ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 14, Number 2, Spring 1984

OUTER GALOIS THEORY OF PRIME RINGS

S. MONTGOMERY AND D.S. PASSMAN

1. Introduction. The purpose of this paper is to present an essentially self-contained account of the Galois theory of a finite group of outer automorphisms of a prime ring R. The major theorems are due to V.K. Kharchenko and are special cases of his more general work [**8**] on the Galois theory of semiprime rings.

The subject of noncommutative Galois theory was begun by E. Noether in 1933 [**17**] in her work on inner automorphisms of simple algebras. In 1940, N. Jacobson [**5**] established a Galois correspondence theorem for a finite group of outer automorphisms of a division ring. H. Cartan [**1**] added to this by proving that automorphisms extend from intermediate rings, thereby obtaining the usual consequences concerning intermediate Galois subrings. Next, T. Nakayama [**15**] and G. Hochschild [**4**] established a Galois theory for outer automorphisms of simple Artinian rings. Complete rings of linear transformations were studied by T. Nakayama and G. Azumaya [**16**] and by J. Dieudonné [**3**], while continuous transformation rings were studied by A. Rosenberg and D. Zelinsky [**18**]. Finally the outer Galois theory of separable algebras was developed by Y. Miyashita [**12**] and H.F. Kreimer [**10**].

The recent work of Kharchenko is a significant advance since it contains a Galois correspondence theorem for N-groups of automorphisms of semiprime rings. To prove this result in its full generality is a long and difficult task. Indeed this is even true of the prime case which is discussed in our earlier paper [**14**]. However, when we further restrict our attention to outer automorphisms of prime rings, a considerable simplification occurs. In addition, our use of trace forms of minimal length replaces both the independence and trace function results developed in Kharchenko's earlier papers [**6, 7**]. Since the outer case is so much shorter and simpler and since it has a number of interesting applications in its own right, it seems worthwhile to present it separately.

1. The bimodule property. Throughout this paper, R will denote a prime ring with 1, G a finite group of automorphisms of R and R^G the fixed ring

Research supported in part by NSF Grants MCS 81–01730 and MCS 80–02773.
Received by the authors on September 27, 1982.

of G on R. In order to discuss what is meant by G being X-outer, we must first introduce the Martindale ring of quotients of R.

Consider all pairs (f, I) where I is a nonzero ideal of R and $f\colon I \to R$ is a left R-module homomorphism. Two pairs (f, I) and (g, J) are said to be equivalent if f and g agree on the common domain $I \cap J$. It is not difficult to check that this is an equivalence relation. The Martindale ring of quotients $Q = Q_0(R)$ is defined to be the set of these equivalence classes. Q is actually a ring with addition corresponding to addition of maps and with multiplication corresponding to function composition. We let $\hat{f}$ denote the equivalence class of (f, I).

For each $r \in R$ let $r_\rho\colon R \to R$ denote right multiplication by r. Then the map $r \to r_\rho$ imbeds R isomorphically into Q and in this way we view R as a subring of Q with the same 1. Furthermore, if $f\colon I \to R$ is a left R-module homomorphism and if $r \in I$, then the maps $r_\rho f$ and $(rf)_\rho$ are both defined on R and are easily seen to be equal. Thus with R appropriately embedded in Q, we have $r\hat{f} = rf$ or, in other words, the map $f\colon I \to R$ actually describes the right multiplication of $r \in I$ by $\hat{f}$. We now summarize some well known properties of Q, many of which follow from the above observation. In any case, the proofs are elementary and can be found for example in **[13]**.

LEMMA 1. *Let $Q = Q_0(R)$ and let C be the center of Q. Then*
i) *Q is a prime ring, C is a field and C is the centralizer of R in Q.*
ii) *For any $q \in Q$ there exists an ideal $I \neq 0$ of R with $Iq \subseteq R$. Furthermore if $q_1, q_2 \in Q\backslash 0$ and if $J \neq 0$ is an ideal of R, then $q_1 J q_2 \neq 0$.*
iii) *If σ is an automorphism of R, then σ extends uniquely to an automorphism of Q.*

The center C of Q is called the extended centroid of R. Although the definition of Q seems somewhat abstract, the ring Q can be computed in a number of important special cases. If R is simple, then $Q_0(R) = R$. If $R = M_n(A)$, the ring of $n \times n$ matrices over the commutative domain A, then $Q_0(R) = M_n(F)$ where F is the field of fractions of A. Finally if R is the complete ring of linear transformations of a vector space over a division ring, then it is known that $Q_0(R) = R$ (see **[13]**).

DEFINITION. Let S be a subring of R with the same 1. We say S has the bimodule property in R if every nonzero (R, S) – or (S, R) – subbi module M of Q contains a nonzero ideal of R and satisfies $M \cap S \neq 0$. It follows immediately from Lemma 1 (ii) that $S = R$ has the bimodule property in R. We will use this observation freely throughout the remainder of this paper.

The next lemma is an extension of an old result of Martindale **[11]**.

LEMMA 2. *Let S be a subring of R satisfying the bimodule property, let*

$\sigma \in \mathrm{Aut}(R)$ and suppose there exist nonzero elements $a, b, a', b' \in Q$ with $asb' = bs^\sigma a'$ for all $s \in S$. Then there exists a unit $q \in Q$ with $aq = b$, $qa' = b'$ and $q^{-1}sq = s^\sigma$ for all $s \in S$.

PROOF. It is clear that S^σ also satisfies the bimodule property. Define f: $RaS \to RbS^\sigma$ and g: $RbS^\sigma \to RaS$ by f: $\sum x_i a y_i \to \sum x_i b y_i^\sigma$ and g: $\sum x_i b y_i^\sigma \to \sum x_i a y_i$ for all $x_i \in R, y_i \in S$. To see that f is well defined, suppose that $0 = \sum x_i a y_i$. Then since $y_i \in S$ we have for all $s \in S$

$$0 = (\textstyle\sum x_i a y_i)\, sb' = (\sum x_i b y_i^\sigma)\, s^\sigma a'.$$

Thus $0 = (\sum x_i b y_i^\sigma) S^\sigma a' R$. Since $S^\sigma a' R$ contains a nonzero ideal of R, we conclude from Lemma 1 (ii) that $0 = \sum x_i b y_i^\sigma$ and f is well defined. Similarly g is well defined.

Since RaS contains a nonzero ideal I of R, f: $I \to R$ is a left R-module homomorphism and hence determines an element $q = \hat{f} \in Q$. Similarly $g: J \to R$ and we have $\hat{g} \in Q$. Furthermore since fg and gf are the identity maps on appropriate ideals we have $\hat{f}\hat{g} = 1 = \hat{g}\hat{f}$. Thus $\hat{g} = q^{-1}$.

Let $s \in S$. Then for $x \in R$, $y \in S$ we have

$$\begin{aligned}(xby^\sigma)\, gs_\rho f &= (xay)\, s_\rho f = (xa(ys))f \\ &= xby^\sigma s^\sigma = (xby^\sigma)(s^\sigma)_\rho.\end{aligned}$$

Thus the maps $gs_\rho f$ and $(s^\sigma)_\rho$ agree on RbS^σ and hence on the nonzero ideal it contains. From this we conclude that

$$q^{-1}sq = gs_\rho f = (s^\sigma)_\rho = s^\sigma.$$

Now let K be a nonzero ideal of R with $Ka \subseteq R$. Then $IKa \subseteq I$ and since f is defined on I we have $xaq = (xa)f = xb$ for all $x \in IK$. Thus $(IK)\cdot(aq - b) = 0$ and, since $IK \neq 0$ in the prime ring R, Lemma 1 (ii) yields $b = aq$. Finally substituting $s^\sigma = q^{-1}sq$ and $b = aq$ in the original formula yields $asb' = asqa'$ for all $s \in S$. Thus $(RaS)(b' - qa') = 0$ and since RaS contains a nonzero ideal of R we conclude that $b' = qa'$.

The automorphisms which occur above give rise to the following.

DEFINITION. An automorphism σ of R is X-inner if there exists a unit q of Q with $r^\sigma = q^{-1}rq$ for all $r \in R$. In other words, σ is X-inner if it becomes inner when extended to Q. Of course if this does not occur then σ is X-outer.

COROLLARY 3. *Let $\sigma \in \mathrm{Aut}(R)$. Then σ is X-inner if and only if there exist $a, b, a', b' \in R\backslash 0$ such that $arb' = br^\sigma a'$ for all $r \in R$.*

PROOF. If $arb' = br^\sigma a'$ for all $r \in R$, then Lemma 2 implies immediately that σ is X-inner. Conversely suppose σ is conjugation by the unit $q \in Q$. By Lemma 1 (ii) there exist a, $b \in R$ with $aq = b \neq 0$. Now $r^\sigma = q^{-1}rq$

yields $rq = qr^\sigma$ for all $r \in R$. Multiplying the latter identity on the left by a and replacing r by ra yields $arb = br^\sigma a^\sigma$.

Thus we have obtained an internal characterization of X-inner automorphisms. Notice that the above condition is right-left symmetric even though the definition of $Q = Q_0(R)$ is decidedly not symmetric.

2. Truncation of trace forms. A trace form is a formal expression in the variable x given by

$$T(x) = \sum_{i=1}^n a_i x^{\sigma_i} b_i$$

where $a_i, b_i \in Q$ and $\sigma_i \in \mathrm{Aut}(R)$. The σ_i need not be distinct. Of course T clearly gives rise to a linear function from R to Q.

For any finitely many elements $r_k, s_k \in R$, we let

$$\tilde{T}(x) = \sum_k T(xr_k)s_k = \sum_{i=1}^n a_i x^{\sigma_i} \tilde{b}_i$$

where $\tilde{b}_i = \sum_k r_k^{\sigma_i} b_i s_k \in Q$. We call any such $\tilde{T}$ obtained in this way a right truncation of T. More generally if S is a subring of R and if we insist that the s_k above belong to S, then $\tilde{T}$ is a right (R, S) – truncation of T.

PROPOSITION 4. *Let S satisfy the bimodule property in R and let $T(x) = \sum_{i=1}^n a_i x^{\sigma_i} b_i$ be a trace form with $b_1 \neq 0$ and $\sigma_1 = 1$. Then there exists a right (R, S) – truncation*

$$\tilde{T}(x) = \sum_k T(xr_k)s_k = \sum_{i=1}^n a_i x^{\sigma_i} \tilde{b}_i$$

of $T(x)$ with $\tilde{b}_1 \in S\backslash 0$. Furthermore for any i with $\tilde{b}_i \neq 0$ there exists a unit $q_i \in Q$ with $\tilde{b}_i = q_i^{-1}\tilde{b}_1$ and with $s^{\sigma_i} = q_i^{-1} s q_i$ for all $s \in S$. In particular if $S = R$, then σ_i is X-inner.

PROOF. We begin with several general remarks. First the a_i's merely play the role of a place holder here. It is of no concern whether they are zero or not. Second for any such $T = \sum_{i=1}^n a_i x^{\sigma_i} b_i$ we let the support of T be the set of subscripts i with $b_i \neq 0$. It is clear that if $\tilde{T}$ is a right (R, S)-truncation of T, then $\mathrm{Supp}\ \tilde{T} \subseteq \mathrm{Supp}\ T$. If $\mathrm{Supp}\ \tilde{T} = \phi$ we say that T is trivial. Third, if T' is a right (R, S) - truncation of $\tilde{T}$, then it is also a right (R, S) - truncation of T. Finally if $b_j \neq 0$ in the above, then the bimodule property implies that $Rb_jS \cap S \neq 0$. Thus there exists $\tilde{T} = \sum_{i=1}^n a_i x^{\sigma_i} \tilde{b}_i$ with $\tilde{b}_j \in S\backslash 0$.

The proof of the proposition proceeds by induction on the support size of T which we may for convenience assume to be n. By the preceding remark we may further assume that $b_1 \in S\backslash 0$. If $n = 1$, the result now follows by taking $q_1 = 1$. Now suppose $n > 1$ and let $\mathcal{T}$ denote the set of all right (R, S) - truncations of T. If $\tilde{T} = \sum a_i x^{\sigma_i} \tilde{b}_i \in \mathcal{T}$ with $|\mathrm{Supp}\ \tilde{T}| < n$, then the result will follow by induction provided that $\tilde{b}_1 \neq 0$. Thus we may assume that all such $\tilde{T} \in \mathcal{T}$ of support size less than n satisfy $\tilde{b}_1 = 0$.

One further reduction is necessary. For each i, there exists a nonzero ideal I_i of R with $I_i b_i \subseteq R$. Thus if $I = \bigcap_i I_i^{\sigma_i^{-1}}$, then $I \neq 0$ and $I^{\sigma_i} b_i \subseteq R$ for all i. In addition, we can choose $r \in I$ with $rb_1 \neq 0$. Then $\tilde{T}(x) = T(xr)$ is a truncation of T with all $\tilde{b}_i \in R$ and $\tilde{b}_1 \neq 0$. We can now assume that T itself has this property and our goal is to show that T satisfies the conclusion of this proposition. As above we may assume $b_1 \in S\backslash 0$.

We first show that if $T' = \sum a_i x^{\sigma_i} b'_i \in \mathscr{T}$ with $|\text{Supp } T'| < n$, then T' is trivial. We already know that $b'_1 = 0$ but suppose $b'_j \neq 0$ for some $j \neq 1$. By truncating T' if necessary we may assume that $b'_j \in S\backslash 0$. Since Sb'_jR contains a nonzero ideal of R, we have $b_1 Sb'_jR \neq 0$ by Lemma 1 (ii). Thus there exists $s \in S$ with $b_1 s b'_j \neq 0$. For this $s \in S$ let

$$\begin{aligned}\tilde{T}(x) &= T(x)sb'_j - T'(xb_j^{\sigma_j^{-1}} s^{\sigma_j^{-1}}) \\ &= \textstyle\sum_{i=1}^n a_i x^{\sigma_i} \tilde{b}_i \in \mathscr{T}.\end{aligned}$$

Here $\tilde{b}_i = b_i s b'_j - b_j^{\sigma_j^{-1}\sigma_i} s^{\sigma_j^{-1}\sigma_i} b'_i$. Hence since $b'_1 = 0$, we have $\tilde{b}_1 = b_1 s b'_j \neq 0$ by the choice of s. On the other hand, the above formula clearly yields $\tilde{b}_j = 0$ and this contradicts the assumed property of $\mathscr{T}$. Thus all nontrivial elements of $\mathscr{T}$ have support size n.

Finally we return to T itself. For any $s \in S$, let

$$\tilde{T}(x) = T(xb_1 s) - T(x)sb_1 = \textstyle\sum_{i=1}^n a_i x^{\sigma_i} \tilde{b}_i.$$

Then $\tilde{T} \in \mathscr{T}$ since $b_1 \in S$ and $\tilde{b}_i = b_1^{\sigma_i} s^{\sigma_i} b_i - b_i s b_1$. Since $\sigma_1 = 1$ we have $\tilde{b}_1 = 0$ and therefore $\tilde{T}$ must be trivial. Thus for all i and all $s \in S$ we have $b_i s b_1 = b_1^{\sigma_i} s^{\sigma_i} b_i$. Applying Lemma 2, there exists a unit $q_i \in Q$ with $s^{\sigma_i} = q_i^{-1} s\, q_i$ for all $s \in S$ and with $q_i b_i = b_1$. The result follows.

Similarly, suppose $T(x) = \sum_{i=1}^n a_i x^{\sigma_i} b_i$ is a trace form and that we have the finitely many elements $s_k \in S$, $r_k \in R$. Then the trace form

$$\tilde{T}(x) = \textstyle\sum_k s_k T(r_k x) = \sum_{i=1}^n \tilde{a}_i x^{\sigma_i} b_i$$

where $\tilde{a}_i = \sum_k s_k a_i r_k^{\sigma_i}$ is called a left (S, R) - truncation of T.

PROPOSITION 4′. *Let S satisfy the bimodule property in R and let $T(x) = \sum_{i=1}^n a_i x^{\sigma_i} b_i$ be a trace form with $a_1 \neq 0$ and $\sigma_1 = 1$. Then there exists a left (S, R) - truncation*

$$\tilde{T}(x) = \textstyle\sum_k s_k T(r_k x) = \sum_{i=1}^n \tilde{a}_i x^{\sigma_i} b_i$$

of $T(x)$ with $\tilde{a}_1 \in S\backslash 0$. Furthermore for any i with $\tilde{a}_i \neq 0$ there exists a unit $q_i \in Q$ with $\tilde{a}_i = \tilde{a}_1 q_i$ and with $s^{\sigma_i} = q_i^{-1} s q_i$ for all $s \in S$. In particular if $S = R$, then σ_i is X-inner.

PROOF. Since the bimodule property and Lemma 2 are both right-left symmetric, an obvious modification of the previous argument, with one exception, yields the result. The exception concerns the proof that we can take the coefficients a_i to be in R. However, this can be achieved as follows.

Given $T(x) = \sum_1^n a_i x^{\sigma_i} b_i$ with $a_1 \neq 0$, there exists a nonzero ideal I of R with $Ia_i \subseteq R$ for all i. Observe that I is an (S, R)-bimodule and S satisfies the bimodule property so $I \cap S \neq 0$. Furthermore, Sa_1R is a nonzero (S, R)-bimodule so it contains a nonzero ideal of R and hence $\ell_R(Sa_1R) = 0$. Therefore $(I \cap S) \cdot (Sa_1R) \neq 0$ and we have shown that $(I \cap S)a_1 \neq 0$. Finally choose $s \in I \cap S$ with $sa_1 \neq 0$. Then $\tilde{T}(x) = sT(x)$ is a left (S, R)-truncation of T with all $\tilde{a}_i \in R$ and $\tilde{a}_1 \neq 0$. With this observation, the proof goes through and the result follows.

As a consequence we see that certain trace forms are nontrivial as functions.

COROLLARY 5. *Let $T(x) = \sum_{i=1}^n a_i x^{\sigma_i} b_i$ be a trace form and let I be a nonzero ideal of R. Suppose that for some subscript j we have $a_j \neq 0$, $b_j \neq 0$ and $\sigma_j^{-1}\sigma_i$ is X-outer for all $i \neq j$. Then $T(I) \neq 0$.*

PROOF. For convenience, we may assume that $j = 1$. Furthermore, replacing $T(x)$ by $T(x^{\sigma_1^{-1}})$ and I by I^{σ_1} if necessary, we may assume that $\sigma_1 = 1$. The hypothesis now asserts that $a_1 \neq 0, b_1 \neq 0$ and σ_i is X-outer for all $i \neq 1$. If $T(I) = 0$ and if $\tilde{T}(x)$ is any right (R, R) - truncation of T, then clearly $\tilde{T}(I) = 0$. Now let $\tilde{T}$ be given by Proposition 4 using $S = R$. Then by deleting zero terms we have clearly $\tilde{T}(x) = a_1 x \tilde{b}_1$ for some $\tilde{b}_1 \neq 0$. But then $\tilde{T}(I) = a_1 I \tilde{b}_1 \neq 0$ by Lemma 1 (ii) and thus we must have $T(I) \neq 0$.

3. Galois Correspondence. As we will see, the results of the previous section have a number of lovely, yet immediate, consequences.

DEFINITION. Let G be a group of automorphisms of the prime ring R. We say that G is X-outer if all the nonidentity elements of G are X-outer. Of course the identity map is always X-inner.

If G is a finite group of automorphisms of R, we define the G-trace $t_G(x)$ to be $t_G(x) = \sum_{g \in G} x^g$. Then $t_G(x)$ is a trace form and clearly $t_G(R) \subseteq R^G$.

For the remainder of this paper, G will denote a finite group of X-outer automorphisms of the prime ring R.

PROPOSITION 6. *If I is a nonzero ideal of R, then $I \cap R^G \neq 0$.*

PROOF. Replacing I by $\bigcap_{g \in G} I^g \neq 0$ if necessary, we may assume that I is G-invariant. But then $t_G(I) \subseteq I \cap R^G$. Since $t_G(I) \neq 0$ by Corollary 5, the result follows.

PROPOSITION 7. *The centralizer of R^G in Q is precisely C, the extended* *centroid of R. In particular, the only X-inner automorphism of R which fixes R^G elementwise is the identity map.*

PROOF. Certainly $\mathbf{C}_Q(R^G) \supseteq \mathbf{C}_Q(R) = C$. Conversely let $a \in \mathbf{C}_Q(R^G)$ and suppose $a \neq 0$. Since $t_G(R) \subseteq R^G$ we have $at_G(r) = t_G(r)a$ for all $r \in R$. In other words, if $T(x)$ is defined by $T(x) = \sum_{g \in G} ax^g - \sum_{g \in G} x^g a$, then $T(R) = 0$. Furthermore if T is any right (R, R) - truncation of T, then also $\tilde{T}(R) = 0$. In particular this applies if $\tilde{T}$ is the form given by Proposition 4. Deleting zero terms if necessary, we see that $\tilde{T}(x) = axb - 1xb'$ for some $b, b' \in Q$, not both zero. But then $\tilde{T}(R) = 0$ implies first that both b, b' are not zero and then, by Lemma 2 with $S = R$, that there exists a unit $q \in Q$ with $q^{-1}rq = r$ for all $r \in R$ and $a = 1 \cdot q = q$. Thus $a = q \in \mathbf{C}_Q(R) = C$.

DEFINITION. If S is a subring of R we let $\mathscr{G}(R/S)$ be the group of all automorphisms of R fixing S elementwise. We say that R/S is Galois if $R^{\mathscr{G}(R/S)} = S$.

We can now obtain the first of Kharchenko's theorems.

THEOREM A. (Galois group). *Let G be a finite group of X-outer automorphisms of the prime ring R. Then $\mathscr{G}(R/R^G) = G$.*

PROOF. Certainly $\mathscr{G}(R/R^G) \supseteq G$. Conversely let $\sigma \in \mathscr{G}(R/R^G)$. Since $t_G(R) \subseteq R^G$, it follows that the trace form

$$\begin{aligned} T(x) &= \left(\textstyle\sum_{g \in G} x^g\right)^\sigma - \left(\textstyle\sum_{g \in G} x^g\right) \\ &= \textstyle\sum_{g \in G} x^{g\sigma} - \textstyle\sum_{g \in G} x^g \end{aligned}$$

vanishes on R. Since the automorphism $g = 1$ occurs in T, it follows from Corollary 5 that at least one other automorphism appearing in T is X-inner. But all $g \in G \backslash 1$ are X-outer, by assumption. Thus there exists $g \in G$ with $g\sigma$ X-inner. Since $g\sigma$ clearly fixes R^G it follows from Proposition 7 that $g\sigma = 1$ and we conclude that $\sigma = g^{-1} \in G$.

We can now begin our study of the intermediate rings, that is the rings S with $R \supseteq S \supseteq R^G$.

COROLLARY 8. *Let S be* a *subring of R containing R^G. Then $\mathscr{G}(R/S)$ is* a *subgroup of G. Hence R/S is Galois if and only if $S = R^H$ for some subgroup $H \subseteq G$.*

PROOF. Since $S \supseteq R^G$, Theorem A implies that $H = \mathscr{G}(R/S)$ is a subgroup of G. Hence if R/S is Galois, then $S = R^{\mathscr{G}(R/S)} = R^H$. Conversely if $S = R^H$, then surely R/S is Galois.

PROPOSITION 9. *Let S be a subring of R containing R^G. Then*

i) *S is prime.*

ii) *S satisfies the bimodule property in R.*
iii) *If $H = \mathscr{G}(R/S)$, then S contains* a *nonzero ideal of R^H.*

PROOF. (i). Suppose $a, b \in S$ with $aSb = 0$. Since $S \supseteq R^G$ this implies that

$$T(x) = a(\textstyle\sum_{g\in G} x^g)b = \sum_{g\in G} ax^g b$$

vanishes on R. By Corollary 5, either $a = 0$ or $b = 0$.

(ii). Let $M \neq 0$ be an (S, R) - subbimodule of Q and choose $m \in M\backslash 0$. Since $S \supseteq R^G$ it follows that $t_G(R)m \subseteq R^G M \subseteq M$. Thus if $T(x) = \sum_{g\in G} x^g m$, then $T(R) \subseteq M$. Furthermore, since $MR \subseteq M$ it follows that if $\tilde{T}(x)$ is any right (R, R) - truncation of T, then $\tilde{T}(R) \subseteq M$. Now let $\tilde{T}(x)$ be given by Proposition 4. Then by deleting zero terms, we have clearly $\tilde{T}(x) = x\tilde{b}$ for some $\tilde{b} \in R\backslash 0$. Thus $R\tilde{b} \subseteq M$ and M contains the nonzero ideal $I = R\tilde{b}R$. Furthermore we have $I \cap R^G \neq 0$ by Proposition 6 and hence $M \cap S \supseteq I \cap S \neq 0$. A similar argument using Proposition 4′ works for (R, S) - bimodules.

(iii). Let $T(x) = t_G(x)$ so that $T(R) \subseteq R^G \subseteq S$. Hence if $\tilde{T}(x)$ is any right (R, S) - truncation of T, then clearly $\tilde{T}(R) \subseteq S$. By the above, S satisfies the bimodule property so we can let $\tilde{T}(x) = \sum_{g\in G} x^g \tilde{b}_g$ be the right (R, S) - truncation of T given by Proposition 4. If $\tilde{b}_g \neq 0$, then there is a unit $q_g \in Q$ with $s^g = q_g^{-1} s q_g$ for all $s \in S$. But $S \supseteq R^G$ so q_g centralizes R^G and hence S, by Proposition 7. By deleting zero terms if necessary it follows that $\tilde{T}(x) = \sum_{h\in H} x^h \tilde{b}_h$ where $H = \mathscr{G}(R/S) \subseteq G$ and therefore $\tilde{T}(rx) = r\tilde{T}(x)$ for all $r \in R^H$. It now follows from Corollary 5 that $I = \tilde{T}(R)$ is a nonzero left ideal of R^H contained in S. Similarly, using Proposition 4′, there exists a nonzero right ideal J of R^H contained in S. Finally since S is prime, ISJ is a nonzero two-sided ideal of R^H contained in S.

DEFINITION. We say that S is an ideal-cancellable subring of R if for all nonzero ideals I of S, $Ir \subseteq S$ for $r \in R$ implies $r \in S$.

We now obtain Kharchenko's main theorem.

THEOREM B. (Correspondence). *Let G be a finite group of X-outer automorphisms of the prime ring R. Then the map $H \to R^H$ gives a one-to-one correspondence between the subgroups of G and the ideal-cancellable subrings S with $R \supseteq S \supseteq R^G$.*

PROOF. Let H be a subgroup of G. We first show that $S = R^H$ is ideal-cancellable. Let I be a nonzero ideal of S. Since S satisfies the bimodule property, by Proposition 9 (ii), RI contains a nonzero ideal of R. Since R is prime we conclude that $r_R(I) = 0$. Now suppose $Ir \subseteq S$. If $h \in H$ and $s \in I$, then $sr \in S$ so $sr = (sr)^h = s^h r^h = sr^h$ and $I(r - r^h) = 0$. Thus $r = r^h$ for all $h \in H$ and $r \in R^H = S$.

Conversely suppose $S \supseteq R^G$ is ideal-cancellable. Then by Proposition 9(iii), S contains a nonzero ideal I of R^H where $H = \mathscr{G}(R/S)$. Thus I is also an ideal of $S \subseteq R^H$ and if $r \in R^H$ then $Ir \subseteq I \subseteq S$. We conclude from the ideal-cancellable property that $r \in S$ and thus $S = R^H$. Finally, by Theorem A, the map $H \to R^H$ is one-to-one so the result follows.

We remark that the ideal-cancellable property can be restated in terms of the Martindale ring of quotients. Indeed if $S \supseteq R^G$ it can be shown that $Q_0(S)$ is contained naturally in $Q_0(R)$. With this embedding, S is ideal-cancellable if and only if $S = Q_0(S) \cap R$.

4. Galois extensions of the fixed ring. In order to obtain the usual results about normal subgroups and Galois extensions of R^G, we first require a result on extending automorphisms. This was stated by Kharchenko for free algebras [9], but his proof can be adjusted to work for prime rings in general.

THEOREM C. (Extension). *Let G be a finite group of X-outer automorphisms of a prime ring R and let S be a subring containing R^G. If ϕ: $S \to R$ is any monomorphism fixing R^G, then ϕ is the restriction of some $g \in G$.*

PROOF. Let $H = \mathscr{G}(R/S) \subseteq G$ and let M be the set of all finite sums $\sum_k r_k s_k$ such that $r_k \in R$, $s_k \in S$ and $\sum_k r_k^g s_k = 0$ for all $g \in G\backslash H$. Then M is clearly an (R, S) - subbimodule of R. Set $T(x) = t_G(x)$.

We first show that there exists an element $w \in G$ and $m = \sum_k r_k s_k \in M$ with $m \neq 0$ and with $\sum_k r_k s_k^{\phi w^{-1}} \neq 0$ (in fact, it is precisely this element $w \in G$ which, when restricted to S, will agree with ϕ). Since S satisfies the bimodule property in R, let $\tilde{T}$ be the right (R, S) - truncation of T given by Proposition 4. Thus $\tilde{T}(x) = \sum_k T(xr_k)s_k = \sum_g x^g \tilde{b}_g$ with $r_k \in R$ and $s_k \in S$. Furthermore, as we observed earlier, if $\tilde{b}_g \neq 0$ then there exists a unit $q_g \in Q$ with $s^g = q_g^{-1} s q_g$. But then q_g centralizes R^G, so q_g centralizes S, by Proposition 7, and hence $g \in H$. Thus $\sum_k r_k s_k = \tilde{b}_1 \neq 0$ but for all $g \in G\backslash H$ we have $\sum_k r_k^g s_k = \tilde{b}_g = 0$. In other words, $m = \tilde{b}_1 \in M$ and $m \neq 0$. Furthermore by Corollary 5 there exists $r \in R$ with $0 \neq \tilde{T}(r) = \sum_k T(rr_k)s_k$. Since ϕ is a monomorphism fixing R^G and $T(rr_k) \in R^G$ we can therefore apply ϕ to conclude that $0 \neq \sum_k T(rr_k)s_k^\phi$. In other words, if $T'(x)$ is defined by $T'(x) = \sum_k T(xr_k)s_k^\phi = \sum_g x^g b'_g$ then $T'(R) \neq 0$. Hence surely some coefficient say b'_w is not zero. Since $b'_w = \sum_k r_k^w s_k^\phi$, this fact follows by applying w^{-1} to the expression $0 \neq \sum_k r_k^w s_k^\phi$.

Now for each $g \in G$ was define a map f_g: $M \to R$ by f_g: $\sum_k r_k s_k \to \sum_k r_k s_k^{\phi g^{-1}}$. To see that each f_g is well defined, suppose $\sum_k r_k s_k = 0$. Thus since H fixes S we have $0 = (\sum_k r_k s_k)^h = \sum_k r_k^h s_k$ for all $h \in H$ and hence, by definition of M, we have $0 = \sum_k r_k^g s_k$ for all $g \in G$. It follows that if $\tilde{T}(x)$ is defined by $\tilde{T}(x) = \sum_k T(xr_k)s_k = \sum_g x^g \tilde{b}_g$ then $\tilde{b}_g = 0$ for all $g \in G$. Thus surely, for all $r \in R$, we have $0 = \tilde{T}(r) = \sum_k T(rr_k)s_k$. Again $T(rr_k) \in$

$R^G \subseteq S$ so applying ϕ to the expression yields $0 = \sum_k T(rr_k)s_k^\phi$. In other words, if $T'(x)$ is defined by $T'(x) = \sum_k T(xr_k)s_k^\phi = \sum_g x^g b'_g$ then $T'(R) = 0$. Corollary 5 now implies that for all $g \in G$, $0 = b'_g = \sum_k r_k^g s_k^\phi$ and, by applying g^{-1}, we conclude that f_g is well defined. Note that f_g is clearly a left R-module homomorphism.

Since S satisfies the bimodule property and M is a nonzero (R, S)-subbimodule of R, we see that M contains a nonzero ideal I of R. Thus each f_g: $M \to R$ determines an element $\hat{f}_g$ of Q. Now let $m \in M$ and $w \in G$ be the elements given in the second paragraph of the proof and set $f = f_w$ and $q = \hat{f}$. Then the properties of m and w assert precisely that $mf \neq 0$. Furthermore since $0 \neq I(mf) = (Im)f \subseteq If$, we see that $q = \hat{f} \neq 0$. Now let $s \in S$ and let $\sum_k r_k s_k$ be any element of M. Then using ρ to denote right multiplication we have

$$\begin{aligned}(\textstyle\sum_k r_k s_k) s_\rho f &= (\textstyle\sum_k r_k (s_k s))f = \textstyle\sum_k r_k (s_k s)^{\phi w^{-1}} \\ &= (\textstyle\sum_k r_k s_k^{\phi w^{-1}}) s^{\phi w^{-1}} = (\textstyle\sum_k r_k s_k)f \cdot (s^{\phi w^{-1}})_\rho.\end{aligned}$$

Thus since $M \supseteq I$ it follows that

$$sq = s\hat{f} = \hat{f}s^{\phi w^{-1}} = qs^{\phi w^{-1}}$$

for all $s \in S$. But again ϕw^{-1} fixes $R^G \supseteq S$ so $q \in \mathbf{C}_Q(R^G) = C$, by Proposition 7. Since C is a field central in Q and $q \neq 0$, we can cancel q to conclude that $s = s^{\phi w^{-1}}$ for all $s \in S$. In other words, ϕ is the restriction of $w \in G$.

Using the above, we can now obtain analogs of the classical results characterizing the intermediate rings which are Galois over R^G. These do not appear explicitly in Kharchenko's work.

THEOREM D. (Intermediate rings). *Let G be a finite group of X-outer automorphisms of a prime ring R and let S be a subring of R containing R^G. Then S is Galois over R^G if and only if S is G-stable. Moreover, when this occurs then $H = \mathcal{G}(R/S)$ is normal in G, $\mathcal{G}(S/R^G) = G/H$ and $\mathcal{G}(S/R^G)$ is X-outer on S.*

PROOF. Let $K = \{g \in G \mid S^g = S\}$ be the stabilizer of S in G so that K is a subgroup of G containing $H = \mathcal{G}(R/S)$. By restriction, K acts on S fixing R^G and hence we have a homomorphism $K \to \mathcal{G}(S/R^G)$. The kernel of this map is clearly H and hence H is a normal subgroup of K. Furthermore if $\phi \in \mathcal{G}(S/R^G)$, then ϕ is an automorphism of S fixing R^G and Theorem C implies that ϕ is the restriction of some $g \in G$. Clearly this g stablizes S so $g \in K$ and the map $K \to \mathcal{G}(S/R^G)$ is onto. Thus we see that $\mathcal{G}(S/R^G) = K/H$.

Next we observe that K/H is X-outer on the prime ring S. Indeed if $g \in K$ induces an X-inner automorphism on S, then by Corollary 3 there exist a, b, a', $b' \in S\backslash 0$ with $asb' = bs^g a'$ for all $s \in S$. But S satisfies the bimodule property, by Proposition 9 (ii), so Lemma 2 applies. We conclude that there exists a unit $q \in Q$ with $q^{-1}sq = s^g$ for all $s \in S$. This implies that $q \in \mathbf{C}_Q(R^G) = C$, so g acts trivially on S and hence $g \in H$.

Now suppose that S is G-stable so that $K = G$. Then $H \lhd G$, $\mathscr{G}(S/R^G) = G/H$ is X-outer on S and $S^{G/H} \subseteq (R^H)^{G/H} = R^G$. Thus $S^{G/H} = R^G$ and S is Galois over R^G.

Conversely suppose S is Galois over R^G. By Proposition 9 (iii), S contains a nonzero ideal I of R^H. Furthermore we know that

$$R^G = S^{\mathscr{G}(S/R^G)} = S^{K/H} = S^K$$

and that K/H is X-outer on S. Thus by Proposition 6, $I \cap R^G = I \cap S^{K/H}$ is a nonzero ideal of R^G. Finally since $R^K \subseteq R^H$ we have $IR^K \subseteq S$ and hence $(I \cap R^G)R^K \subseteq S^K = R^G$. But R^G is ideal-cancellable in R, by Theorem B, so this yields $R^K \subseteq R^G$ and hence $R^K = R^G$. By Theorem B again we have $K = G$ and S is G-stable.

We remark that in the above situation, the normalizer of H can be strictly larger than the stablizer of S. Thus it is possible for H to be normal in G but with S/R^G not Galois. We close this section with

COROLLARY 10. *Let H be* a *subgroup of G. Then R^H is Galois over R^G if and only if H is normal in G.*

PROOF. If σ is an automorphism of R and S is a subring of R then it follows easily that $\mathscr{G}(R/S^\sigma) = \mathscr{G}(R/S)^\sigma$. Thus Theorem A implies that the stablizer of R^H is the normalizer of H. Hence Theorem D yields the result.

5. Applications. In this final section we briefly discuss several applications of the outer Galois theory.

We first consider simple rings. As we noted in §1, if R is simple, then $Q_0(R) = R$ and X-outer is just outer in the usual sense. The next lemma was originally proved using the Morita theorems, independently by the first author and J. Osterburg; see [**13**, Theorem 2.5]. The present argument is more elementary.

LEMMA 11. *Let G be* a *finite group of outer automorphisms of the simple ring R. Then R^G is simple if and only if R contains an element of trace* 1, *that is if and only if* $1 \in t_G(R)$.

PROOF. Observe that t_G: $R \to R^G$ is clearly an (R^G, R^G) – bimodule homomorphism and thus $t_G(R)$ is an ideal of R^G. Suppose first that R^G is simple. Since $t_G(R) \neq 0$, by Corollary 5, and R^G is simple, we have $t_G(R) = R^G$ and hence $1 \in t_G(R)$.

Conversely suppose $1 \in t_G(R)$ and let I be a nonzero ideal of R^G. Then IR is a nonzero (R^G, R)-subbimodule of R. But R^G satisfies the bimodule condition, by Proposition 9 (ii), and R is simple, so we conclude that $IR = R$. Finally we have $1 \in t_G(R) = t_G(IR) = I \cdot t_G(R) \subseteq I$ so $I = R^G$ and R^G is simple.

THEOREM 12. *Let G be a finite group of outer automorphism of the simple ring R and suppose that $1 \in t_G(R)$. Then the map $H \to R^H$ gives a one-to-one correspondence between the subgroups of G and the intermediate rings $S \supseteq R^G$. In particular there are only finitely many intermediate rings and they are all simple.*

PROOF. If H is a subgroup of G, let Λ be a left transversal for H in G and define $t_\Lambda(x) = \sum_{g \in \Lambda} x^g$. Since $\Lambda H = G$ we conclude that $t_G(x) = t_H(t_\Lambda(x))$ and hence that $t_G(R) \subseteq t_H(R)$. In particular, we now know that $1 \in t_H(R)$ and hence that R^H is simple, by Lemma 11.

Now let $S \supseteq R^G$ be any intermediate ring and let $H = \mathscr{G}(R/S) \subseteq G$. By Proposition 9 (iii), S contains an ideal of R^H. But R^H is simple so we conclude that $S = R^H$. The result follows from Theorem B.

The hypothesis that R contains an element of trace 1 is trivially satisfied if $|G|^{-1} \in R$ or if R is a division ring. Indeed if R is a division ring, then so is R^G and Lemma 11 yields this fact. Thus the Galois correspondence for fields is a consequence of Theorem 12, as is Jacobson's correspondence theorem [5] for division rings. More generally if R is simple Artinian and G is outer, there always exists an element of trace 1, as the following lemma shows. Therefore the Galois correspondence of [4] and [15] can also be recovered from Theorem 12.

LEMMA 13. *Let R be a simple Artinian ring and G a finite group of outer automorphisms of R. Then R^G is simple Artinian and $1 \in t_G(R)$.*

PROOF. By Proposition 9, we know that R^G is prime and satisfies the bimodule property. Now $I = t_G(R)$ is a nonzero ideal of R^G by Corollary 5; thus the (R^G, R)-bimodule IR contains an ideal of R. Since R is simple, $IR = R$ and hence $\ell_R(I) = 0$.

To show that R^G is Artinian, we first prove that if K is any non-zero right ideal of R^G, then K contains a non-zero minimal right ideal of R^G. Since $R = M_n(D)$, the ring of $n \times n$ matrices over the division ring D, we can choose $a \in K$, $a \neq 0$ to have minimal rank as a matrix in R. Then aI is a nonzero minimal right ideal of R^G. To see that it is minimal, choose $b \in aI$, $b \neq 0$. Then $bR \subseteq aIR = aR$, and so $aR = bR$ by the minimality of the rank of a. Applying the trace, $aI = a \cdot t_G(R) = b \cdot t_G(R) \subseteq bR^G$. Thus aI is minimal.

Now in any semiprime ring, a minimal one-sided ideal is generated by an idempotent. Thus if K_1 is a minimal right ideal of R^G, then $K_1 = e_1R^G$ for some idempotent e_1 and $R^G = e_1R^G \oplus (1 - e_1)R^G$. Assuming $(1 - e_1)R^G \neq 0$ we can find a minimal right ideal e_2R^G contained in $(1 - e_1)R^G$

and with $R^G = e_1R^G \oplus e_2R^G \oplus (1 - e_1 - e_2)R^G$. We continue in this manner and observe that the procedure must stop after at most n steps, since $R = M_n(D)$ cannot contain more than n mutually orthogonal idempotents. Thus R^G is a finite sum of minimal right ideals, so it is Artinian. Finally since R^G is prime and Artinian, it is simple Artinian by Wedderburn's theorem. Thus since $I = t_G(R)$ is a nonzero ideal of R^G, we have $t_G(R) = R^G$ and $1 \in t_G(R)$.

In closing, we mention some applications to free algebras. Let $F = k\langle x_1, \ldots, x_n\rangle$ denote the free algebra over the field k generated by the variables $x_1, \ldots, x_n$. A group $G \subseteq \mathrm{Aut}_k(F)$ is said to be linear on F if each $g \in G$ is determined by a k-linear transformation of the k-vector space spanned by $x_1, \ldots, x_n$. If all such linear transformations $g \in G$ are scalars, that is determined by multiplication by nonzero elements of k, then we say G is scalar on F.

Some basic properties here are as follows. First, any group $G \subseteq \mathrm{Aut}_k F$ is X-outer on F. Second, if G is linear on F, then F^G is a free k-algebra. Finally, if S is a free subalgebra of F, then S is ideal-cancellable in F. The latter two are consequences of P.M. Cohn's weak algorithm. By combining these ingredients with the main theorems stated in this paper, we obtain the following result of Kharchenko [9].

THEOREM 14. *Let G be a finite linear group of automorphisms of the free algebra $F = k\langle x_1, \ldots, x_n\rangle$. Then the map $H \to F^H$ gives a one-to-one correspondence between the subgroups H of G and the free intermediate algebras $S \supseteq F^G$. In particular there are only finitely many such free intermediate algebras. Furthermore if $S \supseteq F^G$, then any monomorphism $\phi: S \to F$ fixing F^G is the restriction of an element of G.*

Finally we mention a lovely result of W. Dicks and E. Formanek [2] which determines when the invariant ring of a free algebra is finitely generated. It uses the previous theorem to reduce to the case of a cyclic group of prime order.

THEOREM 15. *Let G be a finite linear group of automorphisms of the free algebra $F = k\langle x_1, \ldots, x_n\rangle$. Then F^G is a finitely generated k-algebra if and only if G is scalar on F.*

REFERENCES

1. H. Cartan, *Théorie de Galois pour les corps non commutatifs*, Ann. Sci. École Norm. Sup. (3) **64** (1947), 59–77.

2. W. Dicks and E. Formanek, *Poincaré series and a problem of S. Montgomery*, Linear and Multilinear Algebra **12** (1982), 21–30.

3. J. Dieudonné, *La théorie de Galois des anneaux simples et semi-simples*, Comment. Math. Helv. **21** (1948), 154–184.

4. G. Hochschild, *Automorphisms of simple algebras*, Trans. A.M.S. **69** (1950), 292–301.

5. N. Jacobson, *The fundamental theorem of the Galois theory for quasi-fields*, Annals of Math. **41** (1940), 1–7

6. V.K. Kharchenko, *Generalized identities with automorphisms*, Algebra i Logika **14** (1975), 215–237 (English translation Algebra and Logic **14** (1976), 132–148).

7. ———, *Fixed elements under a finite group acting on a semiprime ring*, Algebra i Logika **14** (1975), 328–344 (English translation Algebra and Logic **14** (1976), 203–213).

8. ———, *Galois theory of semiprime rings*, Algebra i Logika **16** (1977), 313–363 (English translation Algebra and Logic **16** (1978), 208–258).

9. ———, *Algebras of invariants of free algebras*, Algebra i Logika **17** (1978), 478–487 (English translation Algebra and Logic **17** (1979), 316–321).

10. H.F. Kreimer, *Outer Galois theory for separable algebras*, Pacific J. Math **32** (1970), 147–155.

11. W.S. Martindale III, *Prime rings satisfying a generalized polynomial identity*, J. Algebra **12** (1969), 576–584.

12. Y. Miyashita, *Finite outer Galois theory of non-commutative rings*, J. Fac. Sci. Hokkaido Univ., Ser I **19** (1966), 115–134.

13. S. Montgomery, *Fixed rings of finite automorphism groups of associative rings*, Lecture Notes in Math. No. 818, Springer-Verlag, Berlin, 1980.

14. ——— and D.S. Passman, *Galois theory of prime rings*, E. Noether's 100th birthday issue J. Pure and Appl. Algebra (1984).

15. T. Nakayama, *Galois theory for general rings with minimum condition*, J. Math. Soc. Japan **1** (1949), 203–216.

16. ——— and G. Azumaya, *On irreducible rings*, Annals of Math. (2) **48** (1947), 949–965.

17. E. Noether, *Nichtkommutative algebra*, Math. Z. **37** (1933), 514–541.

18. A. Rosenberg and D. Zelinsky, *Galois theory of continous transformation rings*, Trans. A.M.S. **79** (1955), 429–452.

University of Southern California, Los Angeles, California 90089
University of Wisconsin, Madison, Wisconsin 53706