QUASI-FROBENIUS RINGS AND GALOIS THEORY[1]

BY
CHARLES W. CURTIS

1. Introduction

In one of his fundamental papers on Frobenius algebras, Nakayama proved that if M is a finitely generated free left module for a quasi-Frobenius ring R, then $\mathrm{Hom}_R(M, M)$ is also a quasi-Frobenius ring. It is not necessarily true, however, that M is also a free $\mathrm{Hom}_R(M, M)$-module. This lack of symmetry is removed in the main result of this paper, which states that if M is a faithful finitely generated projective left module for a quasi-Frobenius ring R, then $\mathrm{Hom}_R(M, M)$ is a quasi-Frobenius ring, and M is a projective $\mathrm{Hom}_R(M, M)$-module. An example is given to show that $\mathrm{Hom}_R(M, M)$ is not always quasi-Frobenius if M is not required to be a projective R-module.

In §3 the theorem is applied to obtain sufficient conditions on a group G of automorphisms of finite reduced order of a simple ring $\mathfrak{P}$ with minimum condition in order that the subring of fixed elements be a quasi-Frobenius ring. A formula is derived for the reduced order of G in terms of the height and index relative to $\mathfrak{P}$ of the indecomposable right ideal direct summands of the fixed ring $I(G)$ of G. These results constitute a first step towards a classification of the subrings of a simple ring with minimum condition which are the fixed rings under groups of automorphisms of the simple ring. A quasi-Frobenius ring seems to be a logical candidate for a subring of fixed elements because it has the property that the double centralizer of any faithful module coincides with the set of scalar multiplications by elements of the ring, a property which any ring which is to play a role in the Galois theory must possess. The main problem remains unsolved, namely to characterize those quasi-Frobenius subrings of a simple ring with minimum condition which are the subrings of fixed elements of groups of automorphisms. We have also made no attempt to solve these problems for rings without chain conditions.

The author is indebted to Professor G. Azumaya for some helpful suggestions and comments on the subject of this paper, and to the referee for pointing out some important simplifications in the proofs of Theorems 1 and 4.

2. A theorem on the structure of the centralizer of a module

Let R be a ring with an identity element, and let R satisfy the minimum condition for left and right ideals. We shall be concerned with left and right R-modules on which the identity element of R is always assumed to act as identity operator. We shall use without further comment the result that any finitely generated left or right R-module satisfies both chain conditions for submodules.

Received November 27, 1957.
[1] This research was supported in part by the Office of Naval Research.

A left module M is called *projective* whenever M is a direct summand of a free left R-module. M is projective if and only if every exact sequence of left modules

$$0 \to P \to Q \to M \to 0$$

splits (see [1], Chapter I, Theorems 2.2, 2.4). It can be proved in general ([6], Theorem 1), and it follows easily from the Krull-Schmidt theorem in case M is finitely generated, that the following characterization of projective modules is valid.

(2.1) *M is projective if and only if M is a direct sum of submodules which are isomorphic to left ideal direct components Re, $e^2 = e$, of R.*

The next result contains the first information on the centralizer of M.

(2.2) *Let M be a finitely generated projective left R-module, where R is any ring with an identity element which satisfies the minimum condition for left and right ideals. Then $\mathrm{Hom}_R(M, M)$ also satisfies the minimum condition for left and right ideals.*

Since M is finitely generated and projective, (2.1) implies that M is a direct summand of a finitely generated free R-module F. Then $\mathrm{Hom}_R(M, M) \cong eAe$, where $A = \mathrm{Hom}_R(F, F)$ and $e \in A$ is a projection of F upon M. Since F is finitely generated, A is isomorphic to a full matrix ring over R, and consequently A satisfies the minimum condition for left and right ideals. An easy computation shows that the chain conditions also hold in eAe, since e is idempotent. This completes the proof of (2.2).

Remark. The author's work on the subject of this paper stems in part from the observation that many of the usual theorems (see [3], Chapters VII and VIII) concerning a finite-dimensional vector space over a division ring admit clean generalizations to a finitely generated projective left R-module. We include a brief outline of these results, which yield in particular an alternative proof of (2.2). Proofs will be omitted. First of all the dual module M' of M is defined to be $\mathrm{Hom}_R(M, R)$; as in the vector space situation, M' is a right R-module. M' also turns out to be finitely generated and projective. If $x \in M$, $f \in M'$, then the mapping $\hat{x}: f \to f(x)$ is an element of $M'' = \mathrm{Hom}_R(M', R)$, and $x \to \hat{x}$ is an isomorphism of M onto M''. Now let $C = \mathrm{Hom}_R(M, M)$. Then M is a right C-module, M' a left C-module, and $M' \otimes_R M$ a two-sided C-module. If we define

$$(f \otimes u)(g \otimes v) = f \otimes g(u)v, \qquad f, g \in M', \quad u, v \in M,$$

then $M' \otimes_R M$ becomes a ring. For each $f \in M'$, $u \in M$, we define an endomorphism $f \times u \in C$ by the formula

$$x(f \times u) = f(x)u.$$

Because M is projective, it follows that the mapping

$$\sum f_i \otimes u_i \to \sum f_i \times u_i$$

is a ring isomorphism, and a two-sided C-isomorphism of $M' \otimes_R M$ onto C. Finally a one-to-one correspondence between the set of left ideals in C and the set of all R-submodules in M (and a similar one between right ideals in C and R-submodules of M') can be established by an argument similar to the discussion in [3], Chapter VIII. The last result, of course, contains (2.2).

DEFINITION. *A quasi-Frobenius ring* R is a ring with an identity element, satisfying both chain conditions for left and right ideals, with the property that

$$l(r(I)) = I, \qquad r(l(J)) = J \tag{1}$$

for every left ideal I and every right ideal J, where $r(S)$ and $l(S)$ denote the right and left annihilators, respectively, of a subset S of R.

Various other sets of conditions are known to be equivalent to (1) for rings satisfying the chain conditions (see [5], [8], and [9]). The most important one for our purposes is proved in [8], and will be restated as follows.

(2.3) *A ring R which satisfies the minimum condition for left and right ideals is quasi-Frobenius if and only if the additive group of R, viewed as a left R-module, is an injective left R-module.*

The following result has been proved for algebras by Nesbitt and Thrall [10].

(2.4) *Let R be quasi-Frobenius, and let M be a finitely generated left R-module. Then M is faithful if and only if every indecomposable left ideal Re, $e^2 = e$, in R is isomorphic to some direct summand of M.*

First let M be faithful, and let e be a primitive idempotent in R. Then Re contains a unique minimal subideal K, and because M is faithful, $Ku \neq 0$ for some $u \in M$. Then $b \to bu$ is an R-isomorphism of Re onto Ru (cf. [10], Lemma II-A, p. 558). Since Re is a direct summand of R, Re is an injective module by (2.3); hence Ru is injective, and is a direct summand of M.

Conversely, suppose that every indecomposable left ideal Re is isomorphic to some direct summand of M. Let a be an element of R such that $aM = 0$. Let e be an arbitrary primitive indempotent in R, and let $\theta: Re \to Q$ be an isomorphism of Re onto a submodule Q of M. Then $aQ = 0$ implies $\theta^{-1}(aQ) = a\theta^{-1}(Q) = aRe = 0$. Since R has an identity element which is a sum of primitive idempotents, the last equation implies that $a = 0$. Therefore M is faithful.

Before we come to the main result of the paper, we record a useful identity. Let R and S be rings, P and Q left R-modules, and let P be at the same time a right S-module such that $r(xs) = (rx)s$ for all r in R, x in M, s in S. Briefly we may say we have the situation $({}_RP_S, {}_RQ)$. Then $\mathrm{Hom}_R(P, Q)$ is a left S-module if we define $(sf)(x) = f(xs)$, s in S, f in $\mathrm{Hom}_R(P, Q)$, x in P. In particular if $P = Q$ and S is the ring $\mathrm{Hom}_R(P, P)$, then the composition we have

just defined is identical with left multiplication in the ring S. Let e be an idempotent in S; then Pe is an R-direct summand of P, and $\mathrm{Hom}_R(Pe, Q)$ may be viewed as a subgroup of $\mathrm{Hom}_R(P, Q)$. If Q happens to be a right S-module, then $\mathrm{Hom}_R(P, Q)$ is a right S-module, and $\mathrm{Hom}_R(Pe, Q)$ is an S-submodule of the right S-module $\mathrm{Hom}_R(P, Q)$. With either interpretation, as subgroup or submodule, we have

$$\mathrm{Hom}_R(Pe, Q) = e\,\mathrm{Hom}_R(P, Q). \tag{2.5}$$

Later in the paper we shall use alternative versions of (2.5) without always stating them explicitly. Now we can state our main result.

THEOREM 1. *Let M be a faithful, finitely generated, projective left module for a quasi-Frobenius ring R. Then M is a finitely generated, projective, right $\mathrm{Hom}_R(M, M)$-module, and $\mathrm{Hom}_R(M, M)$ is a quasi-Frobenius ring.*

We begin the proof by expressing the identity element 1 in R as a sum of primitive idempotents, $1 = \sum_{i=1}^{r} e_i$, and $M = \sum\oplus M_j$, where the M_j are indecomposable R-direct summands of M. By (2.1) there exists for each j at least one integer $i(j)$, $1 \leqq i(j) \leqq r$, such that $M_j \cong Re_{i(j)}$ as left R-modules. Then we have by (2.5) and some elementary properties of the functor "Hom" the following identity:

$$\begin{aligned} C = \mathrm{Hom}_R(M, M) &\cong \textstyle\sum_j\oplus\, \mathrm{Hom}_R(M_j, M) \\ &\cong \textstyle\sum_j\oplus\, \mathrm{Hom}_R(Re_{i(j)}, M) \\ &= \textstyle\sum_j\oplus\, e_{i(j)}\,\mathrm{Hom}_R(R, M) \cong \sum_j\oplus\, e_{i(j)} M, \end{aligned} \tag{2}$$

as right C-modules. Since C is a free right C-module, all the C-modules $e_{i(j)} M$ are projective. Now we use the fact that M is faithful. By (2.4), every Re_i, $1 \leqq i \leqq r$, is isomorphic to one of the M_j. Therefore every idempotent e_i, $1 \leqq i \leqq r$, is an idempotent $e_{i(j)}$ corresponding to an indecomposable M_j, and we conclude that every $e_i M$ is a projective right C-module. Thus $M = \sum_{i=1}^{r}\oplus\, e_i M$ is a projective right C-module. By (2.2), C satisfies the minimum condition and hence the maximum condition for left and right ideals. By (2), M is isomorphic to the direct sum of a finite number of right ideals in C, and hence M is a finitely generated right C-module.

By (2.3) the proof will be completed if we can show that whenever we have the situation $({}_RP_S, {}_RQ)$, where P is a projective right S-module, and Q an injective left R-module, then $\mathrm{Hom}_R(P, Q)$ is an injective left S-module. (In our case, $P = M$, $S = C = \mathrm{Hom}_R(M, M)$, $Q = M$.) The required result is Proposition VI.1.4 in [1]; we shall indicate how the argument may be traced back to the definitions. The definition of injective module ([1], p. 8) requires that for every exact sequence of left S-modules

$$0 \longrightarrow A \xrightarrow{\varphi} B; \tag{3}$$

we prove that there exists a group homomorphism Φ such that the sequence

$$0 \to \mathrm{Hom}_S(A, \mathrm{Hom}_R(P, Q)) \xrightarrow{\Phi} \mathrm{Hom}_S(B, \mathrm{Hom}_R(P, Q)) \tag{4}$$

is exact and $(\Phi f)(\varphi a) = f(a)$ for all a in A and f in $\mathrm{Hom}_S(A, \mathrm{Hom}_R(P, Q))$. Starting from (3), since P is projective, we obtain the exact sequence

$$0 \to P \otimes_S A \xrightarrow{1 \otimes \varphi} P \otimes_S B. \tag{5}$$

Because Q is injective as a left R-module, we have an exact sequence

$$0 \to \mathrm{Hom}_R(P \otimes_S A, Q) \xrightarrow{\Psi} \mathrm{Hom}_R(P \otimes_S B, Q) \tag{6}$$

such that for all $T \in \mathrm{Hom}_R(P \otimes_S A, Q)$, $p \in P$, $a \in A$,

$$(\Psi T)(p \otimes \varphi a) = T(p \otimes a). \tag{7}$$

We observe next that there exists an isomorphism λ of $\mathrm{Hom}_R(P \otimes_S A, Q)$ onto $\mathrm{Hom}_S(A, \mathrm{Hom}_R(P, Q))$ such that for all T in $\mathrm{Hom}_R(P \otimes_S A, Q)$, a in A, p in P, $[(\lambda T)a](p) = T(p \otimes a)$. Similarly there is an isomorphism μ of $\mathrm{Hom}_R(P \otimes_S B, Q)$ onto $\mathrm{Hom}_S(B, \mathrm{Hom}_R(P, Q))$. Then it is immediate that the mapping $\Phi = \mu\Psi\lambda^{-1}$ gives rise to the exact sequence (4) and has the required extension property. This completes the proof of Theorem 1.

COROLLARY 1. *Let R be a quasi-Frobenius ring, and let e be an idempotent in R such that Re is a faithful left R-module. Then Re is a projective right eRe-module, and eRe is quasi-Frobenius.*

Since $eRe \cong \mathrm{Hom}_R(Re, Re)$, Theorem 1 is immediately applicable.

COROLLARY 2. *Let M be a commutative group, and let $\mathfrak{F}^*$ be the family of all quasi-Frobenius subrings R of the full ring of endomorphisms $\mathfrak{E}$ of M which contain the identity endomorphism, and for which M is a finitely generated projective left module. Then $R \to \mathrm{Hom}_R(M, M) = \mathfrak{E}(R)$ is a one-to-one mapping of $\mathfrak{F}^*$ onto itself.*

The result is an immediate consequence of Theorem 1 and the fact that $\mathfrak{E}(\mathfrak{E}(R)) = R$ for all R in $\mathfrak{F}^*$. The proof of the latter statement has been given by Nesbitt and Thrall ([10], p. 560) for algebras, and is applicable to rings as soon as it is known that every finitely generated, faithful left module for a quasi-Frobenius ring contains the reduced regular representation of R as a direct summand. This fact is a direct consequence of (2.3) and (2.4).

3. Automorphism groups of simple rings

In this section we assume familiarity with some parts of the Galois theory of simple rings with minimum condition. The notation we use, and proofs of some elementary facts we require, can be found in Jacobson's book [2], Chapter VI, §8–10. Let $\mathfrak{L}$ be the ring of all linear transformations on a left vector space M over a division ring Δ, and let G be a group of automorphisms

of $\mathfrak{L}$. To each automorphism $l \to l'$ in G there corresponds a semilinear transformation s acting on M such that $l' = s^{-1}ls$ for all $l \in \mathfrak{L}$. We shall denote the automorphism $l \to l' = s^{-1}ls$ by A_s ; then $A_{st} = A_s A_t$ and $A_s = A_t$ if and only if $s = \delta_L t$ for some element $\delta \in \Delta$. The *algebra* $\mathfrak{C}(G)$ of G is the subring of $\mathfrak{L}$ generated by all invertible elements $a \in \mathfrak{L}$ such that $A_a \in G$. We shall denote by G_o the invariant subgroup of G consisting of all inner automorphisms belonging to G; then $\mathfrak{C}(G) = \mathfrak{C}(G_o)$. $\mathfrak{C}(G)$ contains Z, the center of Δ, and may be viewed as an algebra over Z. The ring generated by the semilinear transformations s such that $A_s \in G$ and the elements of Δ_L is called the *endomorphism ring* $\mathfrak{U}(G)$ of G. Evidently $\mathfrak{C}(G)$ is a subring of $\mathfrak{U}(G)$. The group G is said to be of *finite reduced order* if the index $(G:G_o)$ of G_o in G and the dimension $(\mathfrak{C}(G):Z)$ of $\mathfrak{C}(G)$ over Z are both finite; the product of these numbers is called the *reduced order* of G. The subring of $\mathfrak{L}$ consisting of those elements left fixed by all the automorphisms in G is called the *fixed ring* $I(G)$ of G; $I(G)$ turns out to be $\mathrm{Hom}_{\mathfrak{U}(G)}(M, M)$. Throughout this section we shall view M as a right $\mathfrak{L}$-module, and as a right $\mathfrak{U}(G)$-module. (The results of §2 apply equally well to right modules.)

THEOREM 2. *Let G be a group of automorphisms of finite reduced order of the full ring $\mathfrak{L}$ of linear transformations on a finite-dimensional space M over Δ. If the algebra $\mathfrak{C}(G)$ of G is quasi-Frobenius, then $\mathfrak{U}(G)$ is quasi-Frobenius. If M is a projective right $\mathfrak{C}(G)\cdot\Delta_L$-module, then M is a projective right $\mathfrak{U}(G)$-module if and only if for some $X \in I(G_o)$,*

$$\sum_{i=1}^{h} \alpha_i(X) = 1, \tag{8}$$

where $\alpha_1, \cdots, \alpha_h$ is a set of coset representatives of G_o in G. If $\mathfrak{C}(G)$ is quasi-Frobenius, M a projective right $\mathfrak{C}(G)\cdot\Delta_L$-module, and if (8) holds, then $I(G)$ is a quasi-Frobenius ring, and M is a finitely generated projective right $I(G)$-module.

Let $\mathfrak{R}$ be the ring $\mathfrak{C}(G)\cdot\Delta_L$. We shall prove that $\mathfrak{U}(G)$ is a Frobenius extension of $\mathfrak{R}$ in the sense of Kasch [4], and then apply certain results of [4].

(3.1) *Let $\alpha_i = A_{s_i}$, $1 \leqq i \leqq h$. Then every element of $\mathfrak{U}(G)$ can be expressed uniquely in the form*

$$\sum_{i=1}^{h} s_i r_i , \qquad r_i \in \mathfrak{R}. \tag{9}$$

Moreover $s_i^{-1}\mathfrak{R}s_i \subset \mathfrak{R}$, and if we denote the automorphism $r \to s_i^{-1}rs_i$ of $\mathfrak{R}$ by α_i, then

$$rs_i = s_i \alpha_i(r), \tag{10}$$

and for each (i, j) there is a k such that

$$s_i s_j = s_k a_{i,j} , \tag{11}$$

where $a_{i,j}$ is an invertible element of $\mathfrak{R}$.

Let $\alpha = A_s \in G$; then $A_s = A_{s_i} A_a$ for some i and some $a \in \mathfrak{C}(G)$. Then $s = s_i a\delta_L$ for some $\delta \in \Delta$, and it follows that every element of $\mathfrak{U}(G)$ has the

form (9). For a proof of the uniqueness of the coefficients of the expressions (9), we refer to the proof of Proposition 1, §10, Chapter VI of [2]. For the second statement, let $A_a \in G_o$, $a \in \mathfrak{C}(G)$. Then for each i, $A_{s_i}^{-1} A_a A_{s_i} = A_{s_i}^{-1} {}_{as_i} \in G_o$ and $s_i^{-1} a s_i \in \mathfrak{C}(G)$. Since s_i is semilinear, $s_i^{-1}\delta_L s_i \in \Delta_L$. Since $\mathfrak{R} = \mathfrak{C}(G)\Delta_L$ we have $s_i^{-1}\mathfrak{R}s_i \subset \mathfrak{R}$. The formula (10) is immediate from the definition of α_i. For the proof of (11), consider a pair of indices (i, j); then there is a unique k such that

$$A_{s_i} A_{s_j} = A_{s_k} A_a ,$$

where $A_a \in G_o$. Thus $s_k^{-1} s_i s_j = a\delta_L \equiv a_{ij} \in \mathfrak{R}$ since $a \in \mathfrak{C}(G)$, $\delta \in \Delta$; thus (11) is proved.

By (3.1) we see that $\mathfrak{U}(G)$ is a free left $\mathfrak{R}$-module and a free right $\mathfrak{R}$-module. $\mathfrak{U}(G)$ is a *Frobenius extension* of $\mathfrak{R}$ in the sense of Kasch [4] if we can produce a function $f: \mathfrak{U}(G) \to \mathfrak{R}$ such that

$$f(x + y) = f(x) + f(y)$$

$$f(rx) = rf(x), \qquad f(xr) = f(x)r,$$

for all $x, y \in \mathfrak{U}(G)$, $r \in \mathfrak{R}$, and whose kernel contains no right or left ideal different from zero. The mapping f is then called a *Frobenius homomorphism* of $\mathfrak{U}(G)$ into $\mathfrak{R}$; and the associated $\mathfrak{R}$-bilinear mapping

$$F: F(x, y) = f(xy),$$

the *scalar product* determined by f. If $\mathfrak{U}(G)$ possesses a left basis $\{u_i\}$ over $\mathfrak{R}$ and a right basis $\{v_i\}$ over $\mathfrak{R}$, then $\{u_i\}$ and $\{v_i\}$ are *orthogonal* relative to the scalar product F if

$$F(u_i, v_j) = \delta_{ij} \qquad \text{(Kronecker delta)}$$

for all i and j.

(3.2) *$\mathfrak{U}(G)$ is a Frobenius extension of $\mathfrak{R}$ with Frobenius homomorphism $f: f(\sum s_i r_i) = r_1$ where we assume that $A_{s_1} = 1$. The sets $\{s_1^{-1}, \cdots, s_h^{-1}\}$ and $\{s_1, \cdots, s_h\}$ are orthogonal left and right bases of $\mathfrak{U}(G)$ relative to the scalar product determined by f.*

By (3.1) the mapping f is well defined and bilinear. Let $u = \sum_1^h s_i r_i$ be an element of $\mathfrak{U}(G)$ such that $f(vu) = 0$ for all $v \in \mathfrak{U}(G)$. Then for each j, $f(s_1 s_j^{-1} u) = 0$ implies $r_j = 0$, and $u = 0$. Therefore the kernel of f contains no left ideal different from zero. A similar argument, using (10), establishes that no right ideal $\neq 0$ is in the kernel of f. Since $A_{s_1}^{-1}, \cdots, A_{s_h}^{-1}$ is a set of coset representatives of G_o in G, it follows from (3.1) that $s_1^{-1}, \cdots, s_h^{-1}$ is a left basis of $\mathfrak{U}(G)$ over $\mathfrak{R}$. The bases $\{s_i^{-1}\}$ and $\{s_i\}$ are orthogonal by the definition of f.

(3.3) *If $\mathfrak{C}(G)$ is a quasi-Frobenius algebra, finite-dimensional over Z, then $\mathfrak{R}$ is a quasi-Frobenius ring.*

We have $\mathfrak{R} = \mathfrak{C}(G)\Delta_L$, and $a\delta_L = \delta_L a$ for all $a \in \mathfrak{C}(G)$, $\delta \in \Delta$. Since $\mathfrak{C}(G)$ is finite-dimensional over Z, it follows that $\mathfrak{R}$ is a finite-dimensional right vector

space over Δ. From the proof of Proposition 1, §10, Chapter VI of [2], it follows that a Z-basis of $\mathfrak{C}(G)$ is a Δ-basis of $\mathfrak{R}$. Hence $\mathfrak{R}$ is isomorphic to the Kronecker product $\mathfrak{C}(G) \otimes_Z \Delta$, and (3.3) is a consequence of a theorem of Nakayama ([9], Theorem 14); it is also a direct consequence of (2.3).

Finally we come to the proof of Theorem 2. The first statement follows from (3.3), (3.2), and Theorem 10, p. 468 of [4]. Before proving the second statement we recall that a right $\mathfrak{U}(G)$-module is *projective relative to* $\mathfrak{R}$ if every exact sequence

$$0 \to P \to Q \to M \to 0$$

of $\mathfrak{U}(G)$-modules which splits when the modules are viewed as $\mathfrak{R}$-modules also splits with respect to $\mathfrak{U}(G)$. Theorem 12 of [4] states that M is projective relative to $\mathfrak{R}$ if and only if the condition (8) holds. Now let (8) hold, let M be a projective $\mathfrak{R}$-module, and let $\mathfrak{C}(G)$ be quasi-Frobenius. Then M is a faithful finitely generated projective right $\mathfrak{U}(G)$-module, and $\mathfrak{U}(G)$ is quasi-Frobenius. By Theorem 1, $I(G)$ is quasi-Frobenius, and M is a finitely generated projective right $I(G)$-module.

We sketch two further results in the Galois theory. The first may be stated as follows.

THEOREM 3. *Let $\mathfrak{G}$ be the family of all groups of automorphisms of $\mathfrak{L}$ which are complete*[2] *in the sense that $G \in \mathfrak{G}$ implies that G contains every inner automorphism of $\mathfrak{L}$ determined by an invertible element of $\mathfrak{C}(G)$, and for which $\mathfrak{U}(G)$ is quasi-Frobenius and M a finitely generated projective right $\mathfrak{U}(G)$-module. Let $\mathfrak{F}$ be the family of all quasi-Frobenius subrings $\mathfrak{R}$ of $\mathfrak{L}$ such that M is a finitely generated projective right $\mathfrak{R}$-module. Then $G \to I(G)$ is a one-to-one mapping of $\mathfrak{G}$ into $\mathfrak{F}$.*

By Theorem 1 the mapping $G \to I(G)$ is a mapping of $\mathfrak{G}$ into $\mathfrak{F}$. To show that it is one-to-one it is sufficient to prove that, in the terminology of [11], p. 446, the Galois group of $\mathfrak{L}$ over $I(G)$ is G, and for this it is sufficient to prove that G is the group of automorphisms of $\mathfrak{L}$ determined by the semilinear transformations which are units in $\mathfrak{U}(G)$. For this argument in exactly the form we require, we refer to [11], (4.8)–(4.18) and (4.20).

The counterexample given in [2], p. 147 shows that the mapping defined in Theorem 3 is not onto $\mathfrak{F}$.

The second result is a formula for the reduced order of a group $G \in \mathfrak{G}$ (see [11], Proposition 4 or [2], Proposition VI.10.1).

Let $\mathfrak{S}$ be a subring of $\mathfrak{L}$, and let E be an idempotent in $\mathfrak{S}$. We define the (right) *index* $i(E\mathfrak{S}, \mathfrak{L})$ of $E\mathfrak{S}$ in $\mathfrak{L}$ to be the number of minimal right ideals of $\mathfrak{L}$ in a direct decomposition of the right ideal $E\mathfrak{S}\mathfrak{L}$ into minimal $\mathfrak{L}$-ideals. By Proposition III, 7.4 of [2], we see that if $E\mathfrak{S}$ and $F\mathfrak{S}$ are isomorphic right $\mathfrak{S}$-ideals, where E and F are idempotents in $\mathfrak{S}$, then $E\mathfrak{S}\mathfrak{L}$ and $F\mathfrak{S}\mathfrak{L}$ are isomorphic as right $\mathfrak{L}$-ideals, and hence $i(E\mathfrak{S}, \mathfrak{L}) = i(F\mathfrak{S}, \mathfrak{L})$.

[2] This is the terminology of [11]; Jacobson uses the term N-group ([2], p. 140.)

By Theorem 1, if $G \in \mathfrak{G}$ and $\mathfrak{S} = I(G)$, M is a projective right $\mathfrak{S}$-module, and hence to each indecomposable right ideal direct summand $E\mathfrak{S}$ of $\mathfrak{S}$ we can assign a positive integer $h(E\mathfrak{S}, \mathfrak{P})$ called the *height* of $E\mathfrak{S}$ in $\mathfrak{P}$ which counts the number of indecomposable $\mathfrak{S}$-direct summands of M which are isomorphic to $E\mathfrak{S}$. In case $\mathfrak{S}$ is a simple subring of $\mathfrak{P}$ with minimum condition, the concepts of height and index which we have defined coincide with the usual definitions (see [2], p. 135).

THEOREM 4. *Let $G \in \mathfrak{G}$, and let N be the reduced order of G. Let $E_1 I(G), \cdots, E_q I(G)$ be a full set of nonisomorphic indecomposable right ideals of $I(G)$ generated by idempotents $E_1, \cdots, E_q$. Then*

$$\sum_{i=1}^{q} h(E_i I(G), \mathfrak{P}) i(E_i I(G), \mathfrak{P}) = N. \tag{12}$$

The rings $\mathfrak{U}(G)$ and $I(G)$ are both elements of the family $\mathfrak{F}^*$ defined in Corollary 2 of Theorem 1, and are centralizers of each other in the full ring of endomorphisms of M. In our situation, M is a right $\mathfrak{U}(G)$-module and a right $I(G)$-module. We shall write $\mathfrak{C} = \mathrm{Hom}_{I(G)}(M, M)$, and view M as a left $\mathfrak{C}$-module. Then $\mathfrak{C}$ is anti-isomorphic to $\mathfrak{U}(G)$ and contains the ring of scalar multiplications $x \to \alpha x$ written as left operators, which is isomorphic to Δ and will be identified with Δ. By Proposition VI.10.1 of [2], it is sufficient to prove that the expression on the left side of (12) is equal to the left dimension of $\mathfrak{C}$ over Δ.

Let $E_1, \cdots, E_q$ be the full set of primitive idempotents given in the statement of the theorem, and let $M = \sum_{i=1}^{q} \sum_{j=1}^{n_i} \oplus M_{ij}$ be a decomposition of M into indecomposable right $I(G)$-modules, where the M_{ij} are indexed in such a way that for each i, $M_{ij} \cong E_i I(G)$ for all j, and $M_{ij} \cong M_{kl}$ if and only if $i = k$. Then

$$h(E_i I(G), \mathfrak{P}) = n_i, \qquad 1 \leqq i \leqq q. \tag{13}$$

Now let $E_i I(G)\mathfrak{P} = \sum \oplus F_j \mathfrak{P}$, where the $F_j \mathfrak{P}$ are minimal right ideals in $\mathfrak{P}$ generated by orthogonal idempotents F_j. Then $ME_i = \sum \oplus MF_j$, where the MF_j are one-dimensional Δ-subspaces of M. Hence[3]

$$i(E_i I(G), \mathfrak{P}) = [ME_i : \Delta]. \tag{14}$$

Now let $e_{ij} \in \mathfrak{C} = \mathrm{Hom}_{I(G)}(M, M)$ be the projection of M upon M_{ij} determined by the decomposition $M = \sum \sum M_{ij}$. We obtain for each i and j the identifications

$$\begin{aligned} ME_i &\cong \mathrm{Hom}_{I(G)}(I(G), M)E_i = \mathrm{Hom}_{I(G)}(E_i I(G), M) \\ &\cong \mathrm{Hom}_{I(G)}(M_{ij}, M) = \mathrm{Hom}_{I(G)}(e_{ij} M, M) \\ &= \mathrm{Hom}_{I(G)}(M, M)e_{ij} = \mathfrak{C}e_{ij}, \end{aligned}$$

as left $\mathfrak{C}$-modules, by the use of two versions of (2.5). Since $\mathfrak{C} \supseteq \Delta$, the $\mathfrak{C}$-isomorphism of ME_i with $\mathfrak{C}e_{ij}$ is also a Δ-isomorphism, and we have

[3] For this argument, see [11], p. 440.

(15) $$[ME_i:\Delta] = [\mathfrak{C}e_{ij}:\Delta], \quad 1 \leqq i \leqq q, \quad 1 \leqq j \leqq n_i .$$

Upon combining (13), (14), and (15) we obtain

$$[\mathfrak{C}:\Delta]_L = \sum_{i,j} [\mathfrak{C}e_{ij}:\Delta] = \sum_i n_i[ME_i:\Delta]$$
$$= \sum_i h(E_i I(G), \mathfrak{L})i(E_i I(G), \mathfrak{L}),$$

as required.

Remark. Theorem 2 gives one set of sufficient conditions in order that a group G of automorphisms of $\mathfrak{L}$ belong to $\mathfrak{G}$. Another sufficient condition is that $\mathfrak{C}(G)$ be a finite-dimensional semisimple algebra over Z. For then, as Rosenberg and Zelinsky observe ([11], p. 446), $\mathfrak{U}(G)$ is a semisimple ring, and M is a finitely generated projective $\mathfrak{U}(G)$-module.

4. Example

We give an example to show that the hypothesis that the module M be projective cannot be omitted from the statement of Theorem 1.

We present first a few simple results in the theory of a single linear transformation which may be of some independent interest. Let T be a linear transformation on a finite-dimensional space over a field K, and let $R = K[T]$. We shall use the notation and results on the elementary divisor theory of T in the form in which they are presented in [3].

(4.1) *The indecomposable ideal direct summands of the ring $R = K[T]$ are R-isomorphic to the primary components of any cyclic R-submodule of M whose order is the minimum polynomial $\mu(\lambda)$ of T. These components all possess unique minimal submodules.*

Let $\mu(\lambda) = \pi_1(\lambda)^{e_1} \cdots \pi_s(\lambda)^{e_s}$, where the $\pi_i(\lambda)$ are distinct primes in $K[\lambda]$. Let $\{u\}$ be the cyclic submodule whose order is $\mu(\lambda)$. Then $\{u\} = \{u_1\} \oplus \cdots \oplus \{u_s\}$, where $\{u_i\}$ is a cyclic indecomposable submodule whose order is $\pi_i(\lambda)^{e_i}$. The mapping $f(T) \to uf(T)$, $f \in K[\lambda]$, is an R-isomorphism between $K[T]$ and $\{u\}$ since $\mu(\lambda)$ is the minimum polynomial of T. Now consider a fixed $\{u_i\}$, and let $N \neq 0$ be a submodule of $\{u_i\}$. Let $0 \neq u_i\varphi(T) \in N$. Write $\varphi(\lambda) = \pi_i(\lambda)^m\psi(\lambda)$, where $\pi_i(\lambda)$ and $\psi(\lambda)$ are relatively prime, and $m \geqq 0$. It follows that $u_i\,\pi_i(T)^m \in N$, and hence $u_i\,\pi_i(T)^{e_i-1} \in N$, and $\{u_i\,\pi_i(T)^{e_i-1}\}$ is the unique minimal submodule of $\{u_i\}$.

COROLLARY. *$R = K[T]$ is a symmetric algebra, and a fortiori a quasi-Frobenius algebra.*

It is sufficient to consider a single ideal direct summand I of R; then I has a unique minimal subideal $N \neq 0$. Any hyperplane in R which does not contain N cannot contain any ideal different from zero. Hence R is a Frobenius algebra, and since R is commutative, R is a symmetric algebra.

(4.2) *Let T be a linear transformation with minimum polynomial $\mu(\lambda) = \pi_1(\lambda)^{e_1} \cdots \pi_s(\lambda)^{e_s}$, where the $\pi_i(\lambda)$ are distinct primes. Then M is a*

projective $K[T]$-module if and only if every elementary divisor $\pi_j(\lambda)^r$, $r \leqq e_j$, of T has the property that $r = e_j$.

The proof is immediate from (4.1) and (2.1).

In particular the linear transformation with elementary divisors λ^2, λ yields a module which is not projective. We prove that the centralizer $\mathrm{Hom}_R(M, M)$ fails to be quasi-Frobenius. For a suitable basis, the linear transformation has a matrix of the form

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

The set of matrices commuting with this matrix is the algebra C of all matrices

$$\begin{pmatrix} a & 0 & 0 \\ c & b & 0 \\ e & d & a \end{pmatrix},$$

where a, b, c, d, e are arbitrary in K. Let I be the right ideal $e_{31}C$, where e_{ij} denotes a matrix unit. Then $I = Ke_{31}$; $l(I) = Ke_{22} + Ke_{21} + Ke_{31} + Ke_{32}$, and $r(l(I)) = Ke_{31} + Ke_{32} \neq I$. Therefore C is not quasi-Frobenius.

Added in proof. Theorem 1 of this paper has also been proved by K. Morita in his recent article, *Duality for modules and its applications to the theory of rings with minimum condition*, Science Reports of the Tokyo Kyoiku Daigaku, Section A, vol. 6 no. 150 (1958), pp. 83–142; see in particular Theorem 16.6, p. 133.

References

1. H. Cartan and S. Eilenberg, *Homological algebra*, Princeton, 1956.
2. N. Jacobson. *Structure of rings*, Amer. Math. Soc. Colloquium Publications, vol. 37, 1956.
3. ———, *Lectures in abstract algebra*, vol. 2, New York, 1953.
4. F. Kasch, *Grundlagen einer Theorie der Frobeniuserweiterungen*, Math. Ann., vol. 127 (1954), pp. 453–474.
5. K. Morita and H. Tachikawa, *Character modules, submodules of a free module, and quasi-Frobenius rings*, Math. Zeit., vol. 65 (1956), pp. 414–428.
6. H. Nagao and T. Nakayama, *On the structure of (M_0)- and (M_u)-modules*, Math. Zeit., vol. 59 (1953), pp. 164–170.
7. S. Eilenberg, M. Ikeda, and T. Nakayama, *On the dimension of modules and algebras, I*, Nagoya Math. J., vol. 8 (1955), pp. 49–57.
8. S. Eilenberg and T. Nakayama, *On the dimension of modules and algebras, II*, Nagoya Math. J., vol. 9 (1955), pp. 1–16.
9. T. Nakayama, *On Frobeniusean algebras. II*, Ann. of Math. (2), vol. 42 (1941), pp. 1–21.
10. C. J. Nesbitt and R. M. Thrall, *Some ring theorems with applications to modular representations*, Ann. of Math. (2), vol. 47 (1946), pp. 551–567.
11. A. Rosenberg and D. Zelinsky, *Galois theory of continuous transformation rings*, Trans. Amer. Math. Soc., vol. 79 (1955), pp. 429–452.

University of Wisconsin
Madison, Wisconsin