Journal of Pure and Applied Algebra 31 (1984) 139–184
North-Holland

GALOIS THEORY OF PRIME RINGS

S. MONTGOMERY
Dept. of Mathematics, University of Southern California, Los Angeles, CA 90089, USA

D.S. PASSMAN
Dept. of Mathematics, University of Wisconsin–Madison, Madison, WI 53706, USA

Communicated by F. Van Oystaeyen
Received December 1982

Introduction

The Galois theory of noncommutative rings is a natural outgrowth of the classical Galois theory of fields. Let G be a group of automorphisms of a ring R. Then we are concerned with the relationship between R and the fixed ring R^G and with the relationship between the subgroups of G and the intermediate rings $S \supseteq R^G$. Needless to say, some assumptions on R and reasonably strong assumptions on G are required for really good results.

Work on this subject was begun by E. Noether [9 (1933)] in her study of inner automorphisms of central simple algebras. This was continued in the 1940's and 1950's where the work still concerned rather special rings R. For example the Galois theory of division rings was initiated by N. Jacobson [7 (1940)] and [8 (1947)], H. Cartan [1 (1947)] and G. Hochschild [5 (1949)]. Complete rings of linear transformations were investigated by T. Nakayama and G. Azumaya [17 (1947)], J. Dieudonné [3 (1948]) and somewhat later A. Rosenberg and D. Zelinsky [20 (1955)] studied continuous transformation rings. Much of this can be found in Jacobson's book [9 (1956)]. In addition, simple Artinian rings were considered by G. Hochschild [6 (1950)], T. Nakayama [18 (1952)] and in a long series of papers by H. Tominaga and T. Nagahara leading to their monograph [21 (1970)].

In the 1960's a great deal of work was done on the Galois theory of separable algebras. Among the many papers on this subject, we note in particular [15 (1966)] by Y. Miyashita, [2 (1967)] by L.N. Childs and F.R. DeMeyer, [22 (1969)] by O.E. Villamayor and D. Zelinsky and [14 (1970)] by H.F. Kreimer. The best results to date are due to V.K. Kharchenko in [10 (1975)], [11 (1975)] and [12 (1977)] where he develops a Galois theory for semiprime rings.

In the beginning of this paper we discuss the work of Kharchenko in the special case of prime rings. We have made this simplifying assumption to greatly facilitate the exposition. The proofs in the semiprime case invariably start with a Zorn's lemma argument to find an idempotent maximal with some property and then proceed as in the prime case. There are admittedly a number of difficult technical details which must be handled when R is semiprime. Nevertheless, the basic flow of the proofs is the same and at the very least we hope this part of the paper can serve as an introduction to [12].

Although most of the results in Sections 2 through 8 and half of those in Section 9 are due to Kharchenko, there are some new approaches and some new emphasis here. For example in Section 2 we offer a new proof of the existence of trace forms. Later, our use of trace forms of minimal length avoids the notion of independence of automorphisms. In Section 5, we stress the bimodule properties as a key ingredient in the theory. Our formulation of the Galois homogeneity condition in Section 6 differs from the original and we think it is more natural.

In the remainder of this paper, most of the results are new. In Section 9 we consider the minimal primes of R^G. In Sections 10 and 11 we study the problem of extending isomorphisms between intermediate rings, using an idea from [13 (1978)]. This enables us, in Section 12, to determine when certain intermediate rings are Galois over R^G. This paper starts with basic notation and statements of the main results in Section 1. It ends with some examples.

With the exception of a few simple assumed facts on the Martindale ring of quotients, this paper is essentially self-contained. A good basic reference for the missing material and for other aspects of Galois theory is the monograph by S. Montgomery [16 (1980)]. In addition, we recommend the very pleasant survey article [4 (1980)] by J.W. Fisher and J. Osterburg.

1. N-groups of automorphisms

We are concerned with the action of a group G on a prime ring R. As is to be expected, certain finiteness assumptions are required for G. However, in order to even state these, we must first introduce the Martindale ring of quotients of R.

Let R be prime ring and consider the set of all left R-module homomorphisms $f: {}_RI \to {}_RR$ where I ranges over all nonzero two-sided ideals of R. Two such functions are said to be equivalent if they agree on their common domain, which is a nonzero ideal since R is prime. It is easy to see that this is an equivalence relation. Indeed, what is needed here is the observation that if $f: {}_RI \to {}_RR$ with $If=0$ and if f is defined on $r \in R$, then $rf=0$. This follows since $Ir \subseteq I$ so $0=(Ir)f=I(rf)$ and hence $rf=0$ in this prime ring. We let $\hat{f}$ denote the equivalence class of f and let $Q=Q_0(R)$ be the set of all such equivalence classes.

The arithmetic in Q is defined in a fairly obvious manner. Suppose $f: {}_RI \to {}_RR$ and $g: {}_RJ \to {}_RR$. Then $\hat{f}+\hat{g}$ is the class of $f+g: {}_R(I \cap J) \to {}_RR$ and $\hat{f}\hat{g}$ is the class of the composite function $fg: {}_R(JI) \to {}_RR$. It is easy to see that these definitions make sense and that they respect the equivalence relation. Furthermore, the ring axioms are surely satisfied so Q is a ring with 1. Finally let $r_\rho: {}_RR \to {}_RR$ denote right multiplication by $r \in R$. Then the map $r \to \hat{r}_Q$ is easily seen to be a ring homomorphism from R into Q. Moreover, if $r \neq 0$ then $Rr_Q \neq 0$ and hence $\hat{r}_Q \neq 0$ by the observation of the preceding paragraph. We conclude therefore that R is embedded isomorphically in Q with the same 1 and we will view Q as an overring of R. It is the *Martindale ring of quotients* of R.

Suppose $f: {}_R I \to {}_R R$ and $a \in I$. Then $a_Q f$ is defined on ${}_R R$ and for all $r \in R$ we have

$$r(a_Q f) = (ra)f = r(af) = r(af)_Q.$$

Hence $\hat{a}_Q \hat{f} = \widehat{(af)}_Q$ and the map f translates in Q to right multiplication by $\hat{f}$. With this observation, the following well known result is an elementary exercise.

Lemma 1.1. *Let $Q = Q_0(R)$.*

(i) *If $q \in Q$ and $Iq = 0$ for some nonzero ideal I of R, then $q = 0$.*

(ii) *If $q_1, q_2, \ldots, q_n \in Q$, then there exists a nonzero ideal I of R with $Iq_1, Iq_2, \ldots, Iq_n \subseteq R$.*

(iii) *Q is prime. Indeed if $q_1 I q_2 = 0$ for $q_1, q_2 \in Q$ and I a nonzero ideal of R, then $q_1 = 0$ or $q_2 = 0$.*

(iv) *If σ is an automorphism of R, then σ extends uniquely to an automorphism of Q.*

(v) *If $C = \mathbb{C}_Q(R)$, then C is a field and the center of Q.*

The field C above is called the *extended centroid* of R. By (iv), we can view $\operatorname{Aut} R$ as a subgroup of $\operatorname{Aut} Q$. An automorphism σ of R is said to be *X-inner* if and only if it is induced by conjugation by a unit of Q. In other words, these automorphisms arise from those units $q \in Q$ with $q^{-1}Rq = R$. If q and u are two such units, then clearly so is qu^{-1}. Thus we see immediately from (iv) that $\operatorname{Inn} R$, the set of all X-inner automorphisms of R, is a normal subgroup of $\operatorname{Aut} R$.

Now let G act on R and set $G_0 = G \cap \operatorname{Inn} R \lhd G$. Thus for each $g \in G_0$ there exists at least one unit $q \in Q$ such that g is equal to conjugation by q. We now let $B = B(G) = B_R(G)$ denote the linear span of all units $q \in Q$ such that $q^{-1}Rq = R$ and conjugation by q is contained in G and hence in G_0. By definition, B is closed under addition. Furthermore, if $q, u \in Q$ give rise to $g, h \in G$ respectively, then surely qu gives rise to $gh \in G$. Thus we see that B is closed under multiplication. Moreover $B \supseteq C$ since the elements of $C \setminus 0$ are units which centralize R and hence give rise to the identity automorphism. Thus B is a C-subalgebra of Q called the *algebra of the group* of G.

We can now state the necessary finiteness assumptions on G. The group G is said to be an *M-group* of automorphisms of R if and only if

(i) $[G : G_0] < \infty$

(ii) B is a semisimple finite dimensional C-algebra.

The product $[G : G_0] \cdot \dim_C B$ is the *reduced order* of G.

Now let $R^G=\{r\in R \mid r^g=r \text{ for all } g\in G\}$ be the *fixed ring* of G. Since B is spanned by units which act like elements of G, it is clear that B centralizes R^G. In particular, conjugation by any unit of B fixes R^G. Because of this, we introduce the following completeness condition. The group G is said to be an *N-group* (for Emmy Noether) of automorphisms of R if and only if G satisfies (i), (ii) above and

(iii) If b is any unit of B, then $b^{-1}Rb=R$ and conjugation by b is an element of G.

For many results, we can in fact assume the weaker hypothesis that if b is any unit of B which normalizes R, then conjugation by b belongs to G. However we will stay with this stronger assumption.

If S is a subring of R, we define $\mathcal{G}(R/S)=\{\sigma\in \operatorname{Aut} R \mid \sigma \text{ fixes } S\}$.Then S is a *Galois subring* of R if S is the fixed ring of $\mathcal{G}(R/S)$. The first main result, proved in Section 4, is

Theorem A. *Let G be an N-group of automorphisms of the prime ring R. Then $\mathcal{G}(R/R^G)=G$.*

Now suppose R, G and B are as above and let S be an intermediate ring so that $R\supseteq S\supseteq R^G$. In order to decide whether S is a Galois subring of R, the following four conditions come into play.

[GZ] (*Centralizer*) If $Z=\mathbb{C}_B(S)$, then Z is a semisimple algebra spanned by its units.

[GI] (*Idempotent*) Let e be an idempotent of B with $eS(1-e)=0$. Then there exists an idempotent $f\in Z=\mathbb{C}_B(S)$ with $Be=Bf$.

[GH] (*Homogeneity*) Suppose $b\in B\setminus 0$, $g\in G$ and $bs=s^gb$ for all $s\in S$. Then $g=hg_0$ where $h\in \mathcal{G}(R/S)$ and $g_0\in G\cap \operatorname{Inn} R$.

[GC] (*Cancellation*) Suppose K is an ideal of S with $\mathrm{r}_R(K)=0$. If $r\in R$ and $Kr\subseteq S$, then $r\in S$.

The main result on Galois subrings, proved in Section 7 is

Theorem B. *Let G be an N-group of automorphisms of the prime ring R and let $R\supseteq S\supseteq R^G$. Then S is the fixed ring of an N-subgroup H of G if and only if S satisfies* [GZ], [GI], [GH] *and* [GC].

This gives rise to numerous correspondence theorems obtained in Section 8. The next part of this paper is concerned with the structure of the minimal primes of R^G and with the nature of the isomorphisms between intermediate rings. For example, we prove in Section 11 a precise version of

Theorem C. *Let G be an N-group of automorphisms of the prime ring R and let*

$S, \bar{S} \supseteq R^G$ both satisfy [GZ], [GI] *and* [GH]. *Suppose $\varphi: S \to \bar{S}$ is an isomorphism which is the identity on R^G and assume that P and $\bar{P} = P^\varphi$ are corresponding minimal primes of S and $\bar{S}$. Then there exists an element $g \in G$ which 'induces', in a well defined manner, the isomorphism $\varphi: S/P \to \bar{S}/\bar{P}$.*

In Section 12, we consider when certain intermediate rings are Galois over R^G. For this we require some definitions. Let G be an N-group of automorphisms of R. If K is an M-subgroup of G, then K can be completed to an N-subgroup $\tilde{K}$ of G by adjoining to K the action of all units of $B(K)$. Clearly $B(K) = B(\tilde{K})$ and $R^K = R^{\tilde{K}}$ since any element of R fixed by K is fixed by all units of $B(K)$. Now let H be a subgroup of G. Then we say that H is *almost normal* in G if $K = \mathbb{N}_G(H)$ is an M-group with completion $\tilde{K} = G$. In addition we say that H is an *F-group* if it is an N-group with $B(H)$ a simple ring. We remark that if H is an F-group, then R^H is necessarily a prime ring. Finally we say that R is *N-group Galois* over S if $\mathcal{G}(R/S)$ is an N-group with fixed ring S. We prove

Theorem D. *Let G be an N-group of automorphisms of the prime ring R and let H be an F-subgroup of G. Then R^H is N-group Galois over R^G if and only if H is almost normal in G.*

We close this section with two simple, but crucial, observations about the units of Q.

Lemma 1.2. *Let G be an M-group of automorphisms of R and let $b \in B$. Then there exists a nonzero ideal I of R with $Ib \subseteq R$ and $bI \subseteq R$.*

Proof. Suppose first that q is a unit of B which corresponds to an X-inner automorphism $g \in G$. By Lemma 1.1(ii), there exists an ideal $J \neq 0$ of R with $Jq \subseteq R$. Moreover $qJ^g = q(q^{-1}Jq) \subseteq R$ so the result follows for q by taking $I = J \cap J^q$. Finally, by definition of B, any $b \in B$ is a finite sum $b = q_1 + q_2 + \cdots + q_n$ of such units $q_i \in B$. By the above, for each i there is a nonzero ideal I_i of R with $I_i q_i \subseteq R$ and $q_i I_i \subseteq R$. Since R is prime, the result follows for b by taking $I = I_1 \cap I_2 \cap \cdots \cap I_n \neq 0$.

Lemma 1.3. *Let $q \in Q \setminus 0$ and let σ be an automorphism of R with $rq = qr^\sigma$ for all $r \in R$. Then q is a unit of Q and σ is X-inner induced by q.*

Proof. The relation $rq = qr^\sigma$ implies easily that $l_R(q)$ is a two-sided ideal of R. Thus since $q \neq 0$ we conclude from Lemma 1.1(i) that $l_R(q) = 0$. Now let I be a nonzero ideal of R with $Iq \subseteq R$. Since $Iq = qI^\sigma$, we see that $Iq = J$ is also a two-sided ideal of R. Furthermore since $l_R(q) = 0$, the right multiplication map $q: I \to J$ is one-to-one and onto. Hence if $f: J \to I$ denotes the inverse map, then $\hat{f} \in Q$ is clearly the inverse of q in Q. Finally the formula $q^{-1}rq = r^\sigma$ implies that σ is X-inner and in fact induced from q.

2. Existence of trace forms

The goal here is to construct certain trace forms, that is linear maps, which send R to R^G. We start by considering any finite dimensional algebra A over a field C. If $A^* = \mathrm{Hom}_C(A, C)$ is the dual group of A, then A^* can be given a right A-module structure by defining the functional λa to be

$$\lambda a(z) = \lambda(az) \quad \text{for all } z \in A.$$

Here $\lambda \in A^*$ and $a \in A$.

The first part of the following well known result asserts that the module A^* is isomorphic to the left regular representation of A. For the second part, if V is a vector space over C, we say that a basis of V is compatible with the decomposition $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ if and only if it is a union of bases of the subspaces V_i.

Lemma 2.1. *Let $\{a_1, a_2, \ldots, a_n\}$ be a basis for A and let $\{a_1^*, a_2^*, \ldots, a_n^*\}$ be its dual basis in A^*.*

(i) *If $a \in A$ with $aa_i = \sum_j a_j c_{ij}$, then $a_j^* a = \sum_i c_{ij} a_i^*$.*

(ii) *If e is an idempotent of A, then $\{a_i\}$ is compatible with $eA \oplus (1-e)A$ if and only if $\{a_i^*\}$ is compatible with $A^*e \oplus A^*(1-e)$. Furthermore when this occurs then $a_i \in eA$ if and only if $a_i^* \in A^*e$.*

Proof. For (i) write $aa_i = \sum_j a_j c_{ij}$ and write $a_j^* a = \sum_i d_{ij} a_i^*$ with $c_{ij}, d_{ij} \in C$. Then

$$d_{ij} = a_j^* a(a_i) = a_j^*(aa_i) = c_{ij}.$$

For (ii), take $a = e$ in the above. Then $\{a_1, a_2, \ldots, a_n\}$ is compatible with $eA \oplus (1-e)A$ if and only if the matrix $[c_{ij}]$ is diagonal with 0 and 1 entries on the diagonal. Furthermore, by (i) above this is precisely the same criteria for $\{a_1^*, a_2^*, \ldots, a_n^*\}$ to be compatible with $A^*e \oplus A^*(1-e)$. Finally when this occurs then $a_i \in eA$ if and only if $c_{ii} = 1$ and then if and only if $a_i^* \in A^*e$.

We are interested in whether nontrivial module homomorphisms $\theta: A^* \to A$ exist. Indeed, if $A \simeq A^*$, then A is said to be a Frobenius algebra and the following is a well known necessary and sufficient condition for this to occur.

Lemma 2.2. *We have $A \simeq A^*$ if and only if there exists $\lambda \in A^*$ whose kernel contains no nonzero right ideal of A. Furthermore if A is semisimple, then A is Frobenius.*

Proof. Observe that any module homomorphism $f: A \to A^*$ is determined by $f(1) = \lambda$. Moreover $f(a) = \lambda a$ is the zero map if and only if $aA \subseteq \ker \lambda$. Thus f is one-to-one and hence an isomorphism if and only if the kernel of λ contains no nonzero right ideal.

Finally if A is semisimple, write $A = \bigoplus A_i$ as a ring direct sum of simple rings. Since $A^* = \bigoplus A_i^*$, it clearly suffices in view of Lemma 2.1(ii) to show that $A_i \simeq A_i^*$

as A_i-modules. But this is trivial since $\dim A_i = \dim A_i^*$, both modules are completely reducible and A_i has a unique irreducible module.

We remark that the above condition on λ is actually right-left symmetric. Furthermore if A has a 2-dimensional right ideal K all of whose subspaces are right ideals, then it is clear that no such λ exists and A is not Frobenius.

Now we assume that G acts on the prime ring R and that the algebra of the group B is finite dimensional over C. Moreover $[G:G_0]<\infty$ where $G_0 = G \cap \operatorname{Inn} R$. We define certain linear functions $\tau: Q \to Q$.

Lemma 2.3. *Let $\theta: B^* \to B$ be a right B-module homomorphism. Let Λ be a transversal for G_0 in G with $1 \in \Lambda$ and let $b_1, b_2, \ldots, b_n$ be a C-basis for B. Then the trace form*

$$\tau(x) = \sum_{i,g\in\Lambda} (b_i x \theta(b_i^*))^g = \sum_{i,g} a_{ig} x^g b_{ig}$$

satisfies $a_{ig}, b_{ig} \in B$ and $\tau(Q) \subseteq Q^G$.

Proof. Let us first consider $\tau_1(x) = \sum_i b_i x \theta(b_i^*)$. If $b \in B$ and $bb_i = \sum_j b_j c_{ij}$, then by Lemma 2.1(i) since C is the center of Q we have

$$b\Big(\sum_i b_i x\theta(b_i^*)\Big) = \sum_i bb_i x\theta(b_i^*) = \sum_i \Big(\sum_j b_j c_{ij}\Big) x\theta(b_i^*)$$

$$= \sum_j b_j x\theta\Big(\sum_i c_{ij} b_i^*\Big) = \sum_j b_j x\theta(b_j^* b).$$

Moreover since θ is a right B-module homomorphism, this last term equals $(\sum_j b_j x\theta(b_j^*))b$. Thus for all $x \in Q$, $\tau_1(x)$ commutes with B and in particular with G_0. Since Λ is a transversal for $G_0 \lhd G$, it is now immediate that $\tau(x) = \sum_{g\in\Lambda} \tau_1(x)^g$ maps Q to Q^G.

Now let us specialize to the case in which B is semisimple so that an isomorphism $\theta: B^* \to B$ exists.

Lemma 2.4. *Let G be an M-group and let Λ be a transversal for $G_0 = G \cap \operatorname{Inn} R$ in G with $1 \in \Lambda$. Then there exist trace forms*

$$\tau(x) = \sum_{i,g\in\Lambda} a_{ig} x^g b_{ig}$$

with $a_{ig}, b_{ig} \in B$ and $\tau(Q) \subseteq Q^G$ such that

(i) *For each $g \in \Lambda$, $\{a_{ig}\}$ and $\{b_{ig}\}$ are C-bases of B.*

(ii) *Either basis $\{a_{i1}\}$ or $\{b_{i1}\}$ may be prescribed beforehand.*

(iii) *If $e \in B$ is an idempotent, then $\{a_{i1}\}$ is compatible with $B = eB \oplus (1-e)B$ if and only if $\{b_{i1}\}$ is compatible with $B = Be \oplus B(1-e)$. Furthermore when this occurs then $a_{i1} \in eB$ if and only if $b_{i1} \in Be$.*

Proof. Since G is an M-group, B is semisimple so a right B-module isomorphism $\theta: B^* \to B$ exists by Lemma 2.2. We now apply Lemma 2.3 with this particular θ. Then for any choice of basis $\{b_i\}$, the trace form $\tau(x)$ so constructed satisfies $\tau(Q) \subseteq Q^G$ and $a_{ig}, b_{ig} \in B$. Note that $1 \in \Lambda$ by assumption.

Now $a_{i1} = b_i$ and $b_{i1} = \theta(b_i^*)$ so both $\{a_{i1}\}$ and $\{b_{i1}\}$ are bases of B. Moreover the basis $\{a_{i1}\}$ may clearly be prescribed beforehand by taking $b_i = a_{i1}$ and the basis $\{b_{i1}\}$ may be prescribed by choosing $\{b_i\}$ to be the dual basis to $\{\theta^{-1}(b_{i1})\}$ in $B^{**} = B$. Indeed if $b_i = \theta^{-1}(b_{i1})^*$, then $b_i^* = \theta^{-1}(b_{i1})^{**} = \theta^{-1}(b_{i1})$ so $\theta(b_i^*) = b_{i1}$. Thus we have (i) and (ii) since $a_{ig} = a_{i1}^g$ and $b_{ig} = b_{i1}^g$.

Finally let $e \in B$ be an idempotent. Since θ is an isomorphism and $b_{i1} = \theta(b_i^*)$ it is clear that $\{b_1^*, b_2^*, \ldots, b_n^*\}$ is compatible with $B^* = B^*e \oplus B^*(1-e)$ if and only if $\{b_{11}, b_{21}, \ldots, b_{n1}\}$ is compatible with $B = Be \oplus B(1-e)$. Therefore since $a_{i1} = b_i$, part (iii) now follows immediately from Lemma 2.1(ii).

Since the coefficients of these trace forms belong to B, it is not necessarily true that $\tau(R) \subseteq R$. However we do have

Lemma 2.5. *Let $\tau(x) = \sum_{i,g} a_{ig} x^g b_{ig}$ be as in Lemma 2.3 or 2.4. Then there exists a nonzero ideal I of R such that $\tau(I) \subseteq R^G$. Indeed if J is any nonzero ideal of R, then there exists a nonzero ideal $K \subseteq J$ with $\tau(K) \subseteq J \cap R^G$.*

Proof. Let J be a nonzero ideal of R and let $a, b \in B$ and $g \in G$. Then by Lemma 1.2 there exist nonzero ideals K_1 and K_2 of R with $a^{g^{-1}} K_1 \subseteq R$ and $K_2 b^{g^{-1}} \subseteq R$. Thus

$$a^{g^{-1}}(K_1 J^{g^{-1}} K_2) b^{g^{-1}} \subseteq J^{g^{-1}}$$

and hence $a(K_1 J^{g^{-1}} K_2)^g b \subseteq J$. In other words we have shown that for each summand $a_{ig} x^g b_{ig}$ of τ there exists a nonzero ideal K_{ig} with $a_{ig}(K_{ig})^g b_{ig} \subseteq J$. Thus setting $K = J \cap \bigcap_{i,g} K_{ig} \neq 0$ we see that $K \subseteq J$ and $\tau(K) \subseteq J$. Since $\tau(Q) \subseteq Q^G$, by Lemma 2.3 or 2.4, we therefore have $\tau(K) \subseteq J \cap R^G$. The result now follows by taking I to be the appropriate ideal for $J = R$.

3. Truncation of trace forms

In this section we consider certain trace forms

$$T(x) = \sum_i a_i x^{\sigma_i} b_i$$

with $a_i, b_i \in Q$ and $\sigma_i \in \operatorname{Aut} R$. If $r, s \in R$, then

$$rT(sx) = \sum_i (r a_i s^{\sigma_i}) x^{\sigma_i} b_i$$

is also a trace form with the same b_i, σ_i. The idea here is to study sums of expressions of this type and any such expression

$$\tilde{T}(x)=\sum_k r_k T(s_k x)$$

is called a (left) *truncation* of T. Notice that

$$\tilde{T}(x)=\sum_i \tilde{a}_i x^{\sigma_i} b_i \quad \text{with} \quad \tilde{a}_i=\sum_k r_k a_i s_k^{\sigma_i}.$$

If the (left) support of T is defined by $\{i \mid a_i \neq 0\}$, then it is clear that $\operatorname{Supp} \tilde{T} \subseteq \operatorname{Supp} T$. Furthermore, any truncation of $\tilde{T}$ is certainly also one of T. We seek truncations of T of minimal support size.

Observe that if any σ is X-inner, induced by $q \in Q$, then for any $x \in R$ we have $x^\sigma = q^{-1}xq$. Because of this we can usually assume that no X-inner automorphisms other than $\sigma = 1$ occur in T. Indeed we say that T, as above, is an *outer form*, if $\sigma_i \in \operatorname{Inn} R$ implies $\sigma_i = 1$.

Lemma 3.1. *Let $T(x)=\sum_i a_i x^{\sigma_i} b_i$ be an outer trace form with $\sigma_0=1$, $a_0 \neq 0$. Then there exist $r_k, s_k \in R$ (depending only upon the a_i's and σ_i's) such that*

$$\tilde{T}(x)=\sum_k r_k T(s_k x)=\sum_i \tilde{a}_i x^{\sigma_i} b_i$$

satisfies $\tilde{a}_i \in R$, $\tilde{a}_0 \neq 0$. Furthermore, if $\tilde{a}_i \neq 0$, then $\sigma_i = 1$ and $\tilde{a}_i = \tilde{a}_0 c_i$ for some $c_i \in C$ with $c_0 = 1$.

Proof. As we will see, the b_i's merely play the role of a place holder here. Thus the r_k, s_k elements obtained depend only the a_i's and σ_i's.

For each i there exists a nonzero ideal L_i of R with $L_i a_i \subseteq R$. Thus if $L=\bigcap L_i \neq 0$, then $La_i \subseteq R$ for all i. Furthermore $La_0 \neq 0$. Thus if $r \in L$ is chosen with $ra_0 \neq 0$, then $rT(x)$ is a truncation $\tilde{T}$ of T with all $\tilde{a}_i \in R$ and $\tilde{a}_0 \neq 0$. We can now assume that T has this property.

The proof proceeds by induction on $|\operatorname{Supp} T|$, the case $|\operatorname{Supp} T| = 1$ being trivial. Suppose now that $|\operatorname{Supp} T| > 1$. If $\tilde{T}$ is a truncation of T with $|\operatorname{Supp} \tilde{T}| < |\operatorname{Supp} T|$, then the result will follow by induction provided $\tilde{a}_0 \neq 0$. Thus we can assume that in any truncation of T of smaller support size, the $\tilde{a}_0$ term vanishes.

We next show that if $\tilde{T}=\sum_i \tilde{a}_i x^{\sigma_i} b_i$ is a truncation of T with $|\operatorname{Supp} \tilde{T}| < |\operatorname{Supp} T|$, then all $\tilde{a}_i = 0$, that is $\tilde{T}=0$. To this end, we already know that $\tilde{a}_0 = 0$ and we consider $\tilde{a}_k$ for $k \neq 0$. For any $r \in R$ form the truncation

$$T'(x)=\tilde{a}_k r T(x) - \tilde{T}((ra_k)^{\sigma_k^{-1}} x)=\sum_i a_i' x^{\sigma_i} b_i$$

so that

$$a_i' = \tilde{a}_k r a_i - \tilde{a}_i (ra_k)^{\sigma_k^{-1}\sigma_i}.$$

Then $a_k' = 0$ so $|\operatorname{Supp} T'| < |\operatorname{Supp} T|$ and we must have $a_0' = 0$. Since $\tilde{a}_0 = 0$ this yields $0 = a_0' = \tilde{a}_k r a_0$ for all $r \in R$. Since R is prime and $a_0 \neq 0$ we conclude that $\tilde{a}_k = 0$.

We now know that any truncation of T of properly smaller support size must be identically zero. Let $J = Ra_0R$ be the nonzero ideal of R generated by a_0. Then for each $j \in J$, it is clear that there is truncation $\tilde{T}_j(x)$ of T with

$$\tilde{T}_j(x) = \sum_i \tilde{a}_i(j)x^{\sigma_i}b_i$$

and $\tilde{a}_0(j) = j$. Furthermore we claim that the coefficients $\tilde{a}_i(j)$ are uniquely determined. Indeed if $\tilde{T}_j(x)$ and $T_j'(x)$ are two truncations of T with the same 0-coefficient j, then $\tilde{T}_j - T_j'$ is a truncation of smaller support size and hence is identically zero.

Thus for each i, $\tilde{a}_i : J \to R$ is a well defined function. It is surely additive and it is in fact a left R-module homomorphism. Indeed by considering $r\tilde{T}_j(x)$ we see that $\tilde{a}_i(rj) = r\tilde{a}_i(j)$. Thus there exists $q_i \in Q$ with $\tilde{a}_i(j) = jq_i$ and hence

$$\tilde{T}_j(x) = \sum_i (jq_i)x^{\sigma_i}b_i$$

with $q_0 = 1$. Furthermore, since $\sigma_0 = 1$ it follows, by considering $\tilde{T}_j(sx)$, that

$$jsq_i = \tilde{a}_i(js) = \tilde{a}_i(j)s^{\sigma_i} = jq_is^{\sigma_i}.$$

But this holds for all $j \in J$ so $sq_i = q_is^{\sigma_i}$ for all $s \in R$. Since $q_i \neq 0$ for those terms in the support of T we conclude from Lemma 1.3 that q_i is a unit inducing the X-inner automorphism σ_i. By assumption, T is an outer form, so this implies that $\sigma_i = 1$ and $q_i \in C$.

We have therefore shown, summing over the support of T, that

$$\tilde{T}_j(x) = \sum_i (jq_i)xb_i$$

with $q_i \in C$ and $q_0 = 1$. Since $a_0 \in J$, the result follows by taking $j = a_0$.

The right analog of the above also holds. If $T(x) = \sum_i a_ix^{\sigma_i}b_i$ is a trace form and $r, s \in R$, then $T(xr)s = \sum_i a_ix^{\sigma_i}(r^{\sigma_i}b_is)$ is clearly a trace form with the same a_i, σ_i. Thus we consider right truncations of T and we have

Lemma 3.2. *Let $T(x) = \sum_i a_ix^{\sigma_i}b_i$ be an outer trace form with $\sigma_0 = 1$, $b_0 \neq 0$. Then there exist $r_k, s_k \in R$ (depending only upon the b_i's and σ_i's) such that*

$$\tilde{T}(x) = \sum_k T(xr_k)s_k = \sum_i a_ix^{\sigma_i}\tilde{b}_i$$

satisfies $\tilde{b}_i \in R$, $\tilde{b}_0 \neq 0$. Furthermore, if $\tilde{b}_i \neq 0$ then $\sigma_i = 1$ and $\tilde{b}_i = c_ib_0$ for some $c_i \in C$ with $c_0 = 1$.

Proof. This actually follows directly from Lemma 3.1. Consider the outer trace from

$$T'(x) = \sum_i b_i^{\sigma_i^{-1}}x^{\sigma_i^{-1}}a_i.$$

Then by Lemma 3.1 there exist elements r_k, s_k depending only upon the b_i's and

σ_i's with

$$\sum_k r_k T'(s_k x) = \sum_i d_i x^{\sigma_i^{-1}} a_i$$

satisfying $d_i \in R$, $d_0 \neq 0$. Furthermore, if $d_i \neq 0$, then $\sigma_i^{-1} = 1$ and $d_i = c_i d_0$ for some $c_i \in C$. Notice that

$$d_i = \sum_k r_k b_i^{\sigma_i^{-1}} s_k^{\sigma_i^{-1}}.$$

Finally consider

$$\tilde{T}(x) = \sum_k T(xr_k)s_k = \sum_i a_i x^{\sigma_i} \tilde{b}_i.$$

Then

$$\tilde{b}_i = \sum_k r_k^{\sigma_i} b_i s_k = d_i^{\sigma_i}$$

so the result follows from the above properties of the d_i's.

Since elements of C are allowed to pass across x^σ in trace forms, we have immediately

Lemma 3.3. *Let $T(x) = \sum_i a_i x^{\sigma_i} b_i$ be an outer trace form with $\sigma_0 = 1$, $a_0 \neq 0$. Then there exists a left truncation $\tilde{T}(x) = \tilde{a}_0 x \beta$ of $T(x)$ with $\tilde{a}_0 \in R \setminus 0$ and $\beta = \sum' c_i b_i$. Here $c_i \in C$, $c_0 = 1$ and the sum is over $\{i \mid \sigma_i = 1\}$.*

Lemma 3.4. *Let $T(x) = \sum_i a_i x^{\sigma_i} b_i$ be an outer trace form with $\sigma_0 = 1$, $b_0 \neq 0$. Then there exists a right truncation $\tilde{T}(x) = \alpha x \tilde{b}_0$ of $T(x)$ with $\tilde{b}_0 \in R \setminus 0$ and $\alpha = \sum' a_i c_i$. Here $c_i \in C$, $c_0 = 1$ and the sum is over $\{i \mid \sigma_i = 1\}$.*

Finally we show that outer trace forms are nontrivial.

Lemma 3.5. *Let $T(x) = \sum_i a_i x^{\sigma_i} b_i$ be an outer trace form with $\sigma_0 = 1$ and let I be a nonzero ideal of R. Suppose that either $b_0 \neq 0$ and $\{a_i \mid \sigma_i = 1\}$ is C-linearly independent or $a_0 \neq 0$ and $\{b_i \mid \sigma_i = 1\}$ is C-linearly independent. Then $T(I) \neq 0$.*

Proof. If $T(I) = 0$, then certainly $\tilde{T}(I) = 0$ for any right or left truncation $\tilde{T}$ of T. In particular if $b_0 \neq 0$ and $\tilde{T} = \alpha x \tilde{b}_0$ is given as in Lemma 3.4, this yields $\alpha I \tilde{b}_0 = 0$. But $\tilde{b}_0 \neq 0$ so we must have $0 = \alpha = \sum' a_i c_i$ and these a_i's are C-linearly dependent since $c_0 = 1$. Similarly if $a_0 \neq 0$, the result follows from Lemma 3.3.

4. Properties of the fixed ring

We assume throughout that G is an M-group of automorphisms of R and that $B \subseteq Q$ is the algebra of the group. The results here are almost immediate applications of the existence and truncation properties of trace forms.

Proposition 4.1. $\mathbb{C}_Q(R^G)=B$.

Proof. Certainly $\mathbb{C}_Q(R^G)\supseteq B$ since B is spanned by elements which induce the X-inner automorphisms of G. We consider the reverse inclusion. Let $\beta\in\mathbb{C}_Q(R^G)$.

Let e be a primitive idempotent of B and let I and $\tau(x)=\sum a_{ig}x^g b_{ig}$ be as in Lemmas 2.4 and 2.5. Furthermore for $g=1$, we can assume that the C-basis $\{a_{i1}\}$ is chosen compatibly with the decomposition $B=eB\oplus(1-e)B$. Note that $\tau(I)\subseteq R^G$.

Since $\beta e\in\mathbb{C}_Q(R^G)$, if $T(x)$ is defined by

$$T(x)=\beta e\tau(x)-\tau(x)\beta e,$$

then T vanishes on I. Furthermore in the expression $\beta e\tau(x)$ we can delete all those a_{i1} in $(1-e)B$ and we use $\sum'$ to denote such a deleted sum. By Lemma 3.5 the left hand coefficients of

$$T(x)=\sum{}'\beta e a_{ig}x^g b_{ig}-\sum a_{ig}x^g b_{ig}\beta e$$

corresponding to $g=1$ are C-linearly dependent. Thus there exist $c_i,d_i\in C$, not all zero, with

$$\beta e\sum{}'c_i a_{i1}=\sum d_i a_{i1}.$$

Note that those a_{i1} in the left hand sum belong to eB and thus $\beta\alpha=\sum d_i a_{i1}$ where $\alpha=\sum' c_i a_{i1}$ is necessarily a nonzero element of eB. Since e is primitive and B is semisimple, $e\in\alpha B$ and we conclude immediately that $\beta e\in B$.

Finally if $1=e_1+\cdots+e_n$ is a decomposition of 1 into orthogonal primitive idempotents of B, then since $\beta e_i\in B$ for all i we have $\beta\in B$.

As a second application we have

Lemma 4.2. *Let q,q' be nonzero elements of Q, let $\sigma\in\operatorname{Aut}R$ and suppose that*

$$q'r=r^\sigma q\quad\text{for all } r\in R^G.$$

Then $\sigma\in g(\operatorname{Inn}R)$ for some $g\in G$.

Proof. Let I and $\tau(x)=\sum a_{ig}x^g b_{ig}$ be as in Lemmas 2.4 and 2.5 and assume that $a_{11}=1$. If $T(x)$ is defined by

$$T(x)=q'\tau(x)-\tau(x)^\sigma q=\sum q'a_{ig}x^g b_{ig}-\sum a_{ig}^\sigma x^{g\sigma}b_{ig}^\sigma q,$$

then T vanishes on I since $\tau(I)\subseteq R^G$.

If $\sigma\notin g^{-1}(\operatorname{Inn}R)$ for any g above, then the only X-inner automorphisms in $T(x)$ occur when $g=1$ and in the first sum. However $\{b_{i1}\}$ is C-linearly independent and $q'a_{11}=q'\neq 0$ so this contradicts Lemma 3.5. Thus $\sigma\in g^{-1}(\operatorname{Inn}R)$ for some $g\in G$.

If S is a subring of R, let

$$\mathscr{G}(R/S)=\{\sigma\in \operatorname{Aut} R \mid \sigma \text{ centralizes } S\}.$$

We can now quickly prove Theorem A.

Theorem 4.3. *Let G be an N-group. Then $\mathscr{G}(R/R^G)=G$.*

Proof. Certainly $\mathscr{G}(R/R^G)\supseteq G$. Conversely, if $\sigma\in\mathscr{G}(R/R^G)$, then $r^\sigma=r$ for all $r\in R^G$ so, by Lemma 4.2, we have $\sigma g^{-1}\in \operatorname{Inn} R$ for some $g\in G$. If σg^{-1} is the automorphism induced by $q\in Q$, then q clearly centralizes R^G and hence $q\in B$ by Proposition 4.1. Since G is an N-group, the inner automorphism induced by $q\in B$ is also contained in G and hence $\sigma\in G$.

We now consider certain ideals of R and R^G. Observe that G acts as automorphisms on B and hence G permutes the finitely many centrally primitive idempotents of B. If f is the sum of the idempotents in a G-orbit, then f is certainly a central idempotent and we say f is *G-centrally primitive.* Since B is semisimple, it is clear that fB is a G-simple ideal of B.

The following two results are a strengthened version of the fact that every nonzero ideal of R meets R^G nontrivially.

Lemma 4.4. *Let τ be any trace form given by Lemma 2.4 and let J be a nonzero ideal of R. Then for all $q\in Q\setminus 0$ we have $\tau(J)q\neq 0$ and $q\tau(J)\neq 0$. Thus if $\tau(J)\subseteq R$, then $\tau(J)$ is an essential two-sided ideal of R^G.*

Proof. By assumption, $\tau(x)=\sum a_{ig}x^g b_{ig}$ with both $\{a_{i1}\}$ and $\{b_{i1}\}$ bases of B. Thus for some i, $b_{i1}q\neq 0$ and it follows from Lemma 3.4 that the trace form $T(x)=\tau(x)q$ does not vanish on J. Similarly $q\tau(x)$ does not vanish on J. Finally since $a_{ig}, b_{ig}\in B$ and $g\in G$, it is clear that τ is an (R^G,R^G)-bimodule homomorphism. Thus $\tau(J)$ is an (R^G,R^G)-bimodule. In particular, if $\tau(J)\subseteq R$, then $\tau(J)$ is a two-sided ideal of R^G by Lemma 2.4. Furthermore it is essential, as a right or left ideal, since its left and right annihilators in R^G are zero.

Proposition 4.5. *Let I be a nonzero ideal of R.*

(i) *If $q\in Q\setminus 0$, then $(I\cap R^G)q\neq 0$ and $q(I\cap R^G)\neq 0$.*

(ii) *If f is a G-centrally primitive idempotent of B, then there exists $r\in I\cap R^G$ with $r=rf\neq 0$.*

(iii) *There exists $r\in I\cap R^G$ with $\operatorname{ann}_B(r)=0$.*

Proof. (i) By Lemmas 2.4 and 2.5 there is a trace form $\tau(x)=\sum a_{ig}x^g b_{ig}$ and a nonzero ideal $J\subseteq I$ with $\tau(J)\subseteq I\cap R^G$. Now apply Lemma 4.4.

(ii) By Lemma 1.2 there exists a nonzero ideal K of R with $Kf\subseteq R$ so $(IK)f\subseteq I$. Since $IK\neq 0$ we conclude from (i) above that for some $s\in IK\cap R^G$ we have

$r=sf\neq 0$. Observe that $r=rf\neq 0$ and that $r\in IKf\subseteq I$. Finally since both s and f are centralized by G, we see that $r=sf$ is also fixed by G.

(iii) Let $f_1, f_2, \dots, f_k$ be all the G-centrally primitive idempotents of B and, by (ii) above, we choose for each i an element $r_i\in I\cap R^G$ with $r_i=r_if_i\neq 0$. Note that for $i\neq j$, $r_if_j=r_if_if_j=0$. Thus if $r=\sum_1^k r_i$, then $r\in I\cap R^G$ and $rf_j=r_jf_j\neq 0$. But then $\mathrm{ann}_B(r)$ is a G-invariant two sided ideal of B containing no G-centrally primitive idempotent and this clearly implies that $\mathrm{ann}_B(r)=0$.

As was pointed out in Section 2, nontrivial trace forms exist under more general circumstances than B being semisimple. In particular, the following result, where B is merely assumed to be finite dimensional over C, is easily proved using Lemma 2.3 and the above arguments.

Lemma 4.6. *Suppose only that there exists a nontrivial B-module homomorphism* $\theta: B^*\to B$. *If I is any nonzero ideal of R, then* $I\cap R^G\neq 0$.

5. The bimodule property

We start by considering another important property of R^G, namely the bimodule property. This is stated formally in the following few results. Informally it asserts that if M is an (R,R^G)-subbimodule of Q, then $M\supseteq Ie$ for some nonzero ideal I of R and for e an idempotent of B which is as large as possible. Again G is assumed to be an M-group with B the algebra of the group.

Lemma 5.1. *Let M be an* (R,R^G)*-subbimodule of Q and let e be an idempotent of B with* $Me\neq 0$. *Then there exists* $b\in B$ *and a nonzero ideal J of R with* $Jb\subseteq M$ *and* $be\neq 0$.

Proof. Let I and the trace form $\tau(x)=\sum_{i,g} a_{ig}x^g b_{ig}$ be given by Lemmas 2.4 and 2.5. Furthermore assume that for $g=1$, the basis $\{a_{i1}\}$ is chosen compatibly with the decomposition $B=eB\oplus(1-e)B$ with $a_{11}=e$. Note that $e\neq 0$ since $Me\neq 0$. Then by Lemma 2.4 again, for $g=1$ the basis $\{b_{i1}\}$ is compatible with $B=Be\oplus B(1-e)$ and $b_{11}\in Be$.

By assumption there exists $m\in M$ with $0\neq me=ma_{11}$. We now consider $T(x)=m\tau(x)$. Since $\tau(I)\subseteq R^G$ and M is a right R^G-module, it follows that $T(I)\subseteq M$. Moreover, since M is a left R-module, we then see that any left truncation

$$\tilde{T}(x)=\sum_k r_k T(s_k x)$$

also satisfies $\tilde{T}(I)\subseteq M$. In particular, if $\tilde{T}$ is as given in Lemma 3.3, based on the 1, 1-coefficient $ma_{11}\neq 0$, then we have for some $a\in R$, $a\neq 0$

$$aI\beta=\tilde{T}(I)\subseteq M.$$

Here $\beta=\sum_i b_{i1}c_i\in B$ with $c_i\in C$, $c_1=1$. Note that $aI\neq 0$ since R is prime. Furthermore since $\{b_{i1}\}$ is compatible with the decomposition $B=Be\oplus B(1-e)$ and $b_{11}\in Be$, $c_1=1$ it is clear that $\beta e\neq 0$. Finally since $RM\subseteq M$ we have $(RaI)\beta\subseteq M$ and the result follows.

We now obtain the bimodule property.

Proposition 5.2. *Let M be an (R,R^G)-subbimodule of Q and let $\mathrm{r}_B(M)=(1-e)B$ for some idempotent e of B. Then there exists a nonzero ideal I of R with $M\supseteq Ie$.*

Proof. Since $\mathrm{r}_B(M)$ is a right ideal of B, it is generated by an idempotent which we write as $1-e$.

Now let K be the set of all elements $b\in B$ such that $Jb\subseteq M$ for some nonzero ideal J of R depending upon b. We claim that K is a left ideal of B. Indeed it is surely closed under addition. Furthermore let $b\in K$ with $Jb\subseteq M$ and let $b'\in B$. Then there exists a nonzero ideal J' of R with $J'b'\subseteq R$ and then $(JJ')(b'b)\subseteq Jb\subseteq M$, so $b'b\in K$. Observe that for any $b\in K$, $Jb\subseteq M$ implies that $Jb(1-e)=0$ and hence $b(1-e)=0$. Thus we conclude that $K\subseteq Be$ and the goal is to show that we have equality here.

To obtain the reverse inclusion, note that $K=Bf$ for some idempotent f. If $M(1-f)\neq 0$, then by Lemma 5.1 applied to the idempotent $1-f$, there exists $b\in K$ with $b(1-f)\neq 0$ and this is certainly a contradiction. Thus $1-f\in \mathrm{r}_B(M)=(1-e)B$, so $e(1-f)=0$. Hence $e=ef$ and $K=Bf\supseteq (Be)f=Be$. Since $e\in Be$, the proposition is proved.

The analogous result for (R^G,R)-bimodules holds with an almost identical proof. Indeed in the analog of Lemma 5.1 we merely use right truncation of the trace form $T(x)=\tau(x)m$ and then apply Lemma 3.4. For Proposition 5.3, K is of course defined as the set of $b\in B$ with $bJ\subseteq M$. Here to show that K is a right ideal of B we require the additional observation, from Lemma 1.2, that if $b'\in B$, then $b'J'\subseteq R$ for some nonzero ideal J' of R. We then have

Proposition 5.3. *Let M be an (R^G,R)-subbimodule of Q and let $l_B(M)=B(1-e)$ for some idempotent e of B. Then there exists a nonzero ideal I of R with $M\supseteq eI$.*

We will view the conclusions of the above two propositions as saying that R^G satisfies the *bimodule properties* with respect to B. Here of course $B=\mathbb{C}_Q(R^G)$ by Proposition 4.1.

Now let S be a subring of R with $S\supseteq R^G$. Then we recall that the Galois idempotent condition for S is given by

[GI] Let e be an idempotent of B with $eS(1-e)=0$. Then there exists an idempotent $f\in Z=\mathbb{C}_Q(S)$ with $Be=Bf$.

As we now see, this condition is intimately related to S satisfying the bimodule property with respect to $Z=\mathbb{C}_Q(S)$. First we have

Lemma 5.4. *Let H be an M-subgroup of G. Then $S=R^H$ satisfies* [GI].

Proof. Let $e\in B$ be an idempotent with $eR^H(1-e)=0$ and set $M=ReR^H$ so that M is an (R,R^H)-subbimodule of Q. By Proposition 5.2, R^H satisfies the bimodule condition with respect to $Z=\mathbb{C}_Q(R^H)$. Thus there exists an idempotent $f\in Z$ with $\mathrm{r}_Z(M)=(1-f)Z$ and $M\supseteq If$ for some nonzero ideal I of R. Now $M(1-f)=0$ and $e\in M$ implies that $e(1-f)=0$ so $e=ef$ and $Be\subseteq Bf$. On the other hand, $eR^H(1-e)=0$ implies that $If(1-e)\subseteq M(1-e)=0$. Thus $f(1-e)=0$ so $f=fe$ and $Bf\subseteq Be$.

The next two results show conversely that [GI] implies the bimodule property. Here we do not need to assume that Z is semisimple.

Lemma 5.5. *Let S be a subring of R containing R^G and suppose that S satisfies* [GI]. *If M is an (R,S)-subbimodule of Q, then there exists an idempotent $f\in Z=\mathbb{C}_Q(S)$ with $\mathrm{r}_Z(M)=(1-f)Z$. Furthermore for any such f, there exists a nonzero ideal I of R with $M\supseteq If$.*

Proof. Since $S\supseteq R^G$, M is also an (R,R^G)-bimodule. Thus by Proposition 5.2 there exists an idempotent $e\in B$ with $\mathrm{r}_B(M)=(1-e)B$ and $Ie\subseteq M$. But M is a right S-module and $M(1-e)=0$ so $IeS\subseteq M$ and $IeS(1-e)=0$. Thus $eS(1-e)=0$ and by condition [GI] there exists an idempotent $f\in Z$ with $Be=Bf$. Hence also $(1-e)B=(1-f)B$ and therefore

$$\mathrm{r}_Z(M)=\mathrm{r}_B(M)\cap Z=(1-f)B\cap Z=(1-f)Z.$$

Now let f' be any idempotent of Z with $\mathrm{r}_Z(M)=(1-f')Z$. Then $(1-f')Z=(1-f)Z$ so

$$(1-f')B=(1-f)B=(1-e)B=\mathrm{r}_B(M)$$

and by Proposition 5.2 applied to f' we have $Jf'\subseteq M$ for some nonzero ideal J of R.

The (S,R)-bimodule analog follows similarly. Indeed we merely apply [GI] with e replaced by $1-e$ and we denote the resulting idempotent in Z by $1-f$. We then obtain

Lemma 5.6. *Let S be a subring of R containing R^G and suppose that S satisfies* [GI]. *If M is an (S,R)-subbimodule of Q, then there exists an idempotent $f\in Z=\mathbb{C}_Q(S)$ with $l_Z(M)=Z(1-f)$. Furthermore for any such f there exists a nonzero ideal I of R with $M\supseteq fI$.*

Finally it is interesting to observe that [GI] implies a weakened version of semi-simplicity for Z.

Lemma 5.7. *Let S be a subring of R containing R^G and suppose that S satisfies [GI]. Then $Z = \mathbb{C}_Q(S)$ is a p.p.r. (that is, all principal ideals of Z are projective). Furthermore S is semiprime.*

Proof. Let $a \in Z$ and observe that $M = Ra$ is an (R, S)-subbimodule of Q. Thus by Lemma 5.5, $\mathrm{r}_Z(M) = (1-f)Z$ for some idempotent f of Z. Therefore $\mathrm{r}_Z(a) = (1-f)Z$ and we have $aZ \simeq Z/\mathrm{r}_Z(a) \simeq fZ$, so aZ is projective. Similarly using Lemma 5.6 we see that Za is projective.

Now let N be an ideal of S of square zero. Then NR is an (S, R)-bimodule so, by Lemma 5.6, $l_Z(NR) = Z(1-f)$ and $NR \supseteq fI$ for some nonzero ideal I of R. But $N^2 = 0$, so $NfI = 0$ and hence $Nf = 0$. Since $f \in Z$ commutes with N we obtain $(1-f)N = 0$ and $fN = 0$, so $N = 0$ and S is semiprime.

6. Bimodule truncation and homogeneity

It is again necessary to consider the truncation of trace forms. Let S be a subring of R and let

$$T(x) = \sum_i a_i x^{\sigma_i} b_i$$

be a trace form with $a_i, b_i \in Q$ and $\sigma_i \in \operatorname{Aut} R$. If $r_k \in R$, $s_k \in S$, then

$$\tilde{T}(x) = \sum_k T(x r_k) s_k$$

is called a (right) (R, S)-*truncation* of T. Notice that

$$\tilde{T}(x) = \sum_i a_i x^{\sigma_i} \tilde{b}_i \quad \text{with} \quad \tilde{b}_i = \sum_k r_k^{\sigma_i} b_i s_k.$$

For convenience we let the support of T be given by $\operatorname{Supp} T = \{ i \mid b_i \neq 0 \}$. Then clearly $\operatorname{Supp} \tilde{T} \subseteq \operatorname{Supp} T$.

In order to effect this truncation, we must be able to deal with certain identities satisfied by S. For example, if e is an idempotent of B then the condition [GI] enables us to handle identities of the form

$$es = ese \quad \text{for all } s \in S.$$

On the other hand, automorphisms are handled by the Galois homogeneity condition for S which is given by

[GH] Suppose $b \in B \setminus 0$, $g \in G$ and $bs = s^g b$ for all $s \in S$. Then $g = hg_0$ where h centralizes S and $g_0 \in G \cap \operatorname{Inn} R$.

Lemma 6.1. *Let H be an M-subgroup of G. Then $S=R^H$ satisfies* [GH].

Proof. Suppose b and g are as above and apply Lemma 4.2 with $q=q'=b$, $\sigma=g$ and $G=H$. Then by that lemma, $g=hw$ for some $h\in H$ and $w\in \operatorname{Inn} R$. But $g,h\in G$ so we conclude finally that $w\in G\cap \operatorname{Inn} R$.

We now proceed with the truncation. The hypothesis (i) below on the elements σ_i clearly replaces the outer hypothesis considered in Section 3.

Lemma 6.2. *Suppose that S is a subring of R containing R^G and satisfying* [GH] *and* [GI]. *We set $H=G\cap \mathscr{G}(R/S)$ and $Z=\mathbb{C}_B(S)$. Now let $T(x)=\sum_i a_i x^{\sigma_i} b_i$ be a trace form with $b_0\neq 0$, $\sigma_0=1$ and assume that for each i*

(i) $\sigma_i\in G$ and if $\sigma_i\in H(G\cap \operatorname{Inn} R)$, then $\sigma_i\in H$.

(ii) $b_i\in Qf_i$ for some primitive idempotent f_i of Z.

Then there exists a nonzero ideal J of R and a trace form $\bar{T}(x)=\sum_i a_i x^{\sigma_i} z_i$ such that $\bar{T}(xj)$ is an (R,S)-truncation of T for all $j\in J$. Furthermore $z_i\in Zf_i$, $z_0=f_0$ and if $z_i\neq 0$, then $\sigma_i\in H$. Finally if $j\in J$ and $jf_0\in J$, then $\bar{T}(xjf_0)=\bar{T}(xj)$.

Proof. We follow the right analog of the argument in Lemma 3.1. Again the a_i's merely play the role of place holders. Thus the ideal J and the elements $z_i\in Z$ will depend only on the b_i's and σ_i's. Note that $S\supseteq R^G$ satisfies [GI]. Thus by Lemmas 5.5 and 5.6, S satisfies the bimodule condition with respect to Z. We will freely use this fact throughout the remainder of the proof.

Suppose

$$\tilde{T}(x)=\sum T(xr_k)s_k=\sum_i a_i x^{\sigma_i}\tilde{b}_i$$

is any truncation of T. Then $\tilde{b}_i=\sum_k r_k^{\sigma_i} b_i s_k$. But $b_i\in Qf_i$ by (ii) and $f_i\in Z$ centralizes S so we conclude immediately that $\tilde{b}_i\in Qf_i$. In other words, hypothesis (ii) is inherited by all truncations of T.

For each i there exists a nonzero ideal L_i of R with $L_i b_i\subseteq R$. Thus, if $L=\bigcap_i L_i^{\sigma_i^{-1}}\neq 0$, then $L^{\sigma_i} b_i\subseteq R$ for all i. Furthermore $Lb_0\neq 0$. Thus, if $r\in L$ is chosen with $rb_0\neq 0$, then $T(xr)$ is a truncation $\tilde{T}$ of T with all $\tilde{b}_i\in R$ and $\tilde{b}_0\neq 0$. We can now assume that T has this property.

Let $\tilde{T}$ be an (R,S)-truncation of T of minimal support size subject to $\tilde{b}_0\neq 0$. We apply the bimodule condition to $M=R\tilde{b}_0 S\neq 0$. Since $\tilde{b}_0\in Qf_0$ we have $M(1-f_0)=0$. But f_0 is a primitive idempotent of Z, so $(1-f_0)Z$ is maximal among right ideals of Z generated by idempotents. Thus $\mathrm{r}_Z(M)=(1-f_0)Z$ and $M\supseteq Jf_0$ for some nonzero ideal J of R.

Suppose $T'(x)=\sum_i a_i x^{\sigma_i} b_i'$ is another truncation of T with $\operatorname{Supp} T'<\operatorname{Supp}\tilde{T}$. Then by definition we have $b_0'=0$. We claim that $b_i'=0$ for all i. To this end, assume by way of contradiction that some $b_n'\neq 0$. As above, we apply the bimodule condition to $M'=Rb_n'S$ and conclude that $M'\supseteq Kf_n$ for some nonzero ideal K of R. Observe that by Propostion 4.5(iii), there exists $t\in K\cap R^G\subseteq K\cap S$ with $\operatorname{ann}_B(t)=0$.

Since $tf_n \in M'$, we can now further truncate T' and assume that $b'_n = tf_n \neq 0$. Of course we still have $b'_0 = 0$.

Note that $f_0 t \neq 0$ implies that $Jf_0 t \neq 0$ and hence $Mt \neq 0$. Thus there exists $s \in S$ with $\tilde{b}_0 st \neq 0$. With this s, we consider

$$\begin{aligned} T''(x) &= \tilde{T}(x)st - T'(x(\tilde{b}_n s)^{\sigma_n^{-1}}) \\ &= \sum_i a_i x^{\sigma_i}(\tilde{b}_i st - (\tilde{b}_n s)^{\sigma_n^{-1}\sigma_i} b'_i) \\ &= \sum_i a_i x^{\sigma_i} b''_i. \end{aligned}$$

Since Supp $T' \subseteq$ Supp $\tilde{T}$ we have Supp $T'' \subseteq$ Supp $\tilde{T}$. Furthermore at $i = n$,

$$b''_n = \tilde{b}_n st - \tilde{b}_n s b'_n = \tilde{b}_n st - \tilde{b}_n st f_n = 0$$

since f_n commutes with st and $\tilde{b}_n \tilde{f}_n = \tilde{b}_n$. On the other hand, at $i = 0$, since $b'_0 = 0$ we have

$$b''_0 = \tilde{b}_0 st \neq 0$$

by the choice of s. But then Supp $T'' <$ Supp $\tilde{T}$, since $b''_n = 0$, and $b''_0 \neq 0$, so this contradicts the definition of $\tilde{T}$. We have therefore shown that if T' is any (R, S)-truncation of T with Supp $T' <$ Supp $\tilde{T}$, then Supp $T' = \emptyset$.

Recall that $M = R\tilde{b}_0 S \subseteq Jf_0$ for some nonzero ideal J of R. Thus for each $j \in J$ there exists a truncation $T'_j(x)$ of $\tilde{T}$ with

$$T'_j(x) = \sum_i a_i x^{\sigma_i} b'_i(j)$$

and $b'_0(j) = jf_0$. In fact T'_j is unique since if T'_j and T''_j are two truncations of $\tilde{T}$ with the same 0-coefficient jf_0, then $T'_j - T''_j$ is a truncation of T with smaller support than that of $\tilde{T}$. By the above, all right hand coefficients of $T'_j - T''_j$ must therefore be zero and hence $T'_j = T''_j$.

Thus for each i, $b'_i : J \to R$ is a well-defined function. It is surely additive but it is not a left R-module homomorphism. Indeed by comparing $T'_j(xr)$ and $T'_{rj}(x)$ we see that

$$b'_i(rj) = r^{\sigma_i} b'_i(j).$$

But then the composite map $(b'_i)^{\sigma_i^{-1}} : J \to R$ is an R-module homomorphism and hence represents an element $q_i \in Q$. Therefore for all $j \in J$ we have $(b'_i)^{\sigma_i^{-1}}(j) = jq_i$, so

$$b'_i(j) = j^{\sigma_i} q_i^{\sigma_i} = j^{\sigma_i} z_i$$

where we have set $z_i = q_i^{\sigma_i} \in Q$. Observe that $z_0 = f_0$ since $b'_0(j) = jf_0$ by assumption. Furthermore, if $\bar{T}(x)$ is defined by $\bar{T}(x) = \sum_i a_i x^{\sigma_i} z_i$, then for all $j \in J$

$$\bar{T}(xj) = \sum a_i x^{\sigma_i} j^{\sigma_i} z_i = T'_j(x)$$

is a truncation of T.

We note that, if $j\in J$ and $jf_0\in J$, then $T_j'(x)$ and $T_{jf_0}'(x)$ have the same 0-coefficient jf_0. Therefore these trace forms are identical and hence we have $\bar{T}(xjf_0)=\bar{T}(xj)$.

It remains to study $\bar{T}(x)$. Let $s\in S$. Then by comparing $T_j'(x)s$ and $T_{js}'(x)$, using $jf_0s=jsf_0$, we obtain

$$j^{\sigma_i}z_is=(js)^{\sigma_i}z_i=j^{\sigma_i}s^{\sigma_i}z_i.$$

Since this holds for all $j\in J$, we then have

$$z_is=s^{\sigma_i}z_i \quad \text{for all } s\in S.$$

Observe that $S\supseteq R^G$ and $\sigma_i\in G$ so we have $z_i\in \mathbb{C}_Q(R^G)=B$ by Proposition 4.1.

If $z_i=0$, then surely $z_i\in Zf_i$. Now suppose $z_i\neq 0$. Then since S satisfies the Galois homogeneity condition [GH] we conclude from the above identity that $\sigma_i\in H(G\cap \operatorname{Inn} R)$. Thus by hypothesis (i), this implies that $\sigma_i\in H$. Hence $s=s^{\sigma_i}$ and then $z_i\in \mathbb{C}_B(S)=Z$. Finally $J^{\sigma_i}z_i\subseteq Qf_i$ implies that $J^{\sigma_i}z_i(1-f_i)=0$, so $z_i(1-f_i)=0$ and we conclude that $z_i=z_if_i\in Zf_i$. This completes the proof.

7. Galois subrings

In this section, we obtain necessary and sufficient conditions for an intermediate ring to be a Galois subring. Again R is prime and G is an M-group of automorphisms with $G_0=G\cap \operatorname{Inn} R$. We start by constructing a convenient trace form.

Lemma 7.1. *Let $S\supseteq R^G$ and set $Z=\mathbb{C}_B(S)$ and $H=\{g\in G\mid g \text{ fixes } S\}=G\cap \mathcal{G}(R/S)$. If f is a primitive idempotent of Z, then there exists a trace form $\tau(x)=\sum_i a_ix^{g_i}b_i$, a nonzero ideal I of R and a transversal Λ for G_0 in G with the following properties.*

(i) $b_0=f$, $g_0=1$, $\tau(I)\subseteq R^G$.

(ii) *For all i, $g_i\in\Lambda$ and $b_i\in Qf_i$ for some primitive idempotent f_i of Z.*

(iii) *If $g_i\in HG_0$, then $g_i\in H$.*

(iv) *If $g\in\Lambda$, then $\{a_i\mid g_i=g\}$ is a C-basis for B.*

Proof. We can clearly choose a transversal Λ for G_0 in G with $1\in\Lambda$ and $\Lambda\cap G_0H\subseteq H$. For this Λ, let $\tau(x)=\sum_{i,g}a_{ig}x^gb_{ig}$ and I be given by Lemmas 2.4 and 2.5. Then certainly (iii) and (iv) are satisfied for this τ and we have $\tau(I)\subseteq R^G$. It remains to suitably modify the elements b_{ig}.

Let $f_1+f_2+\cdots+f_k=1$ be a decomposition of 1 into orthogonal primitive idempotents of Z with $f_1=f$ and let $\{d_1,d_2,\ldots,d_n\}$ be a C-basis for B compatible with $B=Bf_1\oplus Bf_2\oplus\cdots\oplus Bf_k$. Furthermore assume that $d_1=f_1=f$. Thus each $d_i\in Qf_{i'}$ for some $i'\in\{1,2,\ldots,k\}$. Now fix $g\in\Lambda$. Since $\{b_{ig}\mid i\}$ is a C-basis for B, we can write $b_{ig}=\sum_j c_{ij}d_j$ with the C-matrix $[c_{ij}]$ nonsingular. Since C is central in Q, we observe that for any $x \in Q$

$$\sum_i a_{ig} x^g b_{ig} = \sum_i a_{ig} x^g \Big(\sum_j c_{ij} d_j \Big)$$

$$= \sum_j \Big(\sum_i a_{ig} c_{ij} \Big) x^g d_j = \sum_j a'_{jg} x^g d_j$$

where $a'_{jg} = \sum_i a_{ig} c_{ij}$. But $[c_{ij}]$ is nonsingular so $\{a'_{jg} \mid j\}$ is also a C-basis for B.

Finally by making this basis change for each $g \in \Lambda$, we obtain a trace form $\tau'(x) = \sum_{j,g} a'_{jg} x^g d_j$ with all the necessary properties. The result follows by relabeling the index of summation.

We now come to a key ingredient in characterizing Galois subrings.

Lemma 7.2. *Let G be an N-group of automorphisms of the prime ring R and let $R \supseteq S \supseteq R^G$ with S satisfying* [GI] *and* [GH]. *Assume in addition that $Z = \mathbb{C}_B(S)$ is spanned by units and set $H = \mathcal{G}(R/S)$. Then Z is the algebra of the group of H. Furthermore S has an ideal K which is a right ideal of R^H with $l_Q(K) = \mathrm{r}_Q(K) = 0$ and with KR and RK containing nonzero ideals of R.*

Proof. Clearly $R^H \supseteq S$ and, in view of Theorem 4.3, $H \subseteq G$.

Let f be a primitive idempotent of $Z = \mathbb{C}_B(S)$. We first show that there exists a right ideal $\bar{K}$ of R^H with $\bar{K} \subseteq S$ and $\bar{K}f \neq 0$. To this end, let $\tau(x)$ and I be given by the preceding lemma. Since S satisfies [GI] and [GH] we can apply Lemma 6.2 to this trace form. Thus there exists

$$\bar{T}(x) = \sum_i a_i x^{g_i} z_i$$

as described in that lemma and a nonzero ideal J of R such that, for each $j \in J$, $\bar{T}(xj)$ is an (R, S)-truncation of τ. Set $\bar{K} = \bar{T}(IJ)$.

For each $j \in J$ we have $\bar{T}(xj) = \sum_k \tau(xr_k)s_k$ for some $r_k \in R$, $s_k \in S$. Thus since $\tau(I) \subseteq R^G \subseteq S$, it follows that $\bar{T}(Ij) \subseteq S$ and hence that $\bar{K} = \bar{T}(IJ) \subseteq S$. By assumption, Z is spanned by units and each such unit gives rise via conjugation to an element of G which centralizes S. Thus conjugation by each such unit is an element of H, so Z is clearly the algebra of the group of H and therefore Z centralizes R^H. Furthermore, by Lemma 6.2, each $z_i \in Z$ and if $z_i \neq 0$, then $g_i \in H$. We conclude from this that $\bar{T}: IJ \to S$ is a right R^H-module homomorphism and therefore that $\bar{K}$ is a right ideal of R^H. Furthermore observe that $\bar{K}f = \bar{T}(IJ)f$ and that $\bar{T}(x)f = \sum a_i x^{g_i} z_i f$. Since $z_0 f = f \neq 0$, it follows immediately from the properties of τ and Lemma 3.5 that $\bar{K}f = \bar{T}(IJ)f \neq 0$.

We can now quickly prove the result. Let K be the sum of all right ideals of R^H contained in S. Then K is certainly a right ideal of R^H contained in S and K is a 2-sided ideal of S since SK also has this property. Let $M = RK$ so that M is an (R, S)-bimodule contained in Q and $\mathrm{r}_Q(M) = \mathrm{r}_Q(K)$. Since $\mathrm{r}_Z(K)$ contains no primitive idempotents of Z by the above, we conclude from Lemma 5.5 that $\mathrm{r}_Z(M) = 0$ and that M contains a nonzero ideal of R. Thus $\mathrm{r}_Q(K)=\mathrm{r}_Q(M)=0$. Since $l_Z(K)=\mathrm{r}_Z(K)=0$, a similar argument applies to KR and the lemma is proved.

We remark that since Z is a finite-dimensional C-algebra, it is almost always spanned by its units. The only exceptions occur when $C=\mathrm{GF}(2)$ and Z has a homomorphic image isomorphic to $\mathrm{GF}(2)\oplus\mathrm{GF}(2)$. The Galois centralizer condition for $S\subseteq R$ asserts

[GZ] If $Z=\mathbb{C}_B(S)$, then Z is a semisimple algebra spanned by its units.

With this we can strengthen the preceding lemma and obtain

Proposition 7.3. *Let G be an N-group of automorphisms of the prime ring R and let $S\supseteq R^G$ satisfy* [GZ], [GI] *and* [GH]. *Then $H=\mathscr{G}(R/S)$ is an N-subgroup of G with algebra of the group $Z=\mathbb{C}_B(S)$. Furthermore S contains a two-sided ideal K of R^H with $\mathrm{r}_Q(K)=l_Q(K)=0$.*

Proof. By Theorem 4.3 we have $H\subseteq\mathscr{G}(R/R^G)=G$ and hence $[H:H\cap\operatorname{Inn}R]<\infty$. Furthermore, by the previous lemma, Z is the algebra of the group H. Hence by [GZ], Z is semisimple and H is an N-subgroup of G.

In addition, by Lemma 7.2, S contains a right ideal K of R^H such that $KR\supseteq J$ a nonzero ideal of R. Now let τ be a trace form given by Lemma 2.4 for the N-group H and let I be the ideal, given by Lemma 2.5, with $\tau(I)\subseteq R^H$. From $J\subseteq KR$ we have $JI\subseteq KI$ and hence $\tau(JI)\subseteq\tau(KI)$. But τ is an (R^H,R^H)-bimodule homomorphism and K is a right ideal of R^H so

$$\tau(JI)\subseteq K\cdot\tau(I)\subseteq K\cdot R^H\subseteq S.$$

Finally, by Lemma 4.4, $\tau(JI)$ is a two-sided ideal of R^H with zero annihilator in Q.

It is now a simple matter to prove Theorem B. Let us recall the remaining Galois subring condition for $S\subseteq R$, namely the cancellation property.

[GC] Suppose K is an ideal of S with $\mathrm{r}_R(K)=0$. If $r\in R$ with $Kr\subseteq S$, then $r\in S$.

Theorem 7.4. *Let G be an N-group of automorphisms of the prime ring R and let $R\subseteq S\subseteq R^G$. Then S is the fixed ring of an N-subgroup H of G if and only if S satisfies* [GZ], [GI], [GH] *and* [GC].

Proof. Suppose first that $S=R^H$ for some N-subgroup H of G. Then $Z=\mathbb{C}_B(S)$ is the algebra of the group of H, by Proposition 4.1, and therefore [GZ] holds. Furthermore Lemmas 5.4 and 6.1 imply that S satisfies [GI] and [GH] respectively. Finally let K be an ideal of S with $\mathrm{r}_R(K)=0$ and suppose $Kr\subseteq S$. If $h\in H$ and $k\in K$, then

$$kr = (kr)^h = k^h r^h = kr^h$$

so $r - r^h \in \mathrm{r}_R(K) = 0$. We conclude therefore that $r \in R^H = S$ and S satisfies [GC].

Conversely suppose $S \supseteq R^G$ satisfies the four Galois conditions and let $H = \mathscr{G}(R/S)$. Then by the preceding proposition, H is an N-subgroup of G and S contains a two-sided ideal K of R^H with $\mathrm{r}_R(K) = 0$. In particular, if $r \in R^H$, then $Kr \subseteq K \subseteq S$, so [GC] implies that $r \in S$. We conclude therefore that $S = R^H$ and the theorem is proved.

Since the properties of the ideal K of Proposition 7.3 are right-left symmetric, it is clear that [GC] could be replaced in the above by either of the following conditions.

[GC$_1$] Suppose K is an ideal of S with $l_R(K) = 0$. If $r \in R$ with $rK \subseteq S$, then $r \in S$.

[GC$_2$] Suppose K is an ideal of S with $\mathrm{r}_R(K) = l_R(K) = 0$. If $r \in R$ with $rK \subseteq S$ and $Kr \subseteq S$, then $r \in S$.

8. Correspondence theorems

As an immediate consequence of Theorems 4.3 and 7.4 we obtain the main correspondence theorem.

Corollary 8.1. *Let G be an N-group of automorphisms of the prime ring R. Then the maps $H \to R^H$ and $S \to \mathscr{G}(R/S)$ yields a one-to-one correspondence between the N-subgroups H of G and the intermediate rings $S \supseteq R^G$ which satisfy* [GZ], [GI], [GH] *and* [GC].

While the above does indeed characterize Galois subrings, the verification of the four Galois conditions is frequently tedious. However in certain special situations many of these conditions are automatically satisfied. We consider some of these now and continue to formulate the results as correspondence theorems.

We start with the X-inner case. Here [GH] is clearly always satisfied so we have

Corollary 8.2. *Let G be an N-group of automorphisms of the prime ring R and suppose that G is X-inner. Then the maps $H \to R^H$ and $S \to \mathscr{G}(R/S)$ yield a one-to-one correspondence between the N-subgroups H of G and the intermediate rings $S \supseteq R^G$ which satisfy* [GZ], [GI], *and* [GC].

Next suppose that B, the algebra of the group, is a domain. Then since B is a finite-dimensional C-algebra, it is a division ring. In particular, [GZ] and [GI] are now immediate. Furthermore suppose $b \in B \setminus 0$, $g \in G$ and $bs = s^g b$ for all $s \in S$. Then b is a unit of B so conjugation by b is an element $g_0 \in G \cap \operatorname{Inn} R$. Thus for all $s \in S$

$$s = b^{-1} s^g b = s^{gg_0},$$

so $gg_0 = h \in \mathcal{G}(R/S)$ and [GH] holds. In particular, this applies to the X-outer case where we have

Corollary 8.3. *Let G be a finite group of X-outer automorphisms of the prime ring R. Then the maps $H \to R^H$ and $S \to \mathcal{G}(R/S)$ yield a one-to-one correspondence between the subgroups H of G and the intermediate rings $S \supseteq R^G$ satisfying* [GC].

A subring $S \subseteq R$ is said to be an *anti-ideal* if $sr \in S$ for $s \in S \setminus 0$, $r \in R$ implies that $r \in S$.

Corollary 8.4. *Let R be a domain and let G be an N-group of automorphisms. Then the maps $H \to R^H$ and $S \to \mathcal{G}(R/S)$ yield a one-to-one correspondence between the N-subgroups H of G and the anti-ideals $S \supseteq R^G$ of R. Moreover B is a division ring.*

Proof. We first observe that B is a domain. Indeed suppose $a, b \in B \setminus 0$. Then by Lemma 1.2 there exist nonzero ideals I, J of R with $0 \neq Ia \subseteq R$ and $0 \neq bJ \subseteq R$. But R is a domain, so $(Ia)(bJ) \neq 0$ and hence $ab \neq 0$. Thus B is in fact a division ring.

Now suppose $S \supseteq R^G$ is an anti-ideal of R. Then certainly S satisfies [GC] and thus, by Theorem 7.4, we have $S = R^H$ for $H = \mathcal{G}(R/S)$. Conversely suppose $S = R^H$ and that $sr \in S$ with $s \in S \setminus 0$, $r \in R$. If $h \in H$, then

$$sr = (sr)^h = s^h r^h = sr^h$$

and since R is a domain we have $r = r^h$. Thus $r \in R^H = S$ and S is an anti-ideal.

There is in fact a more general class of intermediate subrings which automatically satisfy [GH], namely those rings with Z simple. For this and later applications, we require the following two lemmas.

Lemma 8.5. *Let A_1, A_2 be simple Artinian rings and let V be a nonzero (A_1, A_2)-bimodule. Then there exists $v \in V$ with $l_{A_1}(v) = 0$ or $\mathrm{r}_{A_2}(v) = 0$.*

Proof. Let U be the unique simple left A_1-module and suppose that the regular module ${}_{A_1}A_1$ is a direct sum of n copies of U. Now ${}_{A_1}V$ is a direct sum of copies of U and suppose first that at least n such copies occur. Then ${}_{A_1}V$ contains a copy of ${}_{A_1}A_1$ and if v generates this submodule, then $l_{A_1}(v) = 0$. On the other hand, suppose ${}_{A_1}V$ is a direct sum of less than n copies of U. Then ${}_{A_1}V$ is a homomorphic image of ${}_{A_1}A_1$ and is therefore a cyclic A_1-module. In this case, $V = A_1 v$ for some $v \in V$. Thus clearly $\mathrm{r}_{A_2}(v) = \mathrm{r}_{A_2}(V)$ is a two-sided ideal of the simple ring A_2 and since $V \neq 0$ we have $\mathrm{r}_{A_2}(v) = 0$.

Observe that in the above, the hypothesis on A_2 can be replaced by V_{A_2} being faithful.

Lemma 8.6. *Let S_1, S_2 be subrings of R containing R^G and let $b \in B$ with $S_1 b = bS_2$.*

(i) *Let S_1 satisfy* [GI] *and let e_1 be an idempotent of $Z_1 = \mathbb{C}_B(S_1)$ with $b = e_1 b$. If $l_{Z_1 e_1}(b)$ contains no nonzero idempotents, then $l_Q(b) = l_Q(e_1)$.*

(ii) *Let S_2 satisfy* [GI] *and let e_2 be an idempotent of $Z_2 = \mathbb{C}_B(S_2)$ with $b = be_2$. If $\mathrm{r}_{e_2 Z_2}(b)$ contains no nonzero idempotents, then $\mathrm{r}_Q(b) = \mathrm{r}_Q(e_2)$.*

Proof. We consider (i). First observe that $b = e_1 b$ yields $l_Q(e_1) \subseteq l_Q(b)$ and hence $Z_1(1 - e_1) \subseteq l_{Z_1}(b)$. Now let $M = S_1 bR = bS_2 R = bR$. Then M is an (S_1, R)-bimodule contained in Q and

$$l_{Z_1}(M) = l_{Z_1}(b) = Z_1(1 - e_1) \oplus l_{Z_1 e_1}(b).$$

Since $S_1 \supseteq R^G$ satisfies [GI], we conclude from Lemma 5.6 that $l_{Z_1}(M)$ is generated by an idempotent. Thus the hypothesis on $l_{Z_1 e_1}(b)$ yields $l_{Z_1 e_1}(b) = 0$ and $l_{Z_1}(M) = Z_1(1 - e_1)$. Lemma 5.6 now implies that $M \supseteq e_1 I_1$ for some nonzero ideal I_1 of R. Since $l_Q(b)M = 0$ we conclude therefore that $l_Q(b)e_1 = 0$ and we obtain the reverse inclusion $l_Q(b) \subseteq l_Q(e_1)$. Part (ii) follows similarly.

It is now convenient to introduce a strengthened Galois centralizer condition, namely

[GZ′] If $Z = \mathbb{C}_B(S)$, then Z is a simple algebra, hence spanned by its units.

Lemma 8.7. *Let G be an N-group of automorphisms of the prime ring R and let $S \supseteq R^G$ satisfy* [GZ′] *and* [GI]. *Then S satisfies* [GH].

Proof. Let $g \in G$, set $V = \{v \in B \mid vs = s^g v \text{ for all } s \in S\}$ and assume that $V \neq 0$. Then V is surely a (Z^g, Z)-bimodule and hence, since both Z and Z^g are simple by assumption, Lemma 8.5 applies. In particular there exists $b \in V$ with either $l_{Z^g}(b) = 0$ or $\mathrm{r}_Z(b) = 0$. Furthermore $bS = S^g b$ and both S and S^g satisfy [GI]. Hence, by Lemma 8.6, with $e_1 = e_2 = 1$ we conclude that either $l_Q(b) = l_Q(e_1) = 0$ or $\mathrm{r}_Q(b) = \mathrm{r}_Q(e_2) = 0$. But B is a finite-dimensional C-algebra so either conclusion implies that b is a unit of B. Now G is an N-group, so conjugation by $b \in B$ is an element $g_0 \in G \cap \mathrm{Inn}\, R$. Thus for all $s \in S$

$$s = b^{-1} s^g b = s^{g g_0},$$

so $g g_0 = h \in \mathscr{G}(R/S)$ and [GH] holds.

We say that G is an *F-group* of automorphisms of R if G is an N-group whose algebra of the group B is simple. We can now obtain another correspondence theorem of interest.

Corollary 8.8. *Let G be an N-group of automorphisms of the prime ring R. Then the maps $H \to R^H$ and $S \to \mathscr{G}(R/S)$ yield a one-to-one correspondence between the F-subgroups H of G and the intermediate rings $S \supseteq R^G$ which satisfy* [GZ'], [GI] *and* [GC].

Proof. Let H be an F-subgroup of G and set $S = R^H$. Since $Z = \mathbb{C}_B(S)$ is the algebra of the group H by Proposition 4.1, it follows from Corollary 8.1 that S satisfies [GZ'], [GI] and [GC]. Conversely if $S \supseteq R^G$ satisfies these conditions, then it also satisfies [GH] by Lemma 8.7. Hence by Corollary 8.1 again, $S = R^H$ with $H = \mathscr{G}(R/S)$ an N-subgroup of G. Since the algebra of the group H is the simple ring Z, we conclude that H is an F-subgroup of G.

Finally we consider a rather special situation.

Lemma 8.9. *Let G be a finite group of X-outer automorphisms of the simple ring R and let $\tau_G(x) = \sum_{g \in G} x^g$. Then R^G is simple if and only if $1 \in \tau_G(R)$.*

Proof. Observe that $\tau = \tau_G$ is an (R^G, R^G)-bimodule homomorphism and hence $\tau(R)$ is an ideal of R^G. Thus $1 \in \tau(R)$ if and only if $\tau(R) = R^G$. Now suppose R^G is simple. Since $\tau(R) \neq 0$, by Lemma 3.5, we have $\tau(R) = R^G$. Conversely suppose $\tau(R) = R^G$ and let K be a nonzero ideal of R^G. Then KR is a nonzero (R^G, R)-bimodule contained in R and hence, since $B = C$, it follows from Lemma 5.6 that KR contains a nonzero ideal of R. But R is simple, so $KR = R$ and hence $R^G = \tau(R) = \tau(KR) = K\tau(R) \subseteq K$. Thus R^G is simple.

Corollary 8.10. *Let G be a finite group of X-outer automorphisms of the simple ring R and let $\tau_G(x) = \sum_{g \in G} x^g$. If $1 \in \tau_G(R)$, then the maps $H \to R^H$ and $S \to \mathscr{G}(R/S)$ yield a one-to-one correspondence between the subgroups H of G and the intermediate rings $S \supseteq R^G$. Furthermore, each such S is simple.*

Proof. Let H be a subgroup of G and let Ω be a left transversal for H in G. Then clearly

$$\tau_G(x) = \sum_{h \in H} \sum_{w \in \Omega} x^{wh} = \tau_H\left(\sum_{w \in \Omega} x^w \right).$$

Thus since $1 \in \tau_G(R)$ we have $1 \in \tau_H(R)$ and hence, by the previous lemma, R^H is simple.

Now let $S \supseteq R^G$ be any intermediate ring and set $H = \mathscr{G}(R/S)$. Since G is X-outer, we know that S satisfies [GZ], [GI] and [GH]. Thus, by Proposition 7.3, S contains a nonzero ideal of R^H. But R^H is simple, by the above, so we conclude that $S = R^H$. In view of Corollary 8.3, this completes the proof.

Observe that the hypothesis $1 \in \tau_G(R)$ is trivially satisfied if $|G|^{-1} \in R$.

9. Prime ideals of the fixed ring

There are numerous applications of these methods to the study of the relationship between R and the fixed ring R^G. We just discuss a few and we start with a rather amazing observation. Again R is a prime ring and G is an M-group of automorphisms.

Proposition 9.1. *Let K be the set of elements $r\in R$ such that rR is contained in a finitely generated right R^G-submodule of R and Rr is contained in a finitely generated left R^G-submodule of R. Then K is a nonzero two-sided ideal of R.*

Proof. For each $b\in B$, define

$$L_b=\left\{r\in R \,\middle|\, rRb\subseteq \sum_{i=1}^{n} r_iR^G \text{ for some } n \text{ and } r_i\in R\right\}.$$

If $rRb\subseteq \sum_1^n r_iR^G$ and $s\in R$, then $srRb\subseteq \sum_1^n sr_iR^G$. It now follows easily that L_b is a 2-sided ideal of R. The goal is to show that $L_1\neq 0$. To this end, define

$$W=\{b\in B \mid L_b\neq 0\}.$$

Then $0\in W$ and W is closed under addition since clearly $L_a\cap L_b\subseteq L_{a+b}$ for $a,b\in B$. Furthermore suppose $b\in W$, $a\in B$ and let $0\neq J$ be an ideal of R with $Ja\subseteq R$. If $r\in L_b$ then, since $rJab\subseteq rRb$, it follows that $rJ\subseteq L_{ab}$. Thus $L_{ab}\supseteq L_bJ\neq 0$, so $ab\in W$ and W is a left ideal of B. In particular, it is a C-subspace and we wish to show that $W=B$.

Suppose by way of contradiction that $W\neq B$. Let τ and I be given by Lemmas 2.4 and 2.5. Furthermore, assume that the basis $\{b_{i1}\}$ is chosen compatibly with $B=W'\oplus W$ where W' is any complementary C-subspace and with $b_{11}\in W'$. Then $a_{11}\neq 0$ and we left truncate τ based on the 1,1-coefficient. By Lemmas 3.1 and 3.3, there exist $r_k, s_k\in R$ such that

$$\tilde{a}_{11}x\beta=\sum_k r_k\tau(s_kx)$$

for some $\tilde{a}_{11}\in R\setminus 0$ and some $\beta=\sum c_ib_{i1}$ with $c_i\in C$, $c_1=1$. But $\tau(I)\subseteq R^G$ so this implies that

$$\tilde{a}_{11}I\beta\subseteq \sum_k r_kR^G.$$

Hence $0\neq \tilde{a}_{11}I\subseteq L_\beta$, by definition, and therefore $\beta\in W$. However, since $c_1=1$, β involves b_{11} and this contradicts the choice of basis.

We have therefore shown that $W=B$ so $1\in W$ and $L=L_1\neq 0$. Similarly using Lemmas 3.2 and 3.4 we can show that

$$L'=\left\{r\in R \,\middle|\, Rr\subseteq \sum_{i=1}^{n} R^Gr_i \text{ for some } n \text{ and } r_i\in R\right\}$$

is also a nonzero 2-sided ideal of R. Since $K=L\cap L'$, the result follows.

For each G-centrally primitive idempotent f of B let $P_f = \mathrm{ann}_{R^G}(f)$. Clearly each P_f is an ideal of R^G.

Lemma 9.2. *With the above notation we have*

(i) $\mathrm{ann}_B(P_f) = Bf$.

(ii) *If L is an ideal of R^G properly containing P_f, then* $\mathrm{ann}_B(L) = 0$ *and hence both LR and RL contain nonzero two-sided ideals of R.*

(iii) *P_f is a prime ideal of R^G and* $\mathrm{ann}_{R^G}(P_f) \neq 0$.

Proof. Observe that if L is a subset of R^G, then $\mathrm{ann}_B(L)$ is a G-invariant two-sided ideal of B.

(i) By definition, $\mathrm{ann}_B(P_f) \supseteq Bf$.Now let f' be any other G-centrally primitive idempotent of B. By Proposition 4.5(ii), with $I = R$, there exists $r \in R^G$ with $r = rf' \neq 0$. Since $f'f = 0$ we have $rf = rf'f = 0$ and $r \in P_f$. On the other hand $rf' \neq 0$ so $f' \notin \mathrm{ann}_B(P_f)$. Since B is semisimple and $\mathrm{ann}_B(P_f)$ is a G-invariant 2-sided ideal, this clearly implies that $\mathrm{ann}_B(P_f) = Bf$.

(ii) Let $L > P_f$. Then $\mathrm{ann}_B(L) \subseteq \mathrm{ann}_B(P_f) = Bf$ by the above. If $\mathrm{ann}_B(L) = Bf$, then $L \subseteq \mathrm{ann}_{R^G}(f) = P_f$, a contradiction. Thus since Bf is G-simple, we have $\mathrm{ann}_B(L) = 0$. It now follows that the (R^G, R)-bimodule LR satisfies $l_B(LR) = 0$, so LR contains a nonzero ideal of R by Proposition 5.3. Similarly, by Proposition 5.2, RL contains a nonzero ideal of R.

(iii) Suppose L_1 *and* L_2 are ideals of R^G containing P_f. If $L_1 L_2 \subseteq P_f$, then $0 = L_1 L_2 f = L_1 f L_2$ and thus $(RL_1)f(L_2R) = 0$. It follows that RL_1 and L_2R cannot both contain nonzero ideals of R. Thus by (ii) above either $L_1 = P_f$ or $L_2 = P_f$ and P_f is prime. Finally by Proposition 4.5(ii) again, with $I = R$, there exists $r \in R^G$ with $r = rf \neq 0$. Since $rP_f = rfP_f = 0$ and $P_f r = P_f fr = 0$, we conclude that $r \in \mathrm{ann}_{R^G}(P_f)$.

As an immediate consequnce we have

Proposition 9.3. *R^G is semiprime and the number of minimal primes of this ring is precisely equal to the number of G-centrally primitive idempotents of B. Indeed the minimal primes of R^G are precisely the ideals P_f. Furthermore the latter are all distinct and $\bigcap_f P_f = 0$.*

Proof. We have already observed above that the ideals P_f are prime. Furthermore since $1 \in B$ is a sum of G-centrally primitive idempotents of B, we conclude that $\bigcap_f P_f = 0$. This implies that R^G is semiprime and that its minimal primes are precisely the minimal members of the set $\{P_f\}$. But by Lemma 9.2(i), if $P_f \subseteq P_{f'}$, then $Bf' = \mathrm{ann}_B(P_{f'}) \subseteq \mathrm{ann}_B(P_f) = Bf$ and hence $f' = f$. Thus the primes P_f are incomparable and hence they are all minimal.

Now we consider the possibility that R is a primitive ring.

Proposition 9.4. *Let f be a G-centrally primitive idempotent of B. Then R is (right or left) primitive if and only if R^G/P_f is (right or left) primitive.*

Proof. The argument is symmetric, so we will consider only right modules.

Suppose first that R is primitive and let V be a faithful irreducible right R-module. Let K be the ideal defined by Proposition 9.1 and choose $r \in K$, $r \neq 0$. Then by assumption, $rR \subseteq \sum_1^k r_i R^G$. If $v \in V$ is chosen with $vr \neq 0$, then since V is irreducible we have

$$V = (vr)R \subseteq \sum_{i=1}^{k} (vr_i)R^G$$

and we deduce that V is a finitely generated R^G-module.

Now note that $VP_f \neq V$ since $\mathrm{r}_{R^G}(P_f) \neq 0$ by Lemma 9.2(iii) and V is faithful. Thus since V is a finitely generated R^G-module, we can choose W to be a maximal R^G-submodule of V containing VP_f. We have now found an irreducible R^G-module, namely V/W, which is annihilated by P_f. Finally let $L = \mathrm{r}_{R^G}(V/W)$ so that L is a 2-sided ideal of R^G containing P_f. Since $VL \subseteq W$ we have $V(RL) \subseteq W$ and hence RL cannot contain a nonzero ideal of R. We conclude therefore from Lemma 9.2(ii) that $L = P_f$ and hence that R^G/P_f is a primitive ring.

In the other direction, let W be a faithful irreducible module for R^G/P_f. Then there exists a maximal right ideal M of R^G with $R^G/M \simeq W$. Hence P_f is the largest 2-sided ideal of R^G contained in M. We first show that $MR \neq R$. To this end, suppose $R = MR$ and let $\tau(x)$ and I be given by Lemmas 2.4 and 2.5. Then

$$I = RI = MRI = MI$$

and since τ is an (R^G, R^G)-bimodule homomorphism we have

$$\tau(I) = \tau(MI) = M\tau(I) \subseteq MR^G \subseteq M.$$

Thus $\tau(I)$ is a 2-sided ideal of R^G contained in M, so $\tau(I) \subseteq P_f$ and $\tau(I)f = 0$. Since this contradicts Lemma 4.4 we therefore have $R > MR$.

We can now choose N to be a maximal right ideal of R containing MR. Then $V = R/N$ is an irreducible right R-module and, since $N \cap R^G = M$ by the maximality of M, we see that V contains the R^G-submodule $(R^G + N)/N \simeq R^G/M \simeq W$. Thus if $J = \mathrm{r}_R(V)$, then $J \cap R^G \subseteq \mathrm{r}_{R^G}(W) = P_f$ and hence $(J \cap R^G)f = 0$. We conclude from Proposition 4.5(i) that $J = 0$ and therefore that V is a faithful irreducible R-module. In other words, R is a primitive ring.

It follows from the above that if P_f is a primitive ideal of R^G then so is $P_{f'}$ for all f'. As a corollary we obtain

Proposition 9.5. *If R is simple, then R^G is a finite direct sum of primitive rings.*

Proof. Since R is simple, $Q = R$ and hence $B \subseteq R$. In particular, if $f_1, f_2, \ldots, f_n$ are the G-centrally primitive idempotents of B, then $f_i \in R^G$ and hence $R^G = \bigoplus_k f_k R^G$.

Furthermore from this decomposition it is clear that

$$P_{f_i} = \operatorname{ann}_{R^G}(f_i) = \bigoplus_{k \neq i} f_k R^G,$$

so $f_i R^G \simeq R^G / P_{f_i}$. But R is surely primitive so each P_{f_i} is a primitive ideal by the preceding result and hence each $f_i R^G$ is primitive.

It is known that these primitive summands need not be simple [16, Example 2.8]. We close with a result needed in Section 12. It is actually true without the assumption that R^G is prime, using a more general definition of the Martindale ring of quotients $Q_0(R)$ which is applicable to semiprime rings.

Proposition 9.6. *Let G be an M-group of automorphisms of the prime ring R. If R^G is prime, then $Q_0(R^G) = Q_0(R)^G$.*

Proof. Observe that G extends uniquely to a group of automorphisms of $Q_0(R)$ so the fixed ring $Q_0(R)^G$ makes sense and is an extension of the prime ring R^G.

Let $q \in Q_0(R)^G$ and let I be a nonzero ideal of R with $Iq \subseteq R$. By Proposition 4.5(i), $I \cap R^G \neq 0$ and if $q \neq 0$, then $(I \cap R^G)q \neq 0$. Now $(I \cap R^G)q \subseteq R$ and since the left hand side is fixed by G we have $(I \cap R^G)q \subseteq R^G$. Thus q determines an element of $Q_0(R^G)$ and in this way we clearly obtain a homomorphism $Q_0(R)^G \to Q_0(R^G)$. Moreover this map is an embedding since if $q \neq 0$, then $(I \cap R^G)q \neq 0$ and hence the image of q is not zero. We can now view $Q_0(R)^G$ as a subring of $Q_0(R^G)$.

Now let $\tilde{q} \in Q_0(R^G)$. Then there exists an ideal $I \neq 0$ of R^G and a left R^G-module homomorphism $\tilde{f}: I \to R^G$ which determines $\tilde{q}$. We extend $\tilde{f}$ to $f: RI \to R$ by defining

$$\left(\sum_k r_k y_k\right) f = \sum_k r_k (y_k \tilde{f})$$

for $r_k \in R$, $y_k \in I$. This map will certainly extend $\tilde{f}$ and be a left R-module homomorphism provided we show it is well defined. To this end it suffices to show that $\sum_k r_k y_k = 0$ implies $\sum_k r_k (y_k \tilde{f}) = 0$.

Let $\tau(x) = \sum_i a_i x^{g_i} b_i$ be an outer trace form given by Lemma 2.4 with $a_i, b_i \in B$. Furthermore we can assume that $g_0 = 1$, $b_0 = 1$ and that $\{a_i \mid g_i = 1\}$ is C-linearly independent. By Lemma 2.5 there exists a nonzero ideal J of R with $\tau(J) \subseteq R^G$. Now suppose $\sum_k r_k y_k = 0$ with $r_k \in R$, $y_k \in I$ and consider the truncation of τ defined by

$$T(x) = \sum_k \tau(x r_k)(y_k \tilde{f}) = \sum_i a_i x^{g_i} \bar{b}_i.$$

Since $g_0 = 1$, $b_0 = 1$ we note that $\bar{b}_0 = \sum_k r_k (y_k \tilde{f})$.

Now let $j \in J$. Then $0 = \sum_k j r_k y_k$ so since $y_k \in R^G$ we have

$$0 = \tau\left(\sum_k j r_k y_k\right) = \sum_k \tau(j r_k) y_k.$$

But $\tau(jr_k)\in R^G$ and $\bar{f}$ is a left R^G-module homomorphism, so applying $\bar{f}$ yields

$$0=\sum_k \tau(jr_k)(y_k\bar{f})=T(j).$$

In other words, T vanishes on the nonzero ideal J of R. Lemma 3.5 now implies that $0=\bar{b}_0=\sum_k r_k(y_k\bar{f})$ and $f:RI\to R$ is well defined.

Since R^G is prime, Lemma 9.2(ii) implies that RI contains a nonzero two-sided ideal L of R. Hence $f:L\to R$ determines an element $q\in Q_0(R)$. It is now easy to see that $yq=y\bar{f}=y\tilde{q}\in R^G$ for all $y\in I$. Thus if $g\in G$ we obtain $yq^g=(yq)^g=yq$, so $RI(q-q^g)=0$ and therefore $q\in Q_0(R)^G\subseteq Q_0(R^G)$. But then $I(q-\tilde{q})=0$ yields $\tilde{q}=q\in Q_0(R^G)$, so we have the reverse inclusion, namely $Q_0(R^G)\subseteq Q_0(R)^G$, and the proposition is proved.

10. Embeddings

We now wish to study the various embeddings of a ring $S\supseteq R^G$ into R. In this regard, the following lemma is crucial. Here R is a prime ring and G is an M-group of automorphisms.

Lemma 10.1. *Let $S\supseteq R^G$ satisfy* [GI] *and* [GH] *and let $\varphi:S\to R$ be an isomorphism into with φ the identity on R^G. If f is a primitive idempotent of $Z=\mathbb{C}_B(S)$, then there exists $b\in B$, $g\in G$ such that $b=f^gb\neq 0$ and $s^gb=bs^\varphi$ for all $s\in S$. Furthermore, if $g\in G\cap \operatorname{Inn} R$, then $g=1$. Finally if e is an idempotent of Z with $fe\neq 0$ and if φ extends to an embedding $\varphi:\langle S,e\rangle\to Q$, then we may assume that $b=be^\varphi$.*

Proof. Let $\tau(x)=\sum_i a_ix^{g_i}b_i$ be the trace form given by Lemma 7.1 for f and use the notation of that lemma. In particular, $H=G\cap \mathscr{G}(R/S)$ and I is a nonzero ideal of R with $\tau(I)\subseteq R^G$. We can now apply Lemma 6.2 to this form and obtain a form $T(x)=\sum_i a_ix^{g_i}z_i$ and a nonzero ideal J of R such that $T(xj)$ is an (R,S)-truncation of τ for all $j\in J$. Additional properties of T are listed in Lemma 6.2 and will be used in the course of the proof.

For each subscript t we define $\theta_t:J\to Q$ as follows. Let $j\in J$ and write $T(xj)=\sum_k \tau(xr_k)s_k$ with $r_k\in R$, $s_k\in S$. Then we let

$$\theta_t(j)=\sum_k r_k^{g_t}b_ts_k^\varphi.$$

We must first show that this is well defined. Thus suppose $T(xj)=\sum_k \tau(x\bar{r}_k)\bar{s}_k$ with $\bar{r}_k\in R$, $\bar{s}_k\in S$. Then for any $y\in I$ we have

$$\sum_k \tau(yr_k)s_k=\sum_k \tau(y\bar{r}_k)\bar{s}_k$$

and since $\tau(I)\subseteq R^G$ we have, applying φ,

$$\sum_k \tau(yr_k)s_k^\varphi=\sum_k \tau(y\bar{r}_k)\bar{s}_k^\varphi$$

In other words, the form

$$\tilde{T}(x)=\sum_k \tau(xr_k)s_k^{\varphi}-\sum_k \tau(x\bar{r}_k)\bar{s}_k^{\varphi}=\sum_i a_i x^{g_i}\tilde{b}_i$$

vanishes on I. Let $g\in \Lambda$, the transversal for G_0 in G, and observe that if $g_i\in G_0 g=gG_0$, then $g_i=g$ by assumption on τ. Furthermore $\{a_i \mid g_i=g\}$ is C-linearly independent. Thus it follows from Lemma 3.5 applied to the form $\tilde{T}(x^{g^{-1}})$ that $\tilde{b}_i=0$ for all i. In particular

$$0=\tilde{b}_t=\sum_k r_k^{g_t}b_t s_k^{\varphi}-\sum_k \bar{r}_k^{g_t}b_t\bar{s}_k^{\varphi}$$

and θ_t is well defined.

We now study $\theta_t: J\to Q$ in more detail. Since $T(x(j_1+j_2))=T(xj_1)+T(xj_2)$, it is clear that θ_t is additive. Furthermore, $T(xrj)$ can be obtained from $T(xj)$ by replacing x by xr so we have easily $\theta_t(rj)=r^{g_t}\theta_t(j)$. Observe that $\theta_t(J)\subseteq Rb_tR$ and for some nonzero ideal L of R we have $L^{g_t}b_t\subseteq R$. Hence $\theta_t(LJ)=L^{g_t}\theta_t(J)\subseteq R$ and, by replacing J with LJ if necessary, we can now assume that $\theta_t: J\to R$. Since $\theta_t^{g_t^{-1}}(rj)=r\theta_t^{g_t^{-1}}(j)$, $\theta_t^{g_t^{-1}}$ is a left R-module homomorphism and there exists an element $\bar{q}_t\in Q$ with $\theta_t^{g_t^{-1}}(j)=j\bar{q}_t$ or equivalently

$$\theta_t(j)=j^{g_t}\bar{q}_t^{g_t}=j^{g_t}q_t \quad \text{where } q_t=\bar{q}_t^{g_t}\in Q.$$

Again, by Lemma 6.2, we have $z_i\in Z$ and if $z_i\neq 0$, then $g_i\in H$. It follows from this that $T(xjs)=T(xj)s$ for $s\in S$ and hence we have easily $\theta_t(js)=\theta_t(j)s^{\varphi}$. Thus the above formula for θ_t yields

$$j^{g_t}s^{g_t}q_t=\theta_t(js)=\theta_t(j)s^{\varphi}=j^{g_t}q_t s^{\varphi}$$

and since this holds for all $j\in J$ we have $s^{g_t}q_t=q_t s^{\varphi}$. Moreover both g_t and φ fix $R^G\subseteq S$, so q_t centralizes R^G and hence $q_t\in B$ by Proposition 4.1. Now let $U\neq 0$ be an ideal of R with $Uf\subseteq R$ and set $W=JU\subseteq J$ so that $W\neq 0$ and $Wf\subseteq J$. Observe that for any $w\in W$, both w and wf belong to J and hence, by Lemma 6.2, $T(xwf)=T(xw)$. This implies that $\theta_t(wf)=\theta_t(w)$, so

$$w^{g_t}f^{g_t}q_t=\theta_t(wt)=\theta_t(w)=w^{g_t}q_t$$

and since this holds for all $w\in W$, we have $f^{g_t}q_t=q_t$. Note further that $g_t\in\Lambda$ so that if $g_t\in G_0$, then $g_t=1$.

It remains to find some t with $q_t\neq 0$. To this end, suppose that e is an idempotent of Z with $fe\neq 0$ and that φ extends to an embedding $\varphi:\langle S,e\rangle\to Q$. Observe that this condition is trivially satisfied with $e=1$. Since $z_0=f$, we have $z_0e=fe\neq 0$ and it follows from Lemma 3.5 that the outer trace form $T(x)e$ does not vanish on the nonzero ideal IJ. Thus there exist $y\in I$, $j\in J$ with $T(yj)e\neq 0$. Now write $T(xj)=\sum_k \tau(xr_k)s_k$ with $r_k\in R$, $s_k\in S$. Then

$$0\neq T(yj)e=\sum_k \tau(yr_k)s_k e.$$

Thus since $\varphi:\langle S,e\rangle\to Q$ is an embedding and $\tau(yr_k)\in R^G$ we have

$$0\neq\sum_k \tau(yr_k)s_k^{\varphi}e^{\varphi}=\sum_t a_t y^{g_t}\theta_t(j)e^{\varphi}.$$

Hence for some t, $\theta_t(j)e^{\varphi}\neq 0$ so $q_te^{\varphi}\neq 0$.

Finally, for this t, set $b=q_te^{\varphi}$ and $g=g_t$. Since $f^{g_t}q_t=q_t$ we have $f^gb=b$ and since e^{φ} is an idempotent we have $be^{\varphi}=b\neq 0$. Furthermore since e centralizes S, e^{φ} centralizes S^{φ}, so multiplying the equation $s^{g_t}q_t=q_ts^{\varphi}$ on the right by e^{φ} yields $s^gb=bs^{\varphi}$. In particular, this implies that b centralizes R^G, so $b\in B$ and the lemma is proved.

In general the question of whether embeddings $\varphi:S\to R$ are actually the restriction of elements of G is closely related to the minimal primes of S and even more so to the central idempotents of Z. In this section we will just indicate some of the more satisfactory consequences of the above lemma. We start with the X-outer case.

Proposition 10.2. *Let G be a finite group of X-outer automorphisms of the prime ring R and let $S\supseteq R^G$. If $\varphi:S\to R$ is an isomorphism into with φ the identity on R^G, then φ is the restriction of some $g\in G$.*

Proof. Since $B=C$, we know that S satisfies [GI] and [GH]. Thus by the previous lemma with $f=1$, there exists $b\in B\setminus 0$, $g\in G$ with $s^gb=bs^{\varphi}$ for all $s\in S$. But b is a central unit of Q, so we can cancel and obtain $s^g=s^{\varphi}$.

Proposition 10.3. *Let G be an N-group of automorphisms of the domain R and let $S\supseteq R^G$. If $\varphi:S\to R$ is an isomorphism into with φ the identity on R^G, then φ is the restriction of some $g\in G$.*

Proof. Since B is a division ring, by Corollary 8.4, we know that S automatically satisfies [GI] and [GH]. Thus by Lemma 10.1 with $f=1$, there exists $b\in B\setminus 0$, $g\in G$ with $s^gb=bs^{\varphi}$ for all $s\in S$. Since b is a unit of B, conjugation by b gives rise to an element $g_0\in G$ and we have $s^{\varphi}=b^{-1}s^gb=s^{gg_0}$.

Proposition 10.4. *Let G be an N-group of X-inner automorphisms of the prime ring R and let $S\supseteq R^G$ satisfy [GI]. Suppose $\varphi:S\to R$ is an isomorphism into with φ the identity on R^G. Then φ is the restriction of some $g\in G$ if and only if φ extends to an embedding $\varphi:\langle S,Z\rangle\to Q$ where $Z=\mathbb{C}_B(S)$.*

Proof. It is clear that if φ is the restriction of some $g\in G$, then φ does indeed extend to an embedding $\varphi:\langle S,Z\rangle\to Q$. Conversely suppose $\varphi:\langle S,Z\rangle\to Q$ exists and let $1=f_1+f_2+\cdots+f_n$ be a decomposition of 1 into orthogonal primitive idempotents of Z. Since S satisfies [GI] and since [GH] is automatically satisfied, Lemma 10.1 applies. Indeed since G is X-inner, we conclude that for each i there exists $b_i\in B$ with $sb_i=b_is^{\varphi}$ for all $s\in S$ and $b_i=f_ib_i=b_if_i^{\varphi}\neq 0$.

Now f_i is a primitive idempotent of Z, so it follows that $l_{Zf_i}(b_i)$ contains no nonzero idempotents. Thus by Lemma 8.6(i), since $Sb_i = b_i S^\varphi$, we conclude that $l_Q(b_i) = l_Q(f_i)$. Set $b = b_1 + b_2 + \cdots + b_n \in B$ and observe that $bf_i^\varphi = b_i$ since for $j \neq i$, $b_j f_i^\varphi = b_j f_j^\varphi f_i^\varphi = 0$. Thus if $qb = 0$ for some $q \in Q$, then $0 = qbf_i^\varphi = qb_i$ and hence $0 = qf_i$ by the above. But $1 = \sum f_i$ so we have $q = 0$ and b is left regular in Q and hence invertible in B. Finally by adding the equations $sb_i = b_i s^\varphi$ we conclude that $sb = bs^\varphi$ so $s^\varphi = b^{-1}sb$. Since conjugation by b is an element of the N-group G, the result follows.

It is clear in the above that we need only assume that φ can be extended to $\langle S, Z' \rangle$ where Z' is a subring of Z containing a full set of orthogonal primitive idempotents of Z.

11. Embeddings and minimal primes

Again let G be an N-group of automorphisms of the prime ring R. If $\varphi : S \to \bar{S}$ is an isomorphism, then surely φ maps the minimal primes of S to those of $\bar{S}$. As we will see, these minimal primes play an important role in understanding the nature of φ.

Lemma 11.1. *Let $S \subseteq R^G$ satisfy* [GZ], [GI] *and* [GH]. *Set $Z = \mathbb{C}_B(S)$, $H = \mathscr{G}(R/S)$ and let $f_1, f_2, \ldots, f_n$ be the H-centrally primitive idempotents of Z. If $P_i = \operatorname{ann}_S(f_i)$, then*

(i) *The ideals $P_1, P_2, \ldots, P_n$ are the distinct minimal primes of S and $P_1 \cap P_2 \cap \cdots \cap P_n = 0$.*

(ii) $\operatorname{ann}_Z(P_i) = Zf_i$.

(iii) *If f is any nonzero idempotent in Zf_i, then* $\operatorname{ann}_S(f) = P_i$ *and hence the map $s \to fs$ yields a natural isomorphism $S/P_i \simeq fS$.*

Proof. By Proposition 7.3, H is an N-subgroup of G with algebra of the group Z. Furthermore, S contains a two-sided ideal K of $R^H = \bar{S}$ with $\mathrm{r}_Q(K) = l_Q(K) = 0$. For each i, let $\bar{P}_i = \operatorname{ann}_{\bar{S}}(f_i)$ so that $P_i = \bar{P}_i \cap S$. Note that $K \not\subseteq \bar{P}_i$ since $Kf_i \neq 0$. By Proposition 9.3, the ideals $\bar{P}_i$ are the distinct minimal primes of $\bar{S}$ and $\bigcap \bar{P}_i = 0$. Thus certainly $\bigcap P_i = 0$. Moreover from $K\bar{P}_i \subseteq \bar{P}_i \cap S = P_i$ and Lemma 9.2(i), we have $\operatorname{ann}_Z(P_i) = \operatorname{ann}_Z(\bar{P}_i) = Zf_i$ and hence the ideals P_i are incomparible. Now suppose $s, t \in S$ with $sSt \subseteq P_i$. Then $sKt \subseteq P_i \subseteq \bar{P}_i$ and since K is an ideal of $\bar{S}$ not contained in $\bar{P}_i$, we deduce that s or t is contained in $\bar{P}_i \cap S = P_i$. Hence each P_i is prime. Finally if f is a nonzero idempotent in Zf_i, then $\operatorname{ann}_Z(\operatorname{ann}_S(f))$ is an H-invariant ideal of Z containing f so we conclude immediately that $\operatorname{ann}_S(f) = \operatorname{ann}_S(f_i) = P_i$ and the lemma is proved.

If e is an idempotent in a semisimple Artinian ring A, then we define $\operatorname{rk}_A e$, the rank of e, to be the composition length of eA. This is of course the maximum m such that e can be written as a sum of m orthogonal idempotents and thus the rank is right-left symmetric.

Lemma 11.2. *Let A be a semisimple Artinian ring and let e_1, e_2 be idempotents in A. Suppose there exists $b \in A$ such that $b = e_1 b = be_2$ and assume that at least two of the three equalities $l_A(e_1) = l_A(b)$, $\mathrm{r}_A(e_2) = \mathrm{r}_A(b)$, $\mathrm{rk}_A(e_1) = \mathrm{rk}_A(e_2)$ are satisfied. Then there is a unit $u \in A$ with $b = e_1 u = ue_2$.*

Proof. Certainly one of the two annihilator conditions is satisfied and by symmetry we may suppose that $l_A(e_1) = l_A(b)$. Now right multiplication by b defines a left A-module homomorphism

$$Ae_1 \to Ae_1 b = Ab = Abe_2 \subseteq Ae_2.$$

This map is one-to-one since if $(ae_1)b = 0$, then $ae_1 \in l_A(b) = l_A(e_1)$ and hence $ae_1 = (ae_1)e_1 = 0$. We claim that the map is onto Ae_2. Indeed if $\mathrm{rk}_A(e_1) = \mathrm{rk}_A(e_2)$, this is obvious since both Ae_2 and the image of Ae_1 have the same composition length. On the other hand if $\mathrm{r}_A(e_2) = \mathrm{r}_A(b)$, then $\mathrm{r}_A(Ab) = \mathrm{r}_A(Ae_2)$ and again, since A is semisimple, we have $Ab = Ae_2$.

Thus $Ae_1 \simeq Ae_2$ via multiplication by b and by the Jordan–Holder theorem we also have $A(1-e_1) \simeq A(1-e_2)$. Combining these we have an isomorphism ${}_AA \simeq {}_AA$ and this of course must be achieved via right multiplication by a unit $u \in A$. Thus we have $e_1 u = e_1 b = b$ and $A(1-e_1)u = A(1-e_2)$. Hence

$$u = 1u = e_1 u + (1-e_1)u = b + a'(1-e_2)$$

for some $a' \in A$ and then $ue_2 = be_2 = b$.

Given the situation of Lemma 11.1, if e_i is a centrally primitive idempotent of Z contained in Zf_i, then we define $\deg P_i = \mathrm{rk}_Z e_i$. Since all such e_i are H-conjugate, this is well defined. Furthermore we let $\mathrm{mult}\, P_i$, the multiplicity of P_i, be the number of distinct H-conjugates of e_i. Thus clearly $\mathrm{rk}_Z f_i = (\deg P_i)(\mathrm{mult}\, P_i)$ and

$$\sum_i (\deg P_i)(\mathrm{mult}\, P_i) = \mathrm{rk}_Z(1).$$

We now come to the main result on embeddings.

Theorem 11.3. *Let G be an N-group of automorphisms of the prime ring R and let $S, \bar{S} \supseteq R^G$ both satisfy* [GZ], [GI] *and* [GH]. *Suppose $\varphi: S \to \bar{S}$ is an isomorphism which is the identity on R^G and assume that P and $\bar{P} = P^\varphi$ are corresponding minimal primes of S and $\bar{S}$. Let e be a centrally primitive idempotent of $Z = \mathbb{C}_B(S)$ with $Pe = 0$ and let f be a primitive idempotent in Ze. Similarly let $\bar{e}$ be a centrally primitive idempotent of $\bar{Z} = \mathbb{C}_B(\bar{S})$ with $\bar{P}\bar{e} = 0$ and let $\bar{f}$ be a primitive idempotent in $\bar{Z}\bar{e}$.*

(i) *There exists an element* $g \in G$ *such that* $(fs)^g = \bar{f}s^\varphi$ *for all* $s \in S$. *Hence* g *'induces' the isomorphism* $\varphi : S/P \to \bar{S}/\bar{P}$ *via the combined map*

$$S/P \simeq fS \xrightarrow{g} \bar{f}\bar{S} \simeq \bar{S}/\bar{P}.$$

(ii) $(\mathrm{rk}_B e)/(\deg P) = (\mathrm{rk}_B \bar{e})/(\deg \bar{P})$.

(iii) *If either* $\deg P = \deg \bar{P}$ or $\mathrm{rk}_B e = \mathrm{rk}_B \bar{e}$, *then there exists* $g \in G$ *with* $(es)^g = \bar{e}s^\varphi$ *for all* $s \in S$.

Proof. (i) By Lemma 10.1 there exists $b \in B$, $g \in G$ such that $b = f^g b \neq 0$ and $s^g b = bs^\varphi$ for all $s \in S$. Now $b \neq 0$ so there exists a primitive idempotent $\bar{f}$ of $\bar{Z}$ with $b\bar{f} \neq 0$. Since $\bar{f}$ commutes with s^φ, we can now clearly replace b by $b\bar{f}$ and assume in addition that $b\bar{f} = b$. Observe that $S^g b = b\bar{S}$ and both S^g and $\bar{S}$ satisfy [GI]. Thus since both f^g and $\bar{f}$ are primitive idempotents of Z^g and $\bar{Z}$ respectively, we conclude from Lemma 8.6(i)(ii) that $l_Q(b) = l_Q(f^g)$ and $\mathrm{r}_Q(b) = \mathrm{r}_Q(\bar{f})$. Lemma 11.2 applied to the semisimple algebra B now implies that there is a unit $u \in B$ with $b = f^g u = u\bar{f}$. Thus for all $s \in S$

$$s^g f^g u = s^g b = bs^\varphi = u\bar{f}s^\varphi$$

and hence $u^{-1}s^g f^g u = \bar{f}s^\varphi$. But conjugation by the unit $u \in B$ corresponds to an element g_0 in the N-group G, so replacing g by gg_0 yields $(sf)^g = \bar{f}s^\varphi$.

Since f annihilates P, it follows that $\bar{f}$ annihilates $\bar{P} = P^\varphi$. But all such primitive idempotents of $\bar{Z}$ which annihilate $\bar{P}$ are in fact $\bar{H}$-conjugate, where $\bar{H} = \mathscr{G}(R/\bar{S})$. This follows since $\bar{H}$ transitively permutes the simple components in $\mathrm{ann}_{\bar{Z}}(\bar{P})$, by Lemma 11.1(ii), and since, within each simple component, primitive idempotents are conjugate via units of $\bar{Z}$ and hence via elements of $\bar{H}$. Thus $\bar{f} = \bar{f}^{\bar{h}}$ for some $\bar{h} \in H$. Since $\bar{h}$ centralizes $\bar{S}$, we conclude that $(sf)^{g\bar{h}} = (\bar{f}s^\varphi)^{\bar{h}} = \bar{f}s^\varphi$ and (i) follows from Lemma 11.1(iii).

(ii) Since the primitive idempotents of eZ are all conjugate to f, we have $\mathrm{rk}_B(e) = \mathrm{rk}_Z(e) \cdot \mathrm{rk}_B(f) = \deg P \cdot \mathrm{rk}_B(f)$ and similarly $\mathrm{rk}_B(\bar{e}) = \deg \bar{P} \cdot \mathrm{rk}_B(\bar{f})$. However, as a consequence of (i) above, we have $f^g = \bar{f}$ and hence

$$\mathrm{rk}_B(e)/\deg P = \mathrm{rk}_B(f) = \mathrm{rk}_B(\bar{f}) = \mathrm{rk}_B(\bar{e})/\deg \bar{P}.$$

(ii) In view of (ii), $\deg P = \deg \bar{P}$ if and only if $\mathrm{rk}_B(e) = \mathrm{rk}_B(\bar{e})$. Thus we can assume that the latter ranks are equal. Let $g \in G$ be as in (i) and define

$$V = \{ b \in B \mid e^g b = b, b\bar{e} = b, s^g b = bs^\varphi \text{ for all } s \in S \}.$$

Then V is clearly a unitary $(Z^g e^g, \bar{Z}\bar{e})$-bimodule and $V \neq 0$ since $f^g = \bar{f} \in V$. Furthermore, $Z^g e^g$ and $\bar{Z}\bar{e}$ are simple Artinian rings, so it follows from Lemma 8.5 that there exists $b \in B$ with $l_{Z^g e^g}(b) = 0$ or $\mathrm{r}_{\bar{Z}\bar{e}}(b) = 0$. Again $S^g b = b\bar{S}$ and both S^g and $\bar{S}$ satisfy [GI]. Thus we conclude from Lemma 8.6(i) or (ii) that either $l_Q(b) = l_Q(e^g)$ or $\mathrm{r}_Q(b) = \mathrm{r}_Q(\bar{e})$. Lemma 11.2 applied to the semisimple algebra B now implies that there exists a unit $u \in B$ with $b = e^g u = u\bar{e}$. Since conjugation by u corresponds to an element $g_0 \in G$ it follows easily as in (i) that $(se)^{gg_0} = u^{-1}(se)^g u = \bar{e}s^\varphi$ for all $s \in S$ and the theorem is proved.

Note that if $\varphi : S \to \bar{S}$ is given, then it is not necessarily true that $\deg P = \deg \bar{P}$. Hence this hypothesis is certainly required in (iii) above. Now suppose that Z and $\bar{Z}$ are simple so that $e = \bar{e} = 1$. Since [GZ′] and [GI] imply [GH], by Lemma 8.7, we obtain immediately

Corollary 11.4. *Let G be an N-group of automorphisms of the prime ring R and let $S, \bar{S} \supseteq R^G$ satisfy* [GZ′] *and* [GI]. *If $\varphi : S \to \bar{S}$ is an isomorphism which is the identity on R^G, then φ is the restriction of some $g \in G$.*

We will consider a number of examples in Section 13 which show that the above results, and in particular Theorem 11.3(iii), precisely indicate the extent to which φ agrees with elements of G. One can of course assume a homogeneity condition on φ to force the group elements g so obtained, for each centrally primitive idempotent, to agree appropriately. However we will not pursue this idea further except to point out in the following lemma that the group elements need only agree modulo X-inners.

Lemma 11.5. *Let $S, \bar{S} \supseteq R^G$ both satisfy* [GZ], [GI] *and* [GH] *and let $\varphi : S \to \bar{S}$ be an isomorphism which is the identity on R^G. Suppose that for each minimal prime P of S we have* $\deg P = \deg P^\varphi$ *and* $\operatorname{mult} P = \operatorname{mult} P^\varphi$. *Then there is a one-to-one correspondence $e_i \leftrightarrow \bar{e}_i$ between the centrally primitive idempotents e_i of $Z = \mathbb{C}_B(S)$ and $\bar{e}_i$ of $\bar{Z} = \mathbb{C}_B(\bar{S})$ such that, for some $g_i \in G$, $(e_i s)^{g_i} = \bar{e}_i s^\varphi$ for all $s \in S$. Furthermore if the elements g_i all agree modulo $G_0 = G \cap \operatorname{Inn} R$, then φ is the restriction of some $g \in G$.*

Proof. Since the minimal primes of S and $\bar{S}$ correspond, it follows from Lemma 11.1(ii) and $\operatorname{mult} P = \operatorname{mult} P^\varphi$ that the centrally primitive idempotents of Z and of $\bar{Z}$ correspond. Furthermore from Theorem 11.3(iii) and $\deg P = \deg P^\varphi$, there exist group elements g_i with $(e_i s)^{g_i} = \bar{e}_i s^\varphi$ for all $s \in S$. Finally suppose all g_i agree with $g \in G$ modulo G_0. Then there exist units $b_i \in B$ with

$$\bar{e}_i s^\varphi = (e_i s)^{g_i} = b_i^{-1}(e_i s)^g b_i$$

so $(b_i \bar{e}_i)s^\varphi = s^g(e_i^g b_i)$. In particular $b_i \bar{e}_i = e_i^g b_i$.

Now let $b = \sum_i b_i \bar{e}_i \in B$. Then $bs^\varphi = s^g b$ for all $s \in S$ and b is a unit of B. Indeed, for the latter, if $qb = 0$, then

$$0 = qb\bar{e}_j = qb_j\bar{e}_j = qe_j^g b_j$$

and hence $0 = qe_j^g$. But $1 = \sum e_j^g$, so $q = 0$ and therefore b is left regular and hence a unit in the finite-dimensional algebra B. Thus conjugation by b gives rise to an element $g_0 \in G$ and we conclude that $s^\varphi = b^{-1}s^g b = s^{gg_0}$ so φ is the restriction of $gg_0 \in G$.

12. Almost normal subgroups

In this section we use the results on extensions of automorphisms to study normal and, more generally, almost normal subgroups of G. Again R is a prime ring and G is an N-group of automorphisms of R unless otherwise indicated. Recall that $H \subseteq G$ is an F-subgroup if H is an N-subgroup of G with $B(H)$, the algebra of the group of H, a simple ring.

Proposition 12.1. *Let H be an F-subgroup of G and let $K = \mathbb{N}_G(H)$. Then R^H is a prime ring and $\mathcal{G}(R^H/R^G) = K/H$.*

Proof. Proposition 9.3 implies that R^H is prime. If $g \in G$, then $(R^H)^g = R^{H^g}$, so g stabilizes R^H if and only if $g \in K$. In particular K acts on R^H and fixes R^G so the restriction map yields a homomorphism of K into $\mathcal{G}(R^H/R^G)$. Observe that $\mathcal{G}(R/R^H) = H$, by Theorem 4.3, so the kernel of this homomorphism is H. Furthermore since H is an F-group, R^H satisfies [GZ′] and [GI] and hence, by Corollary 11.4, every automorphism of R^H fixing R^G is the restriction of some $g \in G$. But then g stabilizes R^H so $g \in K$ and the homomorphism is onto.

Several natural questions now arise in the above situation. First, when is R^G the fixed ring of $\mathcal{G}(R^H/R^G)$ and second, when is this group an N-group of automorphisms of the prime ring R^H. We consider these in the remainder of this section.

If A is a ring we let $\mathrm{usp}(A)$ denote the linear span of its units. It is clear that $\mathrm{usp}(A)$ is a subring of A with the same 1.

Lemma 12.2. *Let A be an Artinian ring. Then A is semisimple if and only if* $\mathrm{usp}(A)$ *is semisimple.*

Proof. If A is semisimple, then $A = \bigoplus A_i$ is a direct sum of simple rings. If no A_i is GF(2), then it follows easily that $\mathrm{usp}(A) = A$. On the other hand if some A_i is GF(2), then $\mathrm{usp}(A) \simeq \bigoplus' A_i$ where $'$ indicates that all but one GF(2) summand is deleted. Conversely suppose $\mathrm{usp}(A)$ is semisimple and let J be the radical of A. Then $1 + J \subseteq \mathrm{usp}(A)$ implies that $J \subseteq \mathrm{usp}(A)$ and hence that $J = 0$.

Again let H be an F-subgroup of G. Then $K/H = \mathcal{G}(R^H/R^G)$ and we now describe the algebra of the group of K/H.

Lemma 12.3. *Let H be an F-subgroup of G and let $K = \mathbb{N}_G(H)$. Then $B_{R^H}(K/H) =$* $\mathrm{usp}(B^H)$ *where $B = B(G)$. Furthermore this is a finite-dimensional algebra over the extended centroid of R^H and every unit of this algebra gives rise to an X-inner automorphism of R^H.*

Proof. By Proposition 9.6 applied to H, we have $Q_0(R^H) = Q_0(R)^H$ and thus

$B^H \subseteq Q_0(R^H)$. Observe that if q is a unit of B^H, then $q^{-1}R^Hq \subseteq R$ and, since the left hand side is fixed by H, we have $q^{-1}R^Hq \subseteq R^H$. Thus each such q gives rise to an X-inner automorphism of R^H fixing R^G. In view of Proposition 12.1 this yields $\mathrm{usp}(B^H) \subseteq B_{R^H}(K/H)$.

Conversely let $q \in Q_0(R^H) = Q_0(R)^H$ be a unit which gives rise to an automorphism of R^H fixing R^G. Then $q \in B$, by Proposition 4.1, so $q \in B \cap Q_0(R)^H = B^H$. Since q is a unit we have $q \in \mathrm{usp}(B^H)$ and the reverse inclusion is proved. Finally observe that $H_0 = H \cap \mathrm{Inn}\, R$ centralizes the extended centroid C of R so the finite group H/H_0 acts on this field. Thus C is finite-dimensional over C^H and hence so is B. But clearly $C^H \subseteq Q_0(R^H)$ is contained in the extended centroid of R^H so the result follows.

We now formally begin the proof of Theorem D and we fix notation for the remainder of this section. Thus we let H be an F-subgroup of G, $K = \mathbb{N}_G(H)$ and $Z = B(H)$. By assumption, Z is simple and we let T denote its center.

Lemma 12.4. *Let $\mathscr{K}$ be the group of units of B which give rise to automorphisms of K and let $\mathscr{H}$ denote the group of units of Z.*

(i) *If $h \in H$ and $k \in \mathscr{K}$, then $k^h = kz$ for some $z \in \mathscr{H}$.*

(ii) *$\mathscr{H} \lhd \mathscr{K}$ and $\mathscr{H}(\mathscr{K} \cap B^H)$ is a subgroup of $\mathscr{K}$ of finite index.*

Proof. (i) Since $k \in B$, $k^{-1}k^h$ is a unit of B. Furthermore since k gives rise to an element of $K = \mathbb{N}_G(H)$, we see that, in its action on R, $k^{-1}k^h = k^{-1}h^{-1}kh$ is an element of H. Thus this unit $k^{-1}k^h$ must belong to $B(H) = Z$.

(ii) Since H is an N-subgroup of G, all units of Z give rise to automorphims in H and hence in K. Thus $\mathscr{H}$ is a subgroup of $\mathscr{K}$ and in fact $\mathscr{H} \lhd \mathscr{K}$ since $H \lhd K$. This implies that $\mathscr{H}(\mathscr{K} \cap B^H)$ is a subgroup of $\mathscr{K}$. Now $\mathscr{K}$ acts on Z by conjugation and hence also on T, the center of Z. Since T is a finite field extension of C and $\mathscr{K}$ centralizes C, we conclude that $\mathscr{K}_1 = \mathscr{K} \cap \mathbb{C}_B(T)$ has finite index in $\mathscr{K}$. Thus it suffices to show that $\mathscr{H}(\mathscr{K} \cap B^H)$ has finite index in $\mathscr{K}_1$.

Let $k \in \mathscr{K}_1$. Then conjugation by k yields an automorphism of the simple finite dimensional algebra Z which fixes the center of Z. By the Skolem–Noether theorem, this automorphism must be inner on Z. Thus there exists $z \in \mathscr{H}$ such that $z^{-1}k$ centralizes Z. We have therefore shown that $\mathscr{K}_1 = \mathscr{H}\mathscr{K}_2$ where $\mathscr{K}_2 = \mathscr{K} \cap \mathbb{C}_B(Z)$ and thus it suffices to show that $[\mathscr{K}_2 : T^\circ(\mathscr{K} \cap B^H)] < \infty$. Here T° denotes the multiplicative group of T and clearly $T^\circ = \mathscr{H} \cap \mathscr{K}_2$. Note that H acts on B, Z and T and that $H_0 = H \cap \mathrm{Inn}\, R$ acts trivially on T. Thus if $L = \mathbb{C}_H(T)$, *then* $L \supseteq H_0$ so $|H/L| < \infty$. Furthermore, since $H \subseteq K$ it is clear that H acts on $\mathscr{K}$ and then on $\mathscr{K}_2$. Our goal is to show that $[\mathscr{K}_2 : \mathscr{K} \cap B^L] < \infty$ and then that $\mathscr{K} \cap B^l = T^\circ(\mathscr{K} \cap B^H)$. This will surely prove the result.

Observe that H_0 centralizes $\mathscr{K}_2$ so that the finite group L/H_0 acts on $\mathscr{K}_2$. Fix $h \in L$ and, for each $k \in \mathscr{K}_2$ write $k^h = k\lambda(k)$ where $\lambda(k) \in \mathscr{H}$ by (i) above. Since $k^h, k \in \mathscr{K}_2$ we see that $\lambda(k) \in \mathscr{H} \cap \mathscr{K}_2 = T^\circ$ and thus λ is a map from $\mathscr{K}_2$ to T°. Indeed if $k_1, k_2 \in \mathscr{K}_2$ then, since $\mathscr{K}_2$ centralizes T°. we have

$$k_1k_2\lambda(k_1k_2) = (k_1k_2)^h = k_1^h k_2^h$$
$$= k_1\lambda(k_1)k_2\lambda(k_2) = k_1k_2\lambda(k_1)\lambda(k_2)$$

and $\lambda : \mathscr{K}_2 \to T^\circ$ is actually a linear character. Furthermore since $h \in L$ acts trivially on T° we have easily $k^{h^m} = k\lambda(k)^m$ for all integers m. But $|L/H_0| < \infty$, so $h^n \in H_0$ for some $n \geq 1$ and thus λ is a homomorphism from $\mathscr{K}_2$ into the finite group of n-th roots of unity in T. We conclude therefore that h centralizes a subgroup of finite index in $\mathscr{K}_2$ namely the kernel of λ. Since this is true for each element $h \in L$ and since L/H_0 is finite, we deduce that $[\mathscr{K}_2 : \mathscr{K} \cap B^L] < \infty$.

Finally observe that $\mathscr{K} \cap B^L \supseteq T^\circ(\mathscr{K} \cap B^H)$ and fix $k \in \mathscr{K} \cap B^L$. Then for each $h \in H$ we have, by (i) above, $k^h = k\mu(h)$ where $\mu(h) \in \mathscr{K}$. Again since $k^h, k \in \mathscr{K}_2$ we see that $\mu(h) \in \mathscr{K} \cap \mathscr{K}_2 = T^\circ$ and thus μ is a map from H to T°. Indeed since L acts trivially on $k \in \mathscr{K} \cap B^L$, μ is actually a map from the finite group H/L to T°. Next suppose $h_1, h_2 \in H$. Then

$$k\mu(h_1h_2) = k^{h_1h_2} = (k\mu(h_1))^{h_2} = k\mu(h_2)\mu(h_1)^{h_2}$$

so μ satisfies Noether's equation $\mu(h_1h_2) = \mu(h_1)^{h_2}\mu(h_2)$. Therefore by the above remarks and the fact that H/L acts faithfully on the field T, we conclude that μ is a trivial crossed homomorphism. In other words, there exists $t \in T^\circ$ with $\mu(h) = t/t^h$ for all $h \in H$. But then $k^h = k\mu(h) = kt/t^h$ implies that $kt \in \mathscr{K} \cap B^H$ and hence that $k = t^{-1}kt \in T^\circ(\mathscr{K} \cap B^H)$. Thus $\mathscr{K} \cap B^L = T^\circ(\mathscr{K} \cap B^H)$ and, as indicated above, this completes the proof.

Lemma 12.5. *$B(K)$ is semisimple if and only if* $\mathrm{usp}(B^H)$ *is semisimple.*

Proof. It is clear that $A = \mathrm{usp}(B^H)$ is a subalgebra of $B(K)$.

Suppose first that $B(K)$ is semisimple and let J be the radical of A. Then J is a characteristic nilpotent ideal of the finite-dimensional algebra A. Now if k is a unit of $B(K)$ giving rise to an element of K, then $K = \mathbf{N}_G(H)$ implies that $k^{-1}(B^H)k = B^H$ and hence that $k^{-1}Jk = J$. Since $B(K)$ is spanned by such elements k, it follows that $J \cdot B(K) = B(K) \cdot J$ is a two-sided ideal of $B(K)$ which is clearly also nilpotent. Thus since $B(K)$ is semisimple, we have $J = 0$.

Conversely suppose A is semisimple and let I be the radical of $B(K)$. Then since $H \subseteq K$ we see that $B(K)$ and hence I is H-invariant. Moreover $Z = B(H) \subseteq B(K)$. Suppose k is a unit of $B(K)$ giving rise to an element of K. Then $k^{-1}Zk = Z$ implies that kZ is a (Z, Z)-subbimodule of $B(K)$. Moreover Z is a simple ring and k is a unit so kZ is therefore a simple (Z, Z)-bimodule. Since $B(K)$ is the linear span of all such k, we see that $B(K) = \sum_k kZ$ and hence that $B(K) = \bigoplus k_iZ$, a direct sum of certain of these simple subbimodules.

Now suppose $I \neq 0$. For each $w \in I \setminus 0$ and direct sum $B(K) = \bigoplus k_iZ$ as above, we look at the number of nonzero components of w written in this decomposition. We now choose w and the decomposition $B(K)=\bigoplus k_i Z$ so that this number, say n, is minimal. In particular if we write $w=\sum k_i z_i$ with $z_i \in Z$, then precisely n of the z_i are nonzero and say $z_1 \neq 0$. Now $\bigoplus k_1^{-1} k_i Z$ is also a decomposition of $B(K)$ and, in this decomposition, $\sum k_1^{-1} k_i z_i = k_1^{-1} w \in I$ has the same parameter n. Thus we can replace w by $k_1^{-1} w$ if necessary and assume that $k_1 = 1$. Next, since Z is a simple ring we have $1 \in Z z_1 Z$. Thus since each $k_i Z$ is a (Z,Z)-bimodule, we can clearly replace w by a suitable element of $ZwZ \subseteq I$ to further assume that $z_1 = 1$.

Finally, we observe from Lemma 12.4(i) that each kZ is H-invariant. Thus if $h \in H$, then since $k_1 z_1 = 1$, we see that $w^h - w \in I$ has at most $n-1$ nonzero components in the decomposition $B(K)=\bigoplus k_i Z$. By the minimality of n, we conclude that $w^h = w$ for all $h \in H$ so $w \in B^H$. Furthermore w is nilpotent so $1+w$ is a unit of B^H and hence $w \in \operatorname{usp}(B^H)=A$. We have therefore shown that $I \cap A \neq 0$. But $A \subseteq B(K)$ so $I \cap A$ is a nilpotent ideal of the semisimple ring A and we obtain the necessary contradiction.

In view of Lemma 12.2 and the above, we see that $B(K)$ is semisimple if and only if B^H is semisimple.

We recall some definitions from Section 1 as applied to the present situation. If K is an M-subgroup of G, then K can be completed to an N-subgroup $\tilde{K}$ of G by adjoining to K the action of all units of $B(K)$. Thus clearly $B(K)=B(\tilde{K})$ and furthermore $R^K = R^{\tilde{K}}$ since any element of R fixed by K is fixed by all units of $B(K)$. We say that H is *almost normal* in G if for $K = \mathbb{N}_G(H)$ we have $\tilde{K}=G$. Finally R^H/R^G is N-group Galois if $\mathcal{G}(R^H/R^G)$ is an N-group of automorphisms of the prime ring R^H with fixed ring equal to R^G. We now prove Theorem D.

Theorem 12.6. *Let G be an N-group of automorphisms of the prime ring R and let H be an F-subgroup of G. Then R^H is N-group Galois over R^G if and only if H is almost normal in G.*

Proof. Suppose first that R^H is N-group Galois over R^G. Then $\operatorname{usp}(B^H)$ is semisimple by Lemma 12.3 and hence so is $B(K)$ by Lemma 12.5. Thus K is an M-subgroup of G and we let $\tilde{K}$ denote its completion. In particular $\tilde{K}$ is an N-subgroup of G with $R^K = R^{\tilde{K}}$. Now by assumption and Proposition 12.1, we have

$$R^G = (R^H)^{K/H} = R^K = R^{\tilde{K}}.$$

Thus Theorem 4.3 applied to $\tilde{K}$ yields $\tilde{K}=G$ and H is almost normal.

Conversely, suppose H is almost normal in G. In particular, $B(K)=B$ is semisimple and hence so is $\operatorname{usp}(B^H)$ by Lemma 12.5. Thus by Lemma 12.3, $B_{R^H}(K/H)=\operatorname{usp}(B^H)$ is a semisimple finite-dimensional algebra over the extended centroid of R^H and every unit of this algebra gives rise to an X-inner automorphism of R^H. Moreover, since G is the completion of K we have

$$(R^H)^{K/H} = R^K = R^G.$$

It remains to show that the X-inner automorphisms have finite index in K/H.

We now apply the notation and result of Lemma 12.4(ii). Then $[\mathscr{K}:\mathscr{H}(\mathscr{K}\cap B^H)]<\infty$ and this implies that $[K_0:H_0K_1]<\infty$ where $K_0=K\cap \operatorname{Inn} R$, $H_0=H\cap \operatorname{Inn} R$ and where K_1 is the image of $\mathscr{K}\cap B^H$ in $\operatorname{Aut}(R)$. But, by Lemma 12.3, every element of K_1 gives rise to an X-inner automorphism of R^H. Hence since $\mathscr{G}(R^H/R^G)=K/H$ and $[K:K_0]<\infty$ we conclude that the X-inner automorphisms in $\mathscr{G}(R^H/R^G)$ are indeed a subgroup of finite index and the theorem is proved.

We remark that normal F-subgroups are rather scarce while almost normal ones are plentiful. For example suppose G is an X-inner F-group so that B is simple. Since the group of units of B is a general linear group and hence close to simple, we see that G has few normal subgroups. On the other hand, suppose H is an F-subgroup of G with $Z=B(H)$ having the same center T as that of B. Then it follows that $B=Z\otimes_T \mathbb{C}_B(Z)$. Hence if $\mathbb{C}_B(Z)$ is spanned by its units and $K=\mathbb{N}_G(H)$, we conclude that $B(K)=B$ so H is almost normal in G.

13. Examples

In this final section we discuss a few interesting examples. In all cases, R is a matrix ring over a domain and in fact the domain is either a field K or a noncommutative free algebra. We note that if $F=K\langle x_1,x_2,\dots\rangle$ is such an algebra, then F is a domain with extended centroid K and with no nonidentity X-inner automorphisms.

We begin with three examples related to the existence of trace forms, the third one being due to G.M. Bergman. Recall that the dual group $B^*=\operatorname{Hom}(B,C)$ is a right B-module.

Example 13.1. Let $R=M_n(K)$ and let $G=\operatorname{GL}_n(K)$. Then $B=M_n(K)$ and the map $\theta:B^*\to B$ defined by $\theta(e_{ij}^*)=0$ for $j\neq 1$ and $\theta(e_{i1}^*)=e_{1i}$ is a B-module homomorphism. Here of course $\{e_{ij}\}$ is the set of matrix units of B and $\{e_{ij}^*\}$ is the dual basis of B^*. As in Lemma 2.3, θ yields the well known trace form $\tau(x)=\sum_i e_{i1}xe_{1i}$.

Example 13.2. Let $R=M_2(K)$ with $\operatorname{char} K=p>2$ and let G be the group of inner automorphisms generated by

$$\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix} \quad\text{and}\quad \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}.$$

Then $|G|=2p$ and B is the 3-dimensional K-algebra spanned by e_{11},e_{22} and e_{12}. In particular, B is not semisimple so G is not an M-group. Observe that the map $\theta:B^*\to B$ given by $\theta(e_{11}^*)=0$, $\theta(e_{22}^*)=e_{12}$ and $\theta(e_{12}^*)=e_{11}$ defines a right B-module homomorphism. As in Lemma 2.3, this gives rise to a nontrivial trace form $\tau(x)=e_{22}xe_{12}+e_{12}xe_{11}$.

Example 13.3. Suppose $F=K\langle x,y\rangle$ where char $K=p>2$, let $R=M_2(F)$ and let G be the finite group of inner automorphisms generated by

$$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\quad \begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\quad\text{and}\quad \begin{pmatrix}1 & y\\ 0 & 1\end{pmatrix}.$$

Then $|G|=2p^2$ and $R^G=K$, embedded as scalars. Furthermore, the algebra of the group B is the 4-dimensional K-algebra spanned by e_{11}, e_{22}, xe_{12} and ye_{12}. It is easy to verify directly that there is no nonzero B-module homomorphism $\theta: B^*\to B$. Alternately let I be the ideal of R generated by x and y. Then $I\neq 0$ is G-invariant, but $I\cap R^G=I\cap K=0$. Hence the nonexistence of θ follows from Lemmas 2.3 and 4.6.

The next two examples concern the independence of the four Galois subring conditions, the second being due to Teichmüller. We could of course offer numerous examples to cover other possibilities, but these are the only really interesting cases.

Example 13.4. *Let* $K=\mathrm{GF}(2)$, $R=M_2(K)$, $G=\mathrm{GL}_2(K)\simeq\mathrm{Sym}_3$ and let S be the diagonal subring of R. Then G is an N-group of inner automorphisms, $S\supseteq R^G=K$ and $Z=\mathbb{C}_B(S)=S$. Furthermore, S satisfies [GI], [GH], [GC] and Z is semisimple. However, in spite of Theorem 7.4, we have $H=\mathcal{G}(R/S)=\langle 1\rangle$ and $S\neq R^H=R$. What fails here, of course, is that Z is not spanned by its units.

Example 13.5. Let σ be an automorphism of K of finite order $r\geq 3$ and let $k=K^{\langle\sigma\rangle}$. Set $R=M_2(K)$ and let $G=\langle \mathrm{GL}_2(K),\sigma\rangle$. Then G is an N-group of automorphisms with $B=M_2(K)$ and $R^G=k$. Now let $S=\{\mathrm{diag}(a,a^\sigma)\mid a\in K\}$. Then $S\supseteq R^G$, $Z=\mathbb{C}_B(S)$ is the ring of diagonal matrices and $S\simeq K$. Thus S satisfies [GZ], [GC] and, with a little checking, [GI]. On the other hand, since σ has order ≥ 3, it follows easily that $H=\mathcal{G}(R/S)$ is inner and hence that $R^H=Z>S$. In view of Theorem 7.4 this of course implies that S does not satisfy Galois homogeneity and indeed with $b=\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)\in B$ we have $bs=s^\sigma b$ for all $s\in S$ but $\sigma\notin HG_0$.

This also gives rise to the following observation. The subring K, embedded as scalars, is the fixed ring of $\mathrm{GL}_2(K)$ and hence satisfies [GI] and [GH]. Furthermore the map $\varphi: K\to S$ defined by $a\to\mathrm{diag}(a,a^\sigma)$ is an isomorphism which is the identity on R^G. But $S=K^\varphi$ does not satisfy [GH].

The following two examples show that certain embeddings $\varphi: S\to\bar{S}$ cannot extend to elements of G. The first one fails because the degrees of the corresponding minimal primes do not agree. The second one fails because φ is defined 'differently' on the distinct factors S/P.

Example 13.6. Let $R=M_4(K)$ and $G=\mathrm{GL}_4(K)$ so that $R^G=K$. Set

$$S=\{\mathrm{diag}(a,a,b,b)\mid a,b\in K\}\quad\text{and}\quad \bar{S}=\{\mathrm{diag}(a,b,b,b)\mid a,b\in K\}$$

so that S is the fixed subring of $\mathrm{GL}_2(K)\times\mathrm{GL}_2(K)$ and $\bar{S}$ is the fixed subring of $\mathrm{GL}_1(K)\times\mathrm{GL}_3(K)$. Now $\varphi: S\to\bar{S}$ given by $\varphi:\mathrm{diag}(a,a,b,b)\to\mathrm{diag}(a,b,b,b)$ is surely an isomorphism which is the identity on R^G. But φ cannot extend to an element of G since $\mathbb{C}_R(S)$ and $\mathbb{C}_R(\bar{S})$ are not isomorphic. Indeed the minimal primes of S have degrees $2,2$ while those of $\bar{S}$ have degrees $1,3$.

Example 13.7. Let $\sigma\neq 1$ be an automorphism of K of finite order and let $k=K^{\langle\sigma\rangle}$. Set $R=M_2(K)$ and $G=\langle\mathrm{GL}_2(K),\sigma\rangle$ so that $R^G=k$. If S is the subring of diagonal matrices, then S is the fixed subring of $\mathrm{GL}_1(K)\times\mathrm{GL}_1(K)$. Now define $\varphi: S\to S$ by $\varphi:\mathrm{diag}(a,b)\to\mathrm{diag}(a^\sigma,b)$. It is easy to verify that φ cannot extend to an element $g\in G$. In essence, φ extends to two different elements, one for each of the two prime factor rings S/P.

The remaining two examples show that φ need not be extendible to an element of G even if S is prime and φ extends to $\langle S,Z\rangle$.

Example 13.8. Let $F=K\langle x,y,z\rangle$ be the free algebra over $K\neq\mathrm{GF}(2)$ with generators x,y,z and let Sym_3 act on F by permuting these generators. For definiteness take σ and τ to be the transpositions $\sigma=(xy)$ and $\tau=(yz)$. Now suppose $R=M_2(F)$ and let $G=\mathrm{GL}_2(K)\times\mathrm{Sym}_3$ act on R. Then $R^G=F^{\langle\mathrm{Sym}_3\rangle}$, $C=K$ and hence $B=M_2(K)$.

Now let H be the subgroup of G generated by $\mathrm{GL}_1(K)\times\mathrm{GL}_1(K)$, the diagonal elements in $\mathrm{GL}_2(K)$, and the automorphism $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\sigma$ of order 2. Then $S=R^H=\{\mathrm{diag}(a,a^\sigma)\mid a\in F\}$ and $Z=\mathbb{C}_B(S)$ is the set of diagonal matrices in $M_2(K)$. Observe that H interchanges the two idempotents $e_{11},e_{22}\in Z$, so Z is H-simple.

Define $\varphi: S\to S$ by $\mathrm{diag}(a,a^\sigma)\to\mathrm{diag}(a^\tau,a^{\tau\sigma})$. Observe that this is an isomorphism which is the identity on $R^G\subseteq S$. Furthermore φ can clearly extend to $\varphi:\langle S,Z\rangle\to\langle S,Z\rangle$ by defining φ to be the identity on Z. In view of Theorem 11.3, there exist group elements $g_1,g_2\in G$ with $(e_{ii}s)^{g_i}=e_{ii}s^\varphi$; in fact we can clearly take $g_1=\tau$ and $g_2=\sigma^{-1}\tau\sigma$. On the other hand, $1\in Z$ is the unique H-centrally primitive idempotent of Z and there does not exist $g\in G$ with $s^g=s^\varphi$ for all $s\in S$. Indeed suppose $s^g=s^\varphi$ where $g=g_0\lambda$ with $g_0\in\mathrm{GL}_2(K)$ and $\lambda\in\mathrm{Sym}_3$. Then since K is central, g_0 preserves matrix traces, and we have

$$a^\lambda+a^{\sigma\lambda}=(a+a^\sigma)^\lambda=a^\tau+a^{\tau\sigma}$$

for all $a\in F$. But this yields a vanishing trace form and Sym_3 is X-outer on F. Thus this form must be trivial. In particular we have $\lambda=\sigma\lambda,\tau$ or $\tau\sigma$ and by considering each in turn, using $\sigma\neq 1$ and $\sigma\tau\neq\tau\sigma$, we get a contradiction.

Example 13.9. We modify the above slightly and start with $F=K\langle x,y,u,v\rangle$, $\sigma=(xy)$ and $\tau=(uv)$. Then $G=\mathrm{GL}_2(K)\times\langle\sigma,\tau\rangle$ acts on $R=M_2(F)$ with $B=M_2(K)$ and $R^G=F^{\langle\sigma,\tau\rangle}$. Again let

$$H=\langle\mathrm{GL}_1(K)\times\mathrm{GL}_1(K),\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\sigma\rangle$$

and let

$$\bar{H}=\langle \mathrm{GL}_1(K)\times \mathrm{GL}_1(K), (\begin{smallmatrix}0&1\\1&0\end{smallmatrix})\tau\rangle.$$

Then $S=R^H=\{\mathrm{diag}(a,a^\sigma)\mid a\in F\}$ and $\bar{S}=R^{\bar{H}}=\{\mathrm{diag}(a,a^\tau)\mid a\in F\}$. Clearly $Z=\bar{Z}$ is the set of diagonal matrices in $M_2(K)$ and this ring is both H- and $\bar{H}$-simple. Now define $\varphi: S\to\bar{S}$ by $\mathrm{diag}(a,a^\sigma)\to\mathrm{diag}(a,a^\tau)$. This φ is an isomorphism which is the identity on R^G. Furthermore φ can be extended to an isomorphism $\varphi:\langle S,Z\rangle\to\langle\bar{S},\bar{Z}\rangle$ by defining φ to be the identity on Z.

Here we claim that there is no $g\in G$ with $S^g=S^\varphi=\bar{S}$. More generally suppose $J^g\subseteq\bar{S}$ where $g=g_0\lambda$ with $g_0\in\mathrm{GL}_2(K)$, $\lambda\in\langle\sigma,\tau\rangle$ and where J is an ideal of S. Then we show that $J=0$. Observe that $J=\{\mathrm{diag}(a,a^\sigma)\mid a\in I\}$ for some ideal I of F and hence for each $a\in I$ we have

$$\mathrm{diag}(a,a^\sigma)^{g_0\lambda}=\mathrm{diag}(b,b^\tau)$$

for some $b\in F$. Taking traces as before, this yields $(a+a^\sigma)^\lambda=b+b^\tau$ and since the right hand side is fixed by τ we obtain, for all $a\in I$

$$(a+a^\sigma)^\lambda=(a+a^\sigma)^{\lambda\tau}.$$

If $I\neq 0$, then this yields a vanishing trace form. But observe that $\lambda\in\langle\sigma,\tau\rangle$ and that the latter group is a fours group of X-outer automorphisms of F. We can then consider each of the four possibilities $\lambda=1,\sigma,\tau,\sigma\tau$, in turn, and obtain a contradiction. Thus $I=0$ and $J=0$, as claimed.

Acknowledgement

This paper was begun in January 1982 when the second author was a visitor at the University of Southern California. He would like to thank Prof. W.A. Harris, Jr. and the rest of the Math. Department for their kind hospitality. Research supported in part by NSF Grants MCS 81-01730 and MCS 80-02773.

References

[1] H. Cartan, Théorie de Galois pour les corps non commutatifs, Ann. Sci. École Norm. Sup. (3) 64 (1947) 59–77.
[2] L.N. Childs and F.R. DeMeyer, On automorphisms of separable algebras, Pacific J. Math. 23 (1967) 25–34.
[3] J. Dieudonné, La théorie de Galois des anneaux simples et semi-simples, Comment. Math. Helv. 21 (1948) 154–184.
[4] J.W. Fisher and J. Osterburg, Finite group actions on noncommutative rings: a survey since 1970, in: Ring Theory and Algebra III (Marcel Dekker, New York, 1980) 357–393.
[5] G. Hochschild, Double vector spaces over division rings, Amer. J. Math. 71 (1949) 443–460.
[6] G. Hochschild, Automorphisms of simple algebras, Trans. A.M.S. 69 (1950) 292–301.
[7] N. Jacobson, The fundamental theorem of the Galois theory for quasifields, Ann. of Math. 41 (1940) 1-7.

[8] N. Jacobson, A note of division rings, Amer. J. Math. 69 (1947) 27-36.
[9] N. Jacobson, Structure of Rings, A.M.S. Colloq. Publ. 37 (Amer. Math. Soc., Providence, RI, 1956, revised 1964).
[10] V.K. Kharchenko, Generalized identities with automorphisms, Algebra i Logika 14 (1975) 215-237 (English translation 1976, 132-148).
[11] V.K. Kharchenko, Fixed elements under a finite group acting on a semiprime ring, Algebra i Logika 14 (1975) 328-34 (English translation 1976, 203-213).
[12] V.K. Kharchenko, Galois theory of semiprime rings, Algebra i Logika 16 (1977) 313-363 (English translation 1978, 208-258).
[13] V.K. Kharchenko, Algebras of invariants of free algebras, Algebra i Logika 17 (1978) 478-487 (English translation 1979, 316-321).
[14] H.F. Kreimer, On the Galois theory of separable algebras, Pacific J. Math. 34 (1970) 729-740.
[15] Y. Miyashita, Finite outer Galois theory of noncommutative rings, J. Fac. Sci. Hokkaido Univ. (Ser. I) 19 (1966) 115-134.
[16] S. Montgomery, Fixed Rings of Finite Automorphism Groups of Associative Rings, Lecture Notes in Math. 818 (Springer, Berlin, 1980).
[17] T. Nakayama and G. Azumaya, On irreducible rings, Ann. of Math. (2) 48 (1947) 949-965.
[18] T. Nakayama, Galois theory of simple rings, Trans. A.M.S. 73 (1952) 279-292.
[19] E. Noether, Nichtkommutative Algebra, Math. Z. 37 (1933) 514-541.
[20] A. Rosenberg and D. Zelinsky, Galois theory of continuous linear transformation rings, Trans. A.M.S. 79 (1955) 429-452.
[21] H. Tominaga and T. Nagahara, Galois Theory of Simple Rings, Okayama Math. Lectures (Okayama Univ., 1970).
[22] O.E. Villamayor and D. Zelinsky, Galois theory with infinitely many idempotents, Nagoya Math. J. 35 (1969) 83-98.