{ij}(z) \qquad (\lambda_{ij}(z) \in S).$$

Denote the self-representation of R defined by our basis $(u_1(= u_0), u_2, \ldots, u_m)$ of $\mathfrak{M}$ by $(\rho_{hk}(z))$, as in (12). The S-(right-)basis (u_hx_i) of $\mathfrak{M}$ defines then the representation

(19) $$(\lambda_{ij}(\rho_{hk}(z)))$$

[3]This "if" part is valid without our assumption of existence of an independent R-right-basis of $\mathfrak{M}$ in Ru_0, or even without assuming $\mathfrak{M} = Ru_0R$.

of degree ms in S. Restricted to S, this gives the self-representation of S defined by the basis $(u_h x_i)$ of S-module $\mathfrak{M}$. Since here $u_1 x_1 = u_0$, our relation module of u_0 in the S-module $\mathfrak{M}$ is obtained as the first, i.e. (1, 1)-, column module of this representation.

THEOREM 8. *The relation module of u_0 in $\mathfrak{M}$ as S-module is given by* (17), *restricted to S, with π_i in* (16). *If in particular $u_0 = u_1$ and $x_1 = 1$, it is also defined as the* (1, 1)*-column module of the self-representation* (19), *restricted to S, of S, where (ρ_{hk}) is the self-representation of R defined by the (R-right-)basis (u_h) of $\mathfrak{M}$ and (λ_{ij}) is the regular representation of R in S defined by the (S-right-)basis (x_i).*

We supplement the theorem with the following observation: Let $\mathfrak{m}$ be an S-double-module with independent S-right-basis. Then there always exists an R-double-module $\mathfrak{M}$ with independent R-right-basis, which contains, as S-double-module, $\mathfrak{m}$, and which contains $\mathfrak{m}$ as S-right-module indeed as direct summand. (Then the relation module of u_0 $(\in \mathfrak{m})$ in $\mathfrak{m}$ coincides with that in $\mathfrak{M}$, as S-module. Therefore it is thus obtained from the relation module of u_0 in R-module $\mathfrak{M}$ by virtue of the above procedure of referring to S in terms of π_i(in (16)).

Let $(v_1, v_2, \ldots, v_n)$ be an independent S-right-basis of $\mathfrak{m}$,

$$\mathfrak{m} = v_1 S \oplus v_2 S \oplus \ldots \oplus v_n S.$$

$\mathfrak{m} \times_S R$ is an R-right-module $v_1 R \oplus v_2 R \oplus \ldots \oplus v_n R$ with $v_1, v_2, \ldots, v_n$ right-independent over R. Therefore

$$R \times_S \mathfrak{m} \times_S R = x_1(\mathfrak{m} \times_S R) \oplus x_2(\mathfrak{m} \times_S R) \oplus \ldots \oplus x_s(\mathfrak{m} \times_S R)$$

is an R-double-module with independent R-right-basis $(x_i v_k)$. On assuming $x_1 = 1$, it follows that the S-two-sided submodule $x_1 \mathfrak{m} = \mathfrak{m}$ is its direct summand as S-right-module.

5. Supplementary remarks. If R is a primary-decomposable ring, then a regular R-right-module is always a direct summand in a second regular R-right-module which contains it. If R is a simple ring then a (finite) R-right-module is always regular. These remarks are significant in connection with the theorems in §3, in particular with Theorems 4, 6. If, moreover, R is a quasifield, then any R-right-module certainly has an independent basis and any subring is of course also a quasifield. In dealing with relation moduli over a quasifield R we may thus always restrict ourselves to principal R-double-moduli which possess R-right-bases contained in the R-left-module generated by the element in question. Furthermore, the hypergroup formulation of our Galois theory can then be given under a certain assumption.

On the other hand, it may be of some use, in view of the usual Galois theory, to observe the case in which each $u_h R$, with a basis element u_h of $\mathfrak{M}$, is R-left-allowable too. Let an R-double-module $\mathfrak{M}$ possess such an independent R-right-basis $(u_1, u_2, \ldots, u_m)$ and let u_0 be the sum $u_0 = u_1 + u_2 + \ldots + u_m$.

The relation module of u_0 in $\mathfrak{M}$ is $\sum \mu_h R_l$, where we put $zu_0 = \sum u_h \mu_h(z)$. Since $Ru_h \subseteq u_h R$, we have

$$zu_h = u_h \mu_h(z)$$

and each μ_h is simply the self-representation of degree 1, i.e. (ring-) endomorphism, of R defined by the representation module $u_h R = Ru_h R$ (with respect to the basis element u_h). If $\mathfrak{M}$ has an independent R-right-basis contained in Ru_0 then these m endomorphisms μ_h of R are right-independent over R_l.

In this context we note some sufficient conditions that certain given (ring-) endomorphisms, say $\nu_1, \nu_2, \ldots, \nu_n$, of R be right-independent over R_l. Let (R, ν), with a (ring-)endomorphism ν of R, denote an R-double-module which coincides with R itself as R-left-module and on which right-operation of $z \in R$ is defined by $x\ (\in R) \to x.z = x\nu(z)$. Thus (R, ν) may also be looked upon as a module Rw with R-left-independent element w such as $wz = \nu(z)w$. Now we have, firstly: *If each $\nu_i(R)$ possesses no non-zero left-annihilator in R and if*

(*) *the R-double-moduli (R, ν_i), (R, ν_j) with distinct i, j have non-zero (R-two-sided)) isomorphic submoduli, then $\nu_1, \nu_2, \ldots, \nu_n$ are R-right-independent.*

For, from our assumptions we deduce that $\nu_i x_l = 0$ implies $x = 0$, for each i, and the R_l-double-moduli $\nu_i R_l$ and $\nu_j R_l$ with $i \neq j$ have no (R_l-two-sided) isomorphic non-zero submoduli. The sum $\sum \nu_i R_l$ is then necessarily direct [8, §3, Remark 6].

Secondly, if ν_i are (ring-)automorphisms and $\{\nu_i\}$ forms a group which induces a Galois group of the residue-ring R/N of R modulo its radical N in the sense of [8] (that is, a similar assumption (**) obtained from (*) by replacing "submoduli" by "residue-submoduli" is satisfied), then again ν_i are R_l-right-independent [8, Lemma 4 and Remark 5 concerning it].

A similar construction can be used to show that a certain R-double-module is principal. Interchanging "left" and "right", in order to be in accord with our situation, we consider n elements $v_1, v_2, \ldots, v_n$ which are right-independent over R and satisfy $zv_i = v_i \nu_i(z)$, with (ring-)endomorphisms ν_i of R. Suppose that the (left-right-)symmetric counterpart of (**), mentioned above, is satisfied. Then if v_0 is an element in the (direct) sum $\mathfrak{N} = \sum \nu_i R$ of a form $v_0 = v_1 z_1 + v_2 z_2 + \ldots + v_n z_n$ with regular elements z_i of R, we have

$$\mathfrak{N} = Rv_0 R.$$

For, under our assumption, Rv_0R exhausts the whole $\mathfrak{N}$ mod $\sum \nu_i N$ firstly, where N denotes the radical of R, and then actually, since $\sum v_i N$ is (whence is contained in) the intersection of all maximal R-right-submoduli of $\mathfrak{N}$.

Of course all these assumptions are covered by the assumption that $G = \{\nu_i\}$ forms a Galois group of R, under which in [8] the complete correspondence of between-rings, over which R has independent right-basis, with subgroups of G (not only with certain subrings of $\sum \nu_i R_l$) was established.

Let S be a subring of R such that R has not only an independent S-right-basis

https://doi.org/10.4153/CJM-1951-025-5 Published online by Cambridge University Press

of s terms but also an independent S-left-basis of the same number s of terms. Suppose further that $\mathbf{B} = V(S_r)$ contains an independent R_l-right-basis $(\beta_1, \beta_2, \ldots, \beta_s)$ (i.e. a Galois system belonging to S) which forms also an independent R_l-left-basis of $\mathbf{B}$, and that $\beta_1 S_l \oplus \beta_2 S_l \oplus \ldots \oplus \beta_s S_l$ forms a ring $(\ni 1)$ and moreover it equals $S_l\beta_1 \oplus S_l\beta_2 \oplus \ldots \oplus S_l\beta_s$. Then there exists an element x in R such that $\beta_1(x), \beta_2(x), \ldots, \beta_s(x)$ form an independent S-left-basis of R.

To show this, we observe that R is B-regular with rank $1/s$, or, what is the same, the direct sum R^s of s copies of R is $\mathbf{B}$-isomorphic to the $\mathbf{B}$-right-module $\mathbf{B}$. Hence naturally R^s is $(S_l\beta_1 \oplus S_l\beta_2 \oplus \ldots \oplus S_l\beta_s)$-isomorphic to $\mathbf{B}$. On the other hand

$$\mathbf{B} = R_l\beta_1 \oplus R_l\beta_2 \oplus \ldots \oplus R_l\beta_s = y_{1l}(S_l\beta_1 \oplus \ldots \oplus S_l\beta_s) \oplus \ldots \oplus y_{sl}(S_l\beta_1 \oplus \ldots \oplus S_l\beta_s),$$

where $(y_1, y_2, \ldots, y_s)$ is an independent S-left-basis of R. Hence $\mathbf{B}$ is a regular $(S_l\beta_1 \oplus \ldots \oplus S_l\beta_s)$-right-module of rank s. It follows that R is $(S_l\beta_1 \oplus \ldots \oplus S_l\beta_s)$-(right-)isomorphic to $S_{l1}\beta_1 \oplus \ldots \oplus S_l\beta_s = \beta_1 S_l \oplus \ldots \oplus \beta_s S_l$. Let x be the element of R which is mapped on the unit element of $\beta_1 S_l \oplus \ldots \oplus \beta_s S_l$ in such an isomorphism. Then $(x^{\beta_1}, x^{\beta_2}, \ldots, x_1^{\beta_s})$ forms an independent S_l-right-basis, that is, S-left-basis of R. This statement, though complicated, may be regarded as a generalization of the theorem of normal basis.

If here β_h are (ring-)automorphisms of R, then $\beta_h R_l = R_l\beta_h$ and moreover each β_h is elementwise commutative with S_l. Hence the left-symmetric half of the assumption concerning β_h follows automatically.

References

[1] G. Azumaya, *Galois theory of uni-serial rings*, J. Math. Soc. Japan, vol. 1 (1949).

[2] N. Jacobson, *The fundamental theorem of Galois theory for quasifields*, Ann. Math., vol. 41 (1940).

[3] ———, *An extension of Galois theory to non-normal and non-separable fields*, Amer. J. Math., vol. 66 (1944).

[4] ———, *Relations between the composites of a field and those of a subfield*, Amer. J. Math., vol. 66 (1944).

[5] ———, *Galois theory of purely inseparable fields of exponent one*, Amer. J. Math., vol. 66 (1944).

[6] ———, *Note on division rings*, Amer. J. Math., vol. 69 (1947).

[7] T. Nakayama, *Semilinear normal basis for quasifields*, Amer. J. Math., vol. 71 (1949).

[8] ———, *Galois theory for general rings with minimum condition*, J. Math. Soc. Japan, vol. 1 (1949).

[9] ———, *Commuter systems in a ring with radical*, Duke Math. J., vol. 16 (1949).

[10] ———, *Generalized Galois theory for rings with minimum condition*, in Amer. J. Math.

[11] T. Nakayama and G. Azumaya, *On irreducible rings*, Ann. Math., vol. 48 (1947).

Nagoya University