Journal of the Mathematical Society of Japan Vol. 1, No. 3, Dec. 1949.

Galois theory for general rings with minimum condition.

TADASI NAKAYAMA

(Received Feb. 11, 1948)

In a very suggestive paper N. Jacobson founded a Galois theory for division rings.[1] The theory was then skilfully extended by G. Azumaya to simple, and to uni-serial rings.[2] The present work is to establish it for general rings with minimum condition.[3] Most of our arguments are modifications or generalizations of theirs, while the others are those which have been employed in a previous note on semilinear repesentations and normal bases in noncommutative domains,[4] and we shall also resume the theorem of semilinear normal basis in a generalized and improved form.

The writer is grateful to Mr. G. Azumrya for his friendly cooperation during the preparation of the present paper.

§ 1. Crossed product.

Let R be a ring with unit element 1 and satisfying the minimum condition (whence the maximum condition) for ideals. Let σ be an automorphism of R. For a two-sided module $\mathfrak{m}$ of R we can introduce a new two-sided module $(\mathfrak{m}, \sigma)$ of R which coincides with $\mathfrak{m}$ as right-module and for which left operation by R is defined: $a * u = a^{\sigma} u$ $(a \in R, u \in \mathfrak{m})$.

We call a finite group of automorphisms $\mathfrak{G} = \{1, \sigma, \ldots\ldots, \tau\}$ a *Galois group* of R when the following condition is satisfied:

(*) *(R, σ), (R, τ) with distinct σ, τ in $\mathfrak{G}$ have no isomorphic non-vanishing sub-residue-moduli.*

If $\mathfrak{b}$ is a $\mathfrak{G}$-invariant ideal in R, our Galois group $\mathfrak{G}$ of R can be, in natural manner, looked upon as that of the residue-ring $R/\mathfrak{b}$.

A crossed product (=semilinear group ring with factor set) of R with

---

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

2) G. Azumaya, New foundation for the theory of simple rings, forthcoming in Proc. Imp. Acad. Japan: G. Azumaya, Galois theory for uni-serial rings, Journ. Math. Soc. Japan 1 (1949).

3) Another extreme case is that of (closed) irreducible rings. See T. Nakayama, Note on irreducible rings, forthcoming in Proc. Imp. Acad. Japan; T. Nakayama-G. Azumaya, On irreducible rings, Ann. Math. 48 (1947).

4) T. Nakayama, Semilinear normal basis for quasifields, Amer. Journ. Math. 71 (1949).

a finite group $\mathfrak{G}$ of automorphisms is a ring $(R,\mathfrak{G})$ which is decomposed

(1) $$(R, \mathfrak{G}) = u_1 R \oplus u_\sigma R \oplus \cdots\cdots \oplus u_\tau R$$

with regular elements u_σ such that

(2) i) $u_1 = 1$, ii) $x u_\sigma = u_\sigma x^\sigma$ $(x \in R)$,

iii) $u_\sigma u_\tau = u_{\sigma\tau}\, a_{\sigma,\tau}$ $(a_{\sigma,\tau} \in R)$.

Lemma 1. *If* $\mathfrak{b}_\sigma$ *are right-(resp. left-)ideals in* R, *the (direct) sum*

(3) $$\sum u_\sigma \mathfrak{b}_\sigma$$

forms an R*-right-(resp. left-)submodule of* $(R, \mathfrak{G})$. *The module is a right-(resp. left-) ideal of* $(R, \mathfrak{G})$ *if and only if* $\mathfrak{b}_\sigma = \mathfrak{b}_1^\sigma$ *(resp.* $\mathfrak{b}_\sigma = \mathfrak{b}_1$*) for every* $\sigma \in \mathfrak{G}$.

Proof is immediate.

Lemma 2. *Let our* $\mathfrak{G}$ *be a Galois group.*[5] *Then any ring containing* R *and regular elements* $u_1, u_\sigma, \cdots\cdots, u_\tau$ *such that* i), ii) *in* (2) *hold is a crossed product. Every* R*-two-sided submodule of the crossed product* $(R, \mathfrak{G})$ *has a form* (3) *with two-sided ideals* $\mathfrak{b}_\sigma$ *in* R. *Every two-sided ideal in* $(R, \mathfrak{G})$ *has a form*

(4) $\mathfrak{B} = \sum u_\sigma \mathfrak{b}$ *with* $\mathfrak{G}$*-invariant two-sided ideal* $\mathfrak{b}$ *of* R;

we denote it by $(\mathfrak{b}, \mathfrak{G})$. *And*

$$\mathfrak{b} \longrightarrow \mathfrak{B} = (R, \mathfrak{G})\mathfrak{b} = (\mathfrak{b}, \mathfrak{G}), \qquad \mathfrak{b} = \mathfrak{B} \cap R \longleftarrow \mathfrak{B}$$

gives a 1-1 *correspondence between two-stded ideals* $\mathfrak{B}$ *in* $(R, \mathfrak{G})$ *and* $\mathfrak{G}$*-invariant two-sided ideals* $\mathfrak{b}$ *in* R. *In particular,*[6] *if* N *denotes the radical of* R, *the radical of* $(R, \mathfrak{G})$ *is*

$$(N, \mathfrak{G}) = \sum u_\sigma N.$$

Further, if R *is two-sided directly indecomposable, then any regular element* u *in* $(R, \mathfrak{G})$ *such that* $uR = Ru$ *has a form* $u = u_\sigma a$ *with certain* $\sigma \in \mathfrak{G}$, $a \in R$.

Proof. The R-two-sided module $u_\sigma R = R u_\sigma$ is isomorphic to (R, σ). As $\mathfrak{G}$ is assumed to be a Galois group, $u_\sigma R$ with different σ have no isomorphic sub-residue-moduli $\neq 0$. Then every R-two-sided submodule of a direct sum (1) has a form (3) with two-sided ideals $\mathfrak{b}_\sigma$ in R.[7] It follows

---

5) Cf. Remark 6 in § 3.

6) We may make a similar statement for instance for the largest fully reducible two-sided ideals. That $(N, \mathfrak{G})$ is the radical of $(R, \mathfrak{G})$ also follows from a weaker assumption that $\mathfrak{G}$ induces a Galois group in R/N; observe that $(R/N, \mathfrak{G})$ is then semisimple.

7) Cf. e.g. K. Shoda, Über direkt zerlegbare Gruppen, Journ. Fac. Sci. Tokyo Imp. Univ. Sec. I. Vol. 2 (1930), Satz 3.

from this readily that our ring in question is, considered as R-two-sided module, not only homomorphic but isomorphic to the direct sum. The same gives also the second assertion in the lemma, and the third and fourth too when combined with Lemma 1. To prove the last, assume that R is two-sided directly indecomposable and $uR=Ru$ with a regular element u in $(R, \mathfrak{G})$. The two-sided submodule uR is directly indecomposable, whence it assumes a form $uR=u_\sigma \mathfrak{b}_\sigma$ with a $\sigma \in \mathfrak{G}$ when expressed as in (2). Comparing the R-lengths we obtain $\mathfrak{b}_\sigma=R$ and $uR=u_\sigma R$.

Now we consider a unit crossed product (=semilinear group ring), that is, a crossed product with unit factor set $\{a_{\sigma,\tau}\}=\{1\}$;

$$(5) \qquad (R, \mathfrak{G})=u_1R\oplus u_\sigma R\oplus\cdots\cdots\oplus u_\tau R,$$

$$u_1=1, \qquad xu_\sigma=u_\sigma x^\sigma, \qquad u_\sigma u_\tau=u_{\sigma\tau}\ .$$

R itself, or any $\mathfrak{G}$-invariant right-ideal $\mathfrak{b}$ in R in general, can be considered as a right-module of $(R, \mathfrak{G})$ by $x(u_\sigma a)=x^\sigma a$ ($x \in R$ or $\in \mathfrak{b}$). We denote the $(R, \mathfrak{G})$-right-module by $\tilde{R}$, or by $\tilde{\mathfrak{b}}$, and prove the fundamental

Lemma 3. *Assume that $\mathfrak{G}$ is a Galois group of R, or that $\mathfrak{G}$ induces a such in R/N. The direct sum of $g=(\mathfrak{G}:1)$ copies of the $(R, \mathfrak{G})$-right-module $\tilde{R}$ is isomorphic to the $(R, \mathfrak{G})$-right-module $(R, \mathfrak{G})$ itself.*

Proof.[8] Since $(N, \mathfrak{G})$ is the radical of $(R, \mathfrak{G})$ the module $\tilde{R}(N, \mathfrak{G})=N$ is the intersection of all the maximal ($(R, \mathfrak{G})$-right-) submoduli of $\tilde{R}$. We want to show first that the direct sum of g copies of the residue-module $\tilde{R}/\tilde{N}$ is isomorphic to the $(R, \mathfrak{G})$-right-module $(R, \mathfrak{G})/(N, \mathfrak{G})$. This assertion is however nothing but the special case of our lemma when $N=0$, because $\mathfrak{G}$ can be considered as a Galois group of the residue-ring R/N. So, let for a moment R be semisimple. Then $(R, \mathfrak{G})$ is so too. Let

$$R=\mathfrak{a}_1 \oplus \mathfrak{a}_2 \oplus\cdots\cdots\oplus\mathfrak{a}_k$$

with minimal $\mathfrak{G}$-invariant two-sided ideals $\mathfrak{a}_i$ of R. We have $\tilde{R}(\mathfrak{a}_i, \mathfrak{G})=\tilde{\mathfrak{a}}_i$, and each $\tilde{\mathfrak{a}}_i$ is a direct sum of submoduli $(R, \mathfrak{G})$-right-isomorphic to minimal right-ideals contained in the minimal two-sided ideal $(\mathfrak{a}_i, \mathfrak{G})$ of $(R, \mathfrak{G})$, for it is annihilated by $(\mathfrak{a}_j, \mathfrak{G})$ with $j \neq i$. Its R-length is equal to that of $(\mathfrak{a}_i, \mathfrak{G})$ divided by g. It follows that the direct sum of g copies of $\tilde{\mathfrak{a}}_i$ is $(R, \mathfrak{G})$-right-isomorphic to $(\mathfrak{a}_i, \mathfrak{G})$. Since this is the case for each i, the direct sum of g copies of $\tilde{R}$ $(=\tilde{\mathfrak{a}}_1\oplus\cdots\cdots\oplus\tilde{\mathfrak{a}}_k)$ is $(R, \mathfrak{G})$-right-isomorphic to $(R, \mathfrak{G})$.

8) For the following proof cf. Nakayama, l. c. 4), § 1. Cf. also Lemma 5 below (in § 3).

Now we return to the general case of non-semisimple R. The direct sum of g copies of $\tilde{R}/\tilde{N}$, that is, the residue-module of the direct sum of g copies of R modulo the intersection of all its maximal submoduli, is isomorphic to $(R, \mathfrak{G})$ modulo $(N, \mathfrak{G})$. Hence $(R, \mathfrak{G})$ can be homomorphically mapped upon the direct sum of g copies of $\tilde{R}$. The homomorphism must be an isomorphism, for the two moduli have equal R-lengths.

Our lemma, thus proved, can be expressed by saying that $\tilde{R}$ is a regular right-module with rank $1/g$ of the ring $(R, \mathfrak{G})$, if we introduce the following definition: A right-module $\mathfrak{m}$ of a ring R, with unit element and satisfying the minimum condition, is called *regular* when a direct sum of a certain number, say m, of its copies is isomorphic, as R-right-module, to the direct sum of a certain number, say n, of copies ot R itself. The rational number $k=n/m$ we call the *rank* of the regular module $\mathfrak{m}$; that it is uniquely determined by $\mathfrak{m}$ follows readily from the Krull-Remak-Schmidt theorem. We have

α) $\mathfrak{m}$ is also a regular module of rank k^{-1} with respect to its (R-) endomorphism ring R^*.

β) The R^*-endomorphism ring of $\mathfrak{m}$ coincides with R.

These are certainly true in the special case $\mathfrak{m}=R$, and the general case follows easily from that.

γ) If $\mathfrak{m}$, a regular R-module of rank k, is also regular and of rank l with respect to a subring T of R, then any other regular module of R is regular with respect to T and its T-rank is equal to lk^{-1} times its R-rank.

To show this it is perhaps convenient to treat two special cases where respectively $\mathfrak{m}$ or the second module coincides with R.

§ 2. Galois theory.

Let $\mathfrak{G}$ be, throughout in this section, a *Galois group* of the ring R, and let g be its order. Let $\mathfrak{A}$ be the absolute endomorphism ring of R considered as a module. The right multiplication by R forms a subring R of $\mathfrak{A}$. The left multiplication ring R', which is inverse-isomorphic to R, is the commuter $V(R)$ of R in $\mathfrak{A}$ and is the (operator-) endomorphism ring of the R-right-module R; $a'=a_l$: $x \longrightarrow ax$. Automorphisms σ of R can be regarded as those ot R'; $(a')^\sigma=(a^\sigma)'$, and our Galois group $\mathfrak{G}$ of R becomes that of R' as one readily sees. Further, the subring of $\mathfrak{A}$ generated by R (resp. R') and $\mathfrak{G}=\{1, \sigma, \ldots\ldots, \tau\}$ is in fact a unit crossed product

$(R, \mathfrak{G})$ (resp. $(R', \mathfrak{G})$) according to Lemma 2 ;[9]

$$(R, \mathfrak{G}) = 1R \oplus \sigma R \oplus \cdots\cdots \oplus \tau R, \qquad (R', \mathfrak{G}) = 1R' \oplus \sigma R' \oplus \cdots\cdots \oplus \tau R'.$$

The commuter ring $V(R', \mathfrak{G}) = V(R') \cap V(\mathfrak{G}) = R \cap V(\mathfrak{G})$ of $(R', \mathfrak{G})$ in A is indeed the *invariant system* S of $\mathfrak{G}$ in R.

According to our fundamental lemma 3 $R(=\tilde{R})$ is a regular $(R, \mathfrak{G})$--module of rank $1/g$, and similarly R is a regular module of rank $1/g$ with respect to $(R', \mathfrak{G})$.[10] By $a)$ of § 1 we see that R is a regular module of rank g with respect to S, or, what is the same,

Lemma 4. *R has an (independent right-) basis of g terms over S.*

(This can be seen also calculatively as follows : We have, by Lemma 3,

$$(R, \mathfrak{G}) = \mathfrak{m}_1 \oplus \mathfrak{m}_2 \oplus \cdots\cdots \oplus \mathfrak{m}_g,$$

where each $\mathfrak{m}_i$ is isomorphic to the $(R, \mathfrak{G})$-right-module $R=\tilde{R}$. Let $v_i \in \mathfrak{m}_i$ correspond to $1 \in \tilde{R}$. Since it must be invariant under $\mathfrak{G}$, it has a form

$$v_i = a_i + \sigma a_i^{\sigma} + \cdots\cdots + \tau a_i^{\tau} \quad (a_i \in R).$$

These $v_1, v_2, \cdots\cdots, v_g$ are R-right-independent. We have

$$\sum v_i s_i = (\sum a_i s_i) + \sigma(\sum a_i s_i)^{\sigma} + \cdots\cdots + \tau(\sum a_i s_i)^{\tau}$$

for $s_1, s_2, \cdots\cdots, s_g \in S$, and the sum vanishes only when all the s_i vanish, which means that the g elements $a_1, \cdots\cdots, a_g$ in R are S-right-independent. Further, an element in $(R, \mathfrak{G})$ is $\mathfrak{G}$-invariant when and only when it has a form $a + \sigma a^{\sigma} + \cdots\cdots + \tau a^{\tau}$. The same is the case also when and only when each of its $\mathfrak{m}_i$-components is $\mathfrak{G}$-invariant, that is, it is a sum $\sum v_i s_i$ with $s_i \in S$. It follows then that any $a \in R$ can be expressed as $\sum a_i s_i$ $(s_i \in S)$. Thus $(a_1, a_2, \cdots\cdots, a_g)$ forms an (independent) right-basis of R over S.)

This S-right-bais of R forms of course a right-basis of $(R, \mathfrak{G})$ over the subring $(S, \mathfrak{G})$. On the other hand the $(S, \mathfrak{G})$-right-module $(R, \mathfrak{G})$ is, by Lemma 3, directly decomposed into g submoduli isomorphic to the $(S, \mathfrak{G})$-right-module R. By the Krull-Remak-Schmidt theorem the $(R, \mathfrak{G})$-right-module R is isomorphic to $(S, \mathfrak{G})$ itself, which proves

Theorem 1.[11] *R has a normal right- (or left-) basis over the invariant system S.*

Next we prove

Theorem 2. *Assume R to be two-sidtd directly indecomposable. Then*

---

9) Cf. Remarks 5, 6 in § 3. $(R, \mathfrak{G})$ is inverse-isomorphic to $(R, \mathfrak{G})$ $a' u_{\sigma}^{-1} \longleftrightarrow u_{\sigma} a$.

10) The $(R', \mathfrak{G})$-module R is, by $x \longleftrightarrow x'$, isomorphic to the $(R', \mathfrak{G})$-(right-) module R' defined similarly as R.

11) For Lemma 4 and Theorem 1 cf. Remark 5 below in § 3.

$\mathfrak{G}$ *exhausts automorphisms of* R *leaving* S *elementwise invariant.*

Let namely φ be such an automorphism of R. If we consider it as an element of $\mathfrak{A}$, then $\varphi \in V(S)$. Here $V(S)=(R, \mathfrak{G})$ by $\beta)$ of § 1, since R is (right-) regular with respect to S. As $\varphi R'=R'\varphi$ and φ is regular in $(R', \mathfrak{G})$, we have, by Lemma 2 applied to R' instead of R, $\varphi=\sigma a'$ with $a' \in R'$, $\sigma \in \mathfrak{G}$. But we have necessarily $1=1^{\varphi}=1^{\sigma}a'=a$, and $\varphi=\sigma$, which proves the theorem.

Now we consider a between-ring T of R, S; $R \supseteq T \supseteq S$. Its commuter $V(T)$ in $\mathfrak{A}$ is between $R'=V(R)$ and $(R, \mathfrak{G})=V(S)$, and has so, as an R'-two-sided submodule of $(R', \mathfrak{G})$, a form

$$V(T)=1\mathfrak{b}' \oplus \sigma\mathfrak{b}'_{\sigma} \oplus \cdots\cdots \oplus \tau\mathfrak{b}'_{\tau}$$

with $\mathfrak{G}$-invariant two-sided ideals $\mathfrak{b}_{\sigma}$ in R'.

Assume now that R is T-right-regular with a certain rank, say $h=w/v$. T is then, by $\gamma)$ of § 1, a regular S-(right-)module of rank $gh^{-1}=gv/w$. Again[12] by $\alpha)$, $\gamma)$ $(R', \mathfrak{G})=V(S)$ is a regular $V(T)$-module of rank gh^{-1}. So we consider the direct sum $(R', \mathfrak{G})^{w}$ of w copies of the $(R', \mathfrak{G})$-right-modeule $(R', \mathfrak{G})$;

$$(R', \mathfrak{G})^{w}=x^{(1)}(R', \mathfrak{G}) \oplus \cdots\cdots \oplus x^{(w)}(R', \mathfrak{G}).$$

Let further r be the number of components in a direct decomposition of R', or R, into directly indecomposable right ideals. Naturally $(R', \mathfrak{G})^{w}$ is decomposed into wgr directly indecomposable R'-right-submoduli. We consider our module $(R', \mathfrak{G})^{w}$ modulo the submodule $(R', \mathfrak{G})^{w}(N', \mathfrak{G})=x^{(1)}(N', \mathfrak{G}) \oplus \cdots\cdots \oplus x^{(w)}(N', \mathfrak{G})$. The residue-module, the direct sum of w copies of $(R', \mathfrak{G})/(N', \mathfrak{G})$, is decomposed, directly, into wgr irreducible R'-right-moduli. On the other hand $(R', \mathfrak{G})^{w}$ is $V(T)$-, whence R-, isomorphic to $V(T)^{gv}$. Hence it has a $V(T)$-right-basis $y^{(1)}, y^{(2)}, \cdots\cdots, y^{(gv)}$; $(R', \mathfrak{G})^{w}=y^{(1)}V(T) \oplus \cdots\cdots \oplus y^{(gv)}V(T)$. If each $\mathfrak{b}_{\sigma}'$ in $V(T)$ is decomposed into b_{σ} directly indecomposable right-ideals of R', we have so $gv\sum b_{\sigma}=wgr$.

Now we assert that no such direct component in $\mathfrak{b}'_{\sigma}$ is contained in the racical N'. For if such a component $\mathfrak{c}_{\sigma}'$ were contained in N', then $\sigma\mathfrak{c}_{\sigma}' \subseteq (N', \mathfrak{G})$, $y^{(i)}\sigma\mathfrak{c}'_{\sigma} \subseteq (R', \mathfrak{G})^{w}(N', \mathfrak{G})$ and $y^{(i)}\sigma\mathfrak{c}'_{\sigma}$ would contribute nothing to $(R', \mathfrak{G})_{w}$ modulo $(R', \mathfrak{G})^{w}(N', \mathfrak{G})$ and the residue-module would be a direct sum of less irreducible R'-submoduli than $gv\sum b_{\sigma}=wgr$, since each

12) From $\alpha)$, $\gamma)$ follows, generally, that if $\mathfrak{m}$ is an R-regular module and R is regular with rank h over its subring T, then the T-endomorphism-ring T^{*} of $\mathfrak{m}$ is regular and of rank h with respect to the R-endomorphism-ring R^{*}.

direct component of $\mathfrak{b}'_\sigma$, isomorphic to a direct right-ideal component of R', contributes at most one irreducible component to the fully reducible residue-module. Thus every direct component in $\mathfrak{b}_\sigma'$ is not contained in N', whence contains a non-zero idempotent element. Each $\mathfrak{b}_\sigma'$ is thus a direct summand in R'.

Further, h is an integer. To see this, let e' be a primitive idempotent element in R', and there be $r(e')$ components isomorphic to $e'R'$ in a direct decomposition of R' into directly indecomposable right-ideals. As $\mathfrak{b}_\sigma'$ is two-sided, it contains every right-ideal of R' homomorphic to $e'R'$ if it contains $e'R'$. Hence the number $b_\sigma(e')$ of direct components isomorphic to $e'R'$ in $\mathfrak{b}_\sigma'$ is either $r(e')$ or 0. We have on the other hand, considering only those components isomorphic to $e'R'$ in the above decompositions, $gv\sum b_\sigma(e')=wgr(e')$, or, $v\sum b_\sigma(e')=wr(e')$. Since every $b_\sigma(e')$ is divisible by $r(e')$ the rank $h=w/v$ is an integer, and we may set $w=h$, $v=1$.

We now assume R to be two-sided directly indecomposable, and want to show that $\mathfrak{b}_\sigma'=R$ whenever $\neq 0$. For this purpose, let $\mathfrak{r}_1',\ldots\ldots,\mathfrak{r}_t'$ be the sums of the totalities of mutually isomorphic directly indecomposable right-ideal components in R'. Each $\mathfrak{b}_\sigma'$ is, as noted above, a sum of certain number of them. We consider those ideals in R' which are obtained from $\mathfrak{b}_1'$, $\mathfrak{b}_\sigma'$,$\ldots\ldots$, $\mathfrak{b}_\tau'$ by construction of intersection and sum, and consider a maximal such ideal $\mathfrak{c}'$ different from R'. By a suitable numeration we can assume that $\mathfrak{c}'=\mathfrak{r}_1'\oplus\mathfrak{r}_2'\oplus\ldots\ldots\oplus\mathfrak{r}_s'$. Then we consider the intersection $\mathfrak{d}'$ of all those $\mathfrak{b}_\sigma'$ which contain $\mathfrak{r}'_{s+1}$. $\mathfrak{d}'$ contains no $\mathfrak{r}_1'$, $\mathfrak{r}_2'$,$\ldots\ldots\mathfrak{s}_s'$, whence does not meet with $\mathfrak{c}'$. For, if it contained $\mathfrak{r}_1'$, for instance, then $\mathfrak{r}_1'$ would be contained in a greater number of $\mathfrak{r}_\sigma'$ than $\mathfrak{r}'_{s+1}$ does, contrary to that every $\mathfrak{r}_i'$ should appear exactly in h of $\mathfrak{b}_\sigma'$, since $V(T)$ is a regular R'-module of rank h. So the sum of $\mathfrak{c}'$ and $\mathfrak{d}'$ is direct, and coincides with R' because of the maximality of $\mathfrak{c}'$. As R' is directly indecomposable, we have necessarily $\mathfrak{c}'=0$, which shows that every $\mathfrak{b}_\sigma'$ is either R' or 0. Since $V(T)$ is a ring, those σ for which $\mathfrak{b}_\sigma'=R'$ form a certain subgroup $\mathfrak{H}$ of $\mathfrak{G}$. Thus

$$V(T)=1R'\oplus\varphi R'\oplus\ldots\ldots\oplus\psi R'=(R',\mathfrak{H}).$$

Furthermore $T=V(V(T))=V(R',\mathfrak{H})=R\cap V(\mathfrak{H})$ and T is the invariant system of $\mathfrak{H}$ in R.

Combining the result with Theorem 2, applied to subgroups of $\mathfrak{G}$, we have

Theorem 3. *Let R be two-sided directly indecomposable. Subgroups $\mathfrak{H}$*

of $\mathfrak{G}$ *and between-rings* T *of* R, S *such that* R *is* T*-right-(or left-) regular correspond to each other* 1–1 *in the usual manner of Galois theory.*

Remark 1. We can replace the condition for between-rings with a stronger one that R has a right- (or left-) basis over T. In fact both the T-(right- or left-) rank of R and the S-rank of T are integer. The T-right- and T-left-ranks of R coincide, and similarly for S-ranks of T. The T-right- and T-left-regularity of R imply each other.

Remark 2. $\mathfrak{G}$ can be looked upon as a Galois group of the residue-ring $R/\mathfrak{b}$ of R modulo a $\mathfrak{G}$-invariant two-sided ideal $\mathfrak{b}$. The invariant system of a subgroup in $R/\mathfrak{b}$ is obtained by taking the invariant system in R modulo $\mathfrak{b}$, as one easily sees from Lemma 4 for instance. Hence the Galois correspondence of R is in a sense reflected in the residue-ring $R/\mathfrak{b}$, for example in the semisimple residue-ring R/N. But we have to notice that $R/\mathfrak{b}$ is in general directly decomposable, and in that case not every subring of $R/\mathfrak{b}$ for which $R/\mathfrak{b}$ is regular corresponds to a subgroup of $\mathfrak{G}$.

§ 3. Normal basis.

Let $\mathfrak{G}$ be again a Galois group of the ring R, or more generally, let $\mathfrak{G}$ induce a such in R/N. Let U be a subring of R invariant, as a whole, under $\mathfrak{G}$; $U^{\mathfrak{G}}=U$, and assume that R is right-regular[13] with respect to U, including the infinite rank case of generalized sense that R is a direct sum of two U-right-moduli, the first of which is regular with finite rank, while the second has an independent U-right-basis with infiditely many terms; we shall refer to R simply as a regular U-module with rank $f=\infty$, since it has an infinite (independent) U-right-basis.

We consider the unit crossed product $(R, \mathfrak{G})$ and its subring

$$(U, \mathfrak{G})=1U\oplus\sigma U\oplus\cdots\cdots\oplus\tau U,$$

which itself is a unit crossed product of U with $\mathfrak{G}$. Since R^g, the direct sum of g copies of R, and $(R, \mathfrak{G})$ are isomorphic with respect to the right operator-domain $(R, \mathfrak{G})$, they are so even more with respect to the sub-domain $(U, \mathfrak{G})$. Here $(R, \mathfrak{G})$ is $(U, \mathfrak{G})$-right-regular and has the same rank f as R has with respect to U. *Suppose first* i) $f\geq g$. Then, by Krull-Remak-Schmidt theorem,[14] R has as $(U, \mathfrak{G})$-right-module a submodule

13) We may weaken the assumption somewhat by decomposing U into directly indecomposable right-ideals and allowing different ranks, so to speak, with respect to non-isomorphic components.

14) Cf. G. Azumaya. On generalized semi-primary rings and Krull-Remark-Schmidt theorem, in Jap. Journ. Math. 19 (1948).

isomorphic to $(U, \mathfrak{G})$, whence *there exists an element* ξ *in* R *such that* ξ, $\xi^{\sigma_0}, \ldots\ldots \xi^{\sigma_\tau}$ *are right-iudependent over* U. *Suppose next* ii) $f \leq g$. Then R is conversely a direct summand of the $(U, \mathfrak{G})$-right-module $(U, \mathfrak{G})$, and *there exists an element* ξ *in* R *so that* ξ, $\xi^{\sigma_0}, \ldots\ldots, \xi^{\sigma_\tau}$ U-*right-generate* R. *Suppose generally* iii)[15] $f = gq + r$ *where* q *is integral and* r *is a rational number* ≥ 0 *and* $< g$. Then R *is a direct sum of* $q+1$ $(U, \mathfrak{G})$-(*right-*) *submoduli,* q *of which are* $(U, \mathfrak{G})$-*isomorphic to* $(U, \mathfrak{G})$ (*that is, have* (*independent*) *normal* (*right-*) *bases, so to speak, over* U) *and one of which is* $(U, \mathfrak{G})$-*homomorphic to* $(U, \mathfrak{G})$ (*i.e.* U-(*right-*)*generated by* $\mathfrak{G}$-*conjugates of a single element*).

Our above assumption that $\mathfrak{G}$ is a Galois group of R (or of R/N) and the assumptions I, II in our previous note[16] cross each other, and perhaps the present one is more natural. But the argument in the previous note possesses a further range, and we may comprise the cases there and here in one by making the following assumptions:

Let $\mathfrak{G}$ be a finite group of automorphisms of R (which is not necessarily a Galois group), and $\mathfrak{H}$ be an invariant subgroup of $\mathfrak{G}$. Let U be a subring of R such that $U^{\mathfrak{G}} = U$ and assume that R is U-right-regular (in the generalized sense as above). We make

Assumption I*. The group $\mathfrak{G}/\mathfrak{H}$ induces a Galois class-group in the residue-ring of the crossed product $(U, \mathfrak{H})$ modulo its radical; where under a *Galois class-group* we mean a finite group of automorphism-classes[17] satisfying (*) of § 1.

*Assumption II**. $\mathfrak{H}$ induces a Galois group of R/N.

Under I*, II* *the above statements remain valid.* For, by virtue of the second assumption R^h $(h = (\mathfrak{H} : 1))$ and $(R, \mathfrak{H})$ are, again by Lemma 3, $(R, \mathfrak{H})$-, whene $(U, \mathfrak{H})$-(right-) isomorphic. Taking the sums of their g/h copies, we have that R^g and $(R, \mathfrak{G})$, which are $(R, \mathfrak{G})$-moduli, are $(U, \mathfrak{H})$-isomorphic. By the first assumption they are then $(U, \mathfrak{G})$-isomorphic too, in virtue of the following generalized formulation of Lemma 1 of the previous note:

---

15) In case of infinite rank $f = \infty$ we mean by this that $q = \infty$ and r is a rational number $< g$; the restriction being rather inessential.

16) Nakayama, l. c. 4).

17) Classes are with respect to the subgroup of inner automorphisms. Automorphisms σ in a same class (and only those in case $\mathfrak{m} = R$) give isomorphic two-sided moduli $(\mathfrak{m}, \sigma)$. So we can speak of $(\mathfrak{m}, \sigma)$ with an automorphism-class σ.

Lemma 5. *Let P be a ring (with unit element and minimum condition) and Q be its radical. Let a finite group $\mathfrak{R}$ of automorphism-classes of P induces a Galois class-group in the residue-ring P/Q. Consider a crossed product $(P, \mathfrak{R})$ (with factor set) defind similarly as in § 1 by taking representatives of the classes,*[18] *and two $(P, \mathfrak{R})$-right-moduli $\mathfrak{r}$, $\mathfrak{s}$, which are direct sums of P-submoduli P-isomorphic to directly indecomposable right-ideal components of P. If $\mathfrak{r}/\mathfrak{r}Q$ and $\mathfrak{s}/\mathfrak{s}Q$ are P-isomorphic, then $\mathfrak{r}$ and $\mathfrak{s}$ are $(P, \mathfrak{R})$-isomorphic*[19].

Proof runs similarly as in our Lemma 3, or in Lemma 1 in the previous note, if we observe that $(Q, \mathfrak{R})$ forms the radical of $(P, \mathfrak{R})$.[20] For the case of infinite rank, where the argument of composition length fails, consult the previous note, as well as a reproduction below.

Having thus shown the $(U, \mathfrak{G})$-isomorphism of R^g and $(R, \mathfrak{G})$, we can now proceed as before.

We may also make division of $\mathfrak{G}$ finer. Assume namely:

Assumption III.* Let there be a series $\mathfrak{G}=\mathfrak{H}_0, \mathfrak{H}_1, \ldots\ldots, \mathfrak{H}_n$ of subgroups of $\mathfrak{G}$ such that $\mathfrak{H}_{i+1}$ is invariant in $\mathfrak{H}_i$ $(i=0,1,\ldots\ldots,n-1)$, and that of subrings $U_0, U_1, \ldots\ldots, U_n=R$ of R such that $U_i^{\mathfrak{G}}=U_i, U_i \subseteq U_{i+1}$ and R is U_i-right-regular $(i=0,1,\ldots\ldots, n-1)$. Assume further that $\mathfrak{H}_i/\mathfrak{H}_{i+1}$ induces a Galois class-group in the residue-ring of the (unit) crossed product $(U_i, \mathfrak{H}_{i+1})$ modulo its radical $(i=0,1,\ldots\ldots, n-1)$ and $\mathfrak{H}_n$ induces a Galois group of R/N.

Under III* *the above assertions, i.e. the statements of theorem of semilinear normal basis, as we want to call, hold for $U=U_0$.* In fact, R^{h_n} and $(R, \mathfrak{H}_n)$ are $(R, \mathfrak{H}_n)$-, whence $(U_{n-1}, \mathfrak{H})$-(right-) isomorphic, and so R^{h_n-1} and $(R, \mathfrak{H}_{n-1})$ are $(U_{n-1}, \mathfrak{H}_n)$-isomorphic, where h_i denotes the order of $\mathfrak{H}_i$. By Lemma 5 they are $(U_{n-1}, \mathfrak{H}_{n-1})$-isomorphic. They are $(U_{n-2}, \mathfrak{H}_{n-1})$-isomorphic even more. Hence R^{h_n-2} and $(R, \mathfrak{H}_{n-2})$ are so. They are then, by Lemma 5, $(U_{n-2}, \mathfrak{H}_{n-2})$-isomorphic. Repeating this process we find finally that $R^{h_0}=R^g$ is $(U_0, \mathfrak{H}_0)=(U, \mathfrak{G})$-isomorphic to $(R, \mathfrak{H}_0)=(R, \mathfrak{G})$. We may then argue as before.

---

18) Cf. Nakayama-Azumaya, l. c. 3).

19) For the case when $\mathfrak{s}$ is homomorphic to $\mathfrak{r}$, as well as for some remarks on weakening the assumptions, cf. the full proof below at the end of the paper. Cf. also Lemma 2 of the previous note.

20) Our lemmas 1, 2 in §1 remain valid for crossed product with automorphism class-group and Galois class-group.

Remark 3. Our assumption (in I* or III*) that $\mathfrak{G}/\mathfrak{H}$ resp. $\mathfrak{H}_i/\mathfrak{H}_{i+1}$ induces a Galois class-group in the residue-ring of $(U, \mathfrak{H})$ resp. $(U_i, \mathfrak{H}_{i+1})$ modulo the radical may be rather awkward. However, in the case of a division ring U it can be replaced by that U be elementwise invariant under $\mathfrak{H}$ and $\mathfrak{G}/\mathfrak{H}$ be a Galois group of U, and respectively for U_i and $\mathfrak{H}_i/\mathfrak{H}_{i+1}$; cf. the previous note.

Remark 4. Theorem 1 is included not in our theorem of semilinear normal basis itself, but in its combination with Lemma 4.

In connection with Theorem 1 we want also to make

Remark 5. In order to prove Lemma 4 and Theorem 1 we used our assumption that $\mathfrak{G}$ is a Galois group of R only for Lemma 3 and for that the subring $R\mathfrak{G}$ of A generated by R and $\mathfrak{G}$ is not only homomorphic but isomorphic to the (unit) crossed product $(R, \mathfrak{G})$. Lemma 3 was stated under the weaker assumption that $\mathfrak{G}$ induces a Galois group in R/N. But this assumption is sufficient for the isomorphism of $R\mathfrak{G}$ and $(R, \mathfrak{G})$ too.[21] Namely $R\mathfrak{G}/N\mathfrak{G}$ is then $(R,\mathfrak{G})$-, or $R\mathfrak{G}$-, isomorphic to $(\tilde{R}/\tilde{N})^g=\tilde{R}^g/\tilde{N}^g$. Similarly as in the proof of Lemma 3 (or Lemma 5) $R\mathfrak{G}$ is $R\mathfrak{G}$-, homomorphically mapped upon $\tilde{R}^g$. Since the R-length of the former module is at most equal to the latter, the mapping must be an isomorphism. So $R\mathfrak{G}$ has the same length as $\tilde{R}^g$, and $R\mathfrak{G}\cong(R, \mathfrak{G})$.

Hence Theorem 1, the theorem of normal basis, remains valid under the assumption that $\mathfrak{G}$ induces a Galois group in R/N.

We may argue also as follows: Under the assumption Lemma 3 holds. If $R\mathfrak{G}\cong(R, \mathfrak{G})/\mathfrak{a}$ with a two-sided ideal $\mathfrak{a}$ in $(R, \mathfrak{G})$, then $\tilde{R}\mathfrak{a}=0$, $\tilde{R}^g\mathfrak{a}=0$, whence, by Lemma 3, $(R, \mathfrak{G})\mathfrak{a}=0$, which implies $\mathfrak{a}=0$. So $R\mathfrak{G}\cong(R,\mathfrak{G})$

Thus indeed Theorem 1 is true if $\mathfrak{G}$ is a finite group of automorphisms of R and if the $(R, \mathfrak{G})$-right-moduli $(\tilde{R}/\tilde{N})^g$ and $(R/N,\mathfrak{G})$ are isomorphic. For, in the latter half of the proof to Lemma 3 we used only the isomorphism and that $(N, \mathfrak{G})$ is contained in the radical of $(R, \mathfrak{G})$; cf. the proof below to Lemma 5 too.

For Theorems 2, 3, however, we used rather in full the assumption that $\mathfrak{G}$ is a Galois group of R.

Remark 6. That $\mathfrak{G}$ induces a Galois group in R/N is of course equivalent to an assumption $(**)$ obtained from $(*)$ in § 1 by replacing "sub-residue-moduli" by "residue-moduli". The above isomorphism of $R\mathfrak{G}$ and

21) This was pointed out to the writer by G. Azumaya.

$(R, \mathfrak{G})$ follows also from the assumption (***) obtained by replacing "sub-residue-mouduli" in (*) by "submoduli". Indeed, under this (***) the first assertion of Lemma 2 remains true. For, every non-vanishing R-two-sided submodule in a direct sum (1) contains, under (***), a submodule $\neq 0$ of a form $u_\sigma \mathfrak{b}_\sigma$. Suppose namely the contrary and let $\mathfrak{m}$ be a minimal module for which this is not case. There are at least two elements in $\mathfrak{G}$, say $\sigma = \sigma_1, \sigma_2$, such that not all the σ-coordinates $u_\sigma a_\sigma$ of elements in $\mathfrak{m}$ vanish. Observing the decomposition $u_\sigma R \oplus \sum_{\tau \neq \sigma} u_\tau R$ $(\sigma = \sigma_1, \sigma_2)$ we find that those σ-coordinates of $\mathfrak{m}$ form an R-two-sided module isomorphic to $\mathfrak{m}$.[22] Hence $u_{\sigma_1} R$ and $u_{\sigma_2} R$ have isomorphic submoduli $\neq 0$, contrary to (***).[23]

It is perhaps needless to note that in (*), (**) or (***) we may fix σ, say, unchanged; for instance we may set simply $\sigma = 1$.

Proof to Lemma 5. Since Lemma 5, as well as Lemma 3, was rather fundamental, it is perhaps without use to reproduce its proof in the previous note in a form adapted to the present generalized formulation and also to make some remarks on it. Consider namely a $(P, \mathfrak{R})$-right-module $\mathfrak{r}$ and suppose first that $\mathfrak{r}$ is fully reducible as P-module, which is equivalent to that $\mathfrak{r}$ is so as $(P, \mathfrak{R})$-module, since a $(P, \mathfrak{R})$-module is annihilated by the radical $(Q, \mathfrak{R})$ if and only if it is annihilated by Q. Let $P/Q = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_k$ with minimal $\mathfrak{R}$-invariant two-sided ideals $\mathfrak{a}_i$ of P/Q. Then $(P/Q, \mathfrak{R})$ $(\backsimeq (P, \mathfrak{R})/(Q, \mathfrak{R}))$ is decomposed into minimal two-sided ideals $(\mathfrak{a}_i, \mathfrak{R})$; $(P/Q, \mathfrak{R}) = (\mathfrak{a}_1, \mathfrak{R}) \oplus \cdots\cdots \oplus (\mathfrak{a}_k, \mathfrak{R})$. Let r_i be the number, finite or infinite, of irreducible components in $\mathfrak{r}(\mathfrak{a}_i, \mathfrak{R})$. Each such irreducible component, isomorphic to an irreducible right-ideal in $(\mathfrak{a}_i, \mathfrak{R})$, is a direct sum of P-moduli which are decomposed into a same number, say a_i, of isomorphic irreducible P-moduli. The numbers $r_i a_i$ of mutually isomorphic P-irreducible components in $\mathfrak{r}$ are determined completely by the structure of $\mathfrak{r}$ as P-module. By $r_i a_i$ are determined r_i, which determine the structure of $\mathfrak{r}$ as $(P, \mathfrak{R})$-module. So the P-structure of $\mathfrak{r}$ determines its $(P, \mathfrak{R})$-structure, and a second $(P, \mathfrak{R})$-module $\mathfrak{s}$ is $(P, \mathfrak{R})$isomorphic to $\mathfrak{r}$ if it is so with respect to P.

Consider next a general $(P, \mathfrak{R})$-right-module $\mathfrak{r}$. $\mathfrak{r}(Q, \mathfrak{R}) = \mathfrak{r}Q$ is the

22) Cf. K. Shoda, 1, c. 7).

23) It follows from this, combined with Lemma 1, that also the 1–1 correspondence, in Lemma 2, between two-sided ideals of $(R, \mathfrak{G})$ and $\mathfrak{G}$-invariant two-sided ideals of R holds under the weaker assumption that (***) is satisfied for every residue-ring of R modulo a $\mathfrak{G}$-invariant two-sided ideal.

intersection of all the maximal $(P, \mathfrak{R})$-submoduli, and at the same time that of all the maximal P-submoduli. Let e_i be a primitive idempotent element in $(P, \mathfrak{R})$ such that e_i (mod. $(Q, \mathfrak{R})$) is in $(\mathfrak{a}_i, \mathfrak{R})$. Let r_i have the same significance as above with respect to the fully reducible module $\mathfrak{r}/\mathfrak{r}Q$. We construct now for each i a direct sum $\mathfrak{v}_i$ of r_i $(P, \mathfrak{R})$-right-moduli $\mathfrak{v}_{i\nu}$ $(\nu=1,2,\ldots\ldots, r_i)$ $(P, \mathfrak{R})$-isomorphic to $e_i(P, \mathfrak{R})$ by $v_{i\nu} \longleftrightarrow e_i$, and further the direct sum $\mathfrak{v}$ of such $\mathfrak{v}_i$ $(i=1,2,\ldots\ldots, k)$. Then $\mathfrak{v}/\mathfrak{v}Q$ and $\mathfrak{r}/\mathfrak{r}Q$ are $(P, \mathfrak{R})$-isomorphic. Let $v_{i\nu}$ mod. $\mathfrak{v}Q$ correspond to $x_{i\nu}$ mod. $\mathfrak{r}Q$ by the isomorphism. $\mathfrak{v}_{i\nu}=v_{i\nu}(P, \mathfrak{R})$ can be mapped $(P, \mathfrak{R})$-homomorphically upon $x_{i\nu}e_i(P, \mathfrak{R})$ according to $v_{i\nu} \longrightarrow x_{i\nu}e_i$. The mappings together give a mapping of $\mathfrak{v}$ upon the sum of $v_{i\nu}e_\nu(P, \mathfrak{R})$ $(i=1,2,\ldots\ldots, k;$ $\nu=1,2,\ldots\ldots, r_i)$ in $\mathfrak{r}$. The last sum consumes the whole $\mathfrak{r}$, since it does so modulo $\mathfrak{r}Q$ and $\mathfrak{r}Q$ is the intersection of all the maximal ($(P, \mathfrak{R})$-or P-) submoduli. Let $\mathfrak{w}$ be the kernel of this homomorphic mapping of $\mathfrak{v}$ on $\mathfrak{r}$; $\mathfrak{v}/\mathfrak{w}=\mathfrak{r}$ (with respect to $(P, \mathfrak{R})$).

We now assume that $\mathfrak{r}$ is a direct sum of (finite or infinite number of) P-submoduli isomorphic to directly indecomposable right-ideal components of P, and want to show that $\mathfrak{w}=0$. For this purpose, let $\mathfrak{r}=\sum\mathfrak{t}_\mu$ be the assumed decomposition of $\mathfrak{r}$, where each $\mathfrak{t}_\mu$ is isomorphic to a right-ideal $f_\mu P$ of P generated by a primitive idempotent element f_μ; f_μ with distinct μ may coincide of course. Let $t_\mu \longleftrightarrow f_\mu$ in the isomorphism, and let v_μ be a counter image of t_μ in our ($(P, \mathfrak{R})$-whence P-) homomorphic mapping of $\mathfrak{v}$ upon $\mathfrak{r}$. Siuce the sum $\sum t_\mu P$ is direct, so is even more the sum $\sum v_\mu f_\mu P$, and the sums are necessarily isomorphic. Hence $\sum v_\mu f_\mu P$ and $\mathfrak{w}$ do not meet, and their (direct) sum coincides with $\mathfrak{v}$, since its image consumes $\mathfrak{r}$; $\mathfrak{v}=\sum v_\mu f_\mu P \oplus \mathfrak{w}$. Then $\mathfrak{v}Q=\sum v_\mu f_\mu Q \oplus \mathfrak{w}Q$. If here $\mathfrak{w} \neq 0$, then $\mathfrak{w} \neq \mathfrak{w}Q$ and $\mathfrak{v}Q \neq \mathfrak{w}$, which contradicts however to that $\mathfrak{v}/\mathfrak{v}Q$ is mapped by our mapping in 1-1 manner. Hence necessarily $\mathfrak{w}=0$, and $\mathfrak{v}$ is $(P, \mathfrak{R})$-isomorphic to $\mathfrak{r}$.

Now $\mathfrak{v}$ is completely determined (up to $(P, \mathfrak{R})$-isomorphism) (by r_i whence) by the $(P, \mathfrak{R})$-structure of $\mathfrak{r}/\mathfrak{r}Q$ and this last is determined, according to the above fully reducible case, by the P-structure of $\mathfrak{r}/\mathfrak{r}Q$. So $\mathfrak{v}$, whence the $(P, \mathfrak{R})$-structure of $\mathfrak{r}$, is determined by the P-structure of $\mathfrak{r}/\mathfrak{r}Q$. Therefore, if a second $(P, \mathfrak{R})$-right-module $\mathfrak{s}$ has a similar P-decomposition and if $\mathfrak{r}/\mathfrak{r}Q$ and $\mathfrak{s}/\mathfrak{s}Q$ are P-isomorphic, then $\mathfrak{r}$ and $\mathfrak{s}$ are $(P, \mathfrak{R})$-isomorphic.

Generally, if $\mathfrak{s}$ is a $(P, \mathfrak{R})$-module such that $\mathfrak{s}/\mathfrak{s}Q$ is P-homomorphic to $\mathfrak{r}/\mathfrak{r}Q$, then $\mathfrak{s}$ is $(P, \mathfrak{R})$-homomorphic to $\mathfrak{r}$. For, $s_i \leqq r_i$ with s_i

introduced similarly as r_i for $\mathfrak{s}$ and the module $\mathfrak{y}$ defined for $\mathfrak{s}$ similarly as $\mathfrak{v}$ for $\mathfrak{r}$ is a direct summand in $\mathfrak{v}$, while $\mathfrak{s}$ is $((P, \mathfrak{R})$-) homomorphic to $\mathfrak{y}$. If here $\mathfrak{s}$ has a similar P-decomposition as $\mathfrak{r}$, then $\mathfrak{r}$ contains as $(P, \mathfrak{R})$-module a direct summand $(P, \mathfrak{R})$-isomorphic to $\mathfrak{s}$.

The above proof of $\mathfrak{w}=0$ can be formulated as follows: Let R be a ring with unit element and satisfying the minimum condition, and N be its radical, or more generally a right-ideal contained in the radical. Let $\mathfrak{v}$, $\mathfrak{r}$ be R-right-moduli and let $\mathfrak{r}$ be a direct sum of submoduli isomorphic to right-ideal direct components of R. Let there be a homomorphic mapping of $\mathfrak{v}$ upon $\mathfrak{r}$ such that it induces an isomorphism of $\mathfrak{v}/\mathfrak{v}N$ and $\mathfrak{r}/\mathfrak{r}N$. Then the mapping must be a 1–1 correspondence between $\mathfrak{v}$ and (the whole of) $\mathfrak{r}$.

So we have only to assume, in order to prove Lemma 5, that $\mathfrak{r}$ and $\mathfrak{s}$ are direct sum of submoduli isomorphic to right-ideal direct components of, instead of P, a between-ring P_1 of $(P, \mathfrak{R})$ and P such that its radical Q_1 contains Q (or such that $(P, \mathfrak{R})Q_1 \supseteq (Q, \mathfrak{R})$ (which implies $\mathfrak{v}Q_1 \supseteq \mathfrak{v}Q$)). It is even allowed to take different P_1 for $\mathfrak{r}$ and $\mathfrak{s}$. (In the previous note we stated rather the case where P_1 is P for $\mathfrak{r}$ and $(P, \mathfrak{R})$ for $\mathfrak{s}$.)

Furthermore, we may replace $(P, \mathfrak{R})$ by its (fixed) residue-ring (and the subrings by the corresponding sub-residue-rings), as was also noted in the previous note, footnote 9), and this takes care of the isomorphism of $R\mathfrak{S}$ and $(R,\mathfrak{S})$ in Remark 5 too; consider namely the residue ring $R\mathfrak{S}$ of $(R,\mathfrak{S})$ and put $P_1=R\mathfrak{S}$ for $\mathfrak{r}=R\mathfrak{S}$ and $P_1=R$ $(\subseteq R\mathfrak{S})$ for $\mathfrak{s}=R$.

Finally, the above proof is free from finiteness restriction and enables us to extend our Galois theory to a certain type of rings without chain conditions; to this point the writer hopes to come back shortly.

Revised Apr. 10, 1948; *Nov.* 15, 1949.

Department of Mathematics
University of Nagoya