

## IT'S ESSENTIALLY MASCHKE'S THEOREM

D. S. PASSMAN

The Galois theory of noncommutative rings is a new subject with roots in invariant theory and in the Galois theory of fields, commutative rings and division rings. If  $G$  is a finite group of automorphisms of a ring  $R$ , then we are concerned with the relationship between  $R$  and the fixed subring  $R^G = \{r \in R \mid r^g = r \text{ for all } g \in G\}$ . For the best results it is frequently necessary to assume that  $R$  has no  $|G|$ -torsion, so that  $r \cdot |G| = 0$  implies  $r = 0$ , or even the stronger hypothesis that  $|G|^{-1} \in R$ . A delightful introduction to this material can be found in the survey paper [7] of Fisher and Osterburg. An in-depth study appears in the recent monograph [25] of Montgomery.

A useful tool in this subject is the skew group ring  $RG$ , the set of all formal sums  $\sum_{g \in G} r_g g$  with  $r_g \in R$ . Addition in  $RG$  is componentwise and multiplication is defined distributively by the formula

$$rg \cdot sh = rs^{g^{-1}}gh$$

for  $r, s \in R$  and  $g, h \in G$ . In this way,  $RG$  becomes an associative ring containing all the ingredients  $R$ ,  $G$  and  $R^G$  of the theory and results on skew group rings are therefore surely of interest. One particular result, namely Maschke's theorem, immediately comes to mind. It is the first major theorem proved about group algebras of finite groups and it shows the strong effect of  $|G|$ -torsion, or the lack of it, on the structure of these algebras. Indeed we will be able to say of a number of results considered here "It's essentially Maschke's theorem".

In this expository paper we will discuss certain skew group ring applications to the Galois theory of noncommutative rings. The results for the most part are known but some of the proofs are new. Indeed the simplifications appear precisely when Maschke's theorem comes into play. The material considered here is very special and certainly not indicative of the subject as a whole. It was chosen because it fits together nicely, because it can be presented in a self-contained manner with few prerequisites, and frankly because it is of particular interest to the author. Many of the results offered are not best possible but rather they are precisely what is needed for this presentation.

---

Received by the editors on September 22, 1981.

Copyright © 1983 Rocky Mountain Mathematics Consortium

At this point it is appropriate to explain the words in the title. A group algebra  $K[G]$  is the special case of a skew group ring with  $R = K$  a field and with the action of  $G$  on  $K$  trivial. Thus  $K[G]$  is indeed a  $K$ -algebra and Maschke's theorem [22] asserts that all  $K[G]$ -modules are completely reducible if and only if  $|G| \neq 0$  in  $K$ . On the other hand, if  $R$  is any ring and if  $W_R \subseteq V_R$  are  $R$ -modules then  $W_R$  is essential in  $V_R$ , written  $W_R \text{ ess } V_R$ , if and only if for all nonzero submodules  $X_R \subseteq V_R$  we have  $W_R \cap X_R \neq 0$ .

**1.  $R*G$ -modules.** Let  $R$  be an associative ring with 1 and let  $G$  be a finite multiplicative group. Then a crossed product  $R*G$  is an associative ring constructed from  $R$  and  $G$  analogous to but somewhat more general than the skew group ring. More precisely  $R*G$  consists of all formal sums  $\sum_{x \in G} r_x \bar{x}$  with  $r_x \in R$ . Addition in  $R*G$  is componentwise and multiplication is defined distributively using the formulas

$$\begin{aligned}\bar{x}\bar{y} &= t(x, y)\overline{xy}, \\ r\bar{x} &= \bar{x}r^{\bar{x}}\end{aligned}$$

for all  $x, y \in G$  and  $r \in R$ . Here the twisting  $t: G \times G \rightarrow U(R)$  is a map to the group of units of  $R$  and  $\bar{x} \in \text{Aut } R$  for all  $x \in G$ . The skew group ring  $RG$  is then the special case in which the twisting is trivial.

It is a simple exercise to determine the relations on  $t$  and the automorphisms which make  $R*G$  associative. Furthermore,  $R*G$  has an identity element which we may assume without loss of generality to be  $\bar{1}$  for  $1 \in G$  and  $\mathfrak{G} = \{u\bar{x} | u \in U(R), x \in G\}$  is a multiplicative group of units in  $R*G$ . Observe that  $R \subseteq R*G$  by the way of the embedding  $r \rightarrow r\bar{1}$  and that  $\mathfrak{G}$  acts on  $R$  by conjugation. Indeed the equation  $r\bar{x} = \bar{x}r^{\bar{x}}$  is equivalent to  $\bar{x}^{-1}r\bar{x} = r^{\bar{x}}$ . Moreover  $U(R) \triangleleft \mathfrak{G}$  and  $\mathfrak{G}/U(R) \cong G$ .

Crossed products occur quite frequently in various branches of ring theory and are usually no more difficult to deal with than skew group rings. We study these rings in the first three sections of this paper and we start with Maschke's theorem. Here  $W_R | V_R$  indicates that  $W_R$  is a direct summand of  $V_R$ .

**LEMMA 1.1.** *Let  $W \subseteq V$  be  $R*G$ -modules having no  $|G|$ -torsion. If  $W_R | V_R$ , then there exists an  $R*G$ -submodule  $U$  of  $V$  with  $(W \oplus U)_R \text{ ess } V_R$ . Furthermore, if  $V = V \cdot |G|$ , then  $W_{R*G} | V_{R*G}$ .*

**PROOF.** Write  $V_R = W_R \oplus W'_R$ , let  $\pi: V \rightarrow W$  denote the natural  $R$ -projection and define  $\lambda: V \rightarrow W$  by  $v^\lambda = \sum_{x \in G} (v\bar{x})^x \bar{x}^{-1}$ . Then it is easy to see that  $\lambda$  is an  $R*G$ -homomorphism and hence if  $U = \ker \lambda$  then  $U$  is an  $R*G$ -submodule of  $V$ . Let  $n = |G|$  and observe that for  $w \in W$  we have  $w^\lambda = wn$ . Thus since  $V$  has no  $n$ -torsion we see that  $W \cap U = 0$ . Now let  $v \in V$  and set  $w = v^\lambda \in W$ . Then  $(vn)^\lambda = v^\lambda n = w^\lambda$  so  $(vn - w)^\lambda = 0$  and

we deduce that  $Vn \subseteq W \oplus U$ . In particular, if  $X$  is an  $R$ -submodule of  $V$  with  $(W \oplus U) \cap X = 0$ , then  $Xn \subseteq (W \oplus U) \cap X = 0$  and, since  $V$  has no  $n$ -torsion, we conclude that  $X = 0$ . Thus  $(W \oplus U)_R \text{ ess } V_R$ . Finally if  $V = Vn$ , then  $V = W \oplus U$  and  $W_{R*G} | V_{R*G}$ .

As a consequence we have the following lemma.

LEMMA 1.2. *Let  $W \subseteq V$  be  $R*G$ -modules with no  $|G|$ -torsion. Then*

- (i) *there exists an  $R*G$ -module  $U \subseteq V$  with  $(W \oplus U)_R \text{ ess } V_R$ , and*
- (ii)  *$W_R \text{ ess } V_R$  if and only if  $W_{R*G} \text{ ess } V_{R*G}$ .*

PROOF. (i) Let  $L$  be an  $R$ -submodule of  $V$  maximal with respect to the property and  $W \cap L = 0$ . Then certainly  $(W \oplus L)_R \text{ ess } V_R$ . Moreover, if  $E$  is the finite intersection  $E = \bigcap_{x \in G} (W \oplus L)\bar{x}$  then, using  $\bar{x}R = R\bar{x}$ , we see easily that  $E$  is an  $R*G$ -submodule of  $V$  and  $E_R \text{ ess } V_R$ . Observe that  $W \subseteq E \subseteq W \oplus L$  so  $E = W \oplus (E \cap L)$  and we can apply Lemma 1.1 to  $W \subseteq E$ . Thus there exists an  $R*G$ -submodule  $U$  of  $E$  with  $(W \oplus U)_R \text{ ess } E_R$ . But  $E_R \text{ ess } V_R$  so  $(W \oplus U)_R \text{ ess } V_R$  and this part is proved.

(ii) If  $W_R \text{ ess } V_R$  then certainly  $W_{R*G} \text{ ess } V_{R*G}$ . Conversely, if  $W_{R*G} \text{ ess } V_{R*G}$  and if we apply (i) above, then we must have  $U = 0$  and  $W_R \text{ ess } V_R$ .

Part (ii) above is the essential version of Maschke's theorem. Let  $V$  be an  $R$ -module. Then the Goldie rank of  $V$ , written  $\text{rank } V_R$ , is defined to be the largest integer  $k$  such that  $V$  contains  $V_1 \oplus V_2 \oplus \cdots \oplus V_k$  a direct sum of  $k$  nonzero submodules. If no such maximum exists, then  $\text{rank } V_R = \infty$ . Basic properties of this rank can be found in [8]. In particular it is clear that  $W \subseteq V$  implies  $\text{rank } W \leq \text{rank } V$  and that  $W \text{ ess } V$  implies equality of ranks. Modules of rank 1 are called uniform, so that  $U \neq 0$  is uniform if and only if for all nonzero submodules  $X, Y \subseteq U$  we have  $X \cap Y \neq 0$ . Furthermore  $\text{rank } (V \oplus W) = \text{rank } V + \text{rank } W$  and if  $U_1, U_2, \dots, U_k$  are uniform with  $(U_1 \oplus U_2 \oplus \cdots \oplus U_k) \text{ ess } V$ , then  $\text{rank } V = k$ .

LEMMA 1.3. *Let  $V$  be an  $R*G$ -module. Then*

$$\text{rank } V_{R*G} \leq \text{rank } V_R \leq |G| \cdot \text{rank } V_{R*G}.$$

PROOF. The first inequality, namely  $\text{rank } V_{R*G} \leq \text{rank } V_R$ , is obvious. We consider the second. For each  $R$ -submodule  $A_R$  of  $V_R$  define  $\tilde{A} = \bigcap_{x \in G} A\bar{x}$ . Then  $\tilde{A} = \{v \in V | v\bar{x}^{-1} \in A \text{ for all } x \in G\}$  and it is easy to see that  $\tilde{A}$  is an  $R*G$ -submodule of  $V$ . In fact,  $\tilde{A}$  is the largest  $R*G$ -submodule of  $V$  contained in  $A$ . Since  $G$  is finite, Zorn's lemma applies and there exists  $A$  maximal with  $\tilde{A} = 0$ .

Suppose that  $(B_1/A) \oplus (B_2/A) \oplus \cdots \oplus (B_k/A)$  is a direct sum of nonzero  $R$ -submodules of  $V/A$ . Then  $B_i$  is properly larger than  $A$ , so

$\tilde{B}_i \neq 0$  and it is easy to see that  $\tilde{B}_1 \oplus \tilde{B}_2 \oplus \cdots \oplus \tilde{B}_h$  is a direct sum of nonzero  $R^*G$ -submodules of  $V$ . Thus we see that  $\text{rank}(V/A)_R \leq \text{rank } V_{R^*G}$ . Finally each  $A\bar{x}$  is also an  $R$ -submodule of  $V$  with the same property as  $A$  so  $\text{rank}(V/A\bar{x})_R \leq \text{rank } V_{R^*G}$ . Thus since  $\bar{A} = 0$ ,  $V_R$  is embedded isomorphically in  $\bigoplus \sum_{x \in G} (V/A\bar{x})$  and

$$\text{rank } V_R \leq \sum_{x \in G} \text{rank}(V/A\bar{x})_R \leq |G| \cdot \text{rank } V_{R^*G}.$$

REMARKS. The formulation of Maschke's theorem in Lemma 1.1 is due to Higman [10]. In fact there is a more general version which compares  $V_{R^*G}$  and  $V_{R^*H}$  where  $H$  is a subgroup of  $G$  and where  $V$  has no  $[G:H]$ -torsion. However this does not carry over to Lemma 1.2. Lemma 1.2 appears in [21]. The special case of Lemma 1.3 for modules of infinite rank is due to Kharchenko [14]. More recently, variants of this general result have been discovered independently by a number of people.

**2. Semiprime rings.** A ring  $R$  is semiprime if it has no nonzero nilpotent ideals. In other words, if  $I$  is an ideal of  $R$ , written  $I \triangleleft R$ , and if  $I^2 = 0$  then  $I = 0$ . Such rings have a number of nice properties. Indeed, suppose  $A, B \triangleleft R$  with  $AB = 0$ . Then  $(A \cap B)^2 = 0$  so  $A \cap B = 0$  and hence also  $BA = 0$ . It therefore follows that  $r_R(A)$  and  $\ell_R(A)$ , the right and left annihilators of  $A$ , are equal and we denote this common ideal by  $\text{ann}_R A$ . In addition  $A \cap \text{ann } A = 0$  and in fact  $(A \oplus \text{ann } A)_R \text{ ess } R_R$ . To see the latter, observe that if  $X_R$  is a right ideal of  $R$  disjoint from  $A$ , then  $XA \subseteq X \cap A = 0$  and  $X \subseteq \text{ann } A$ .

We continue our study of crossed products  $R^*G$  and we apply the results of §1 to the right ideals of this ring. Note that if  $R$  has no  $|G|$ -torsion, then the same is surely true of  $R^*G$ .

LEMMA 2.1. *Let  $R$  be a ring with no  $|G|$ -torsion and let  $I \triangleleft R^*G$  with  $I_{R^*G} \text{ ess } (R^*G)_{R^*G}$ . We have*

- (i)  $(I \cap R)_R \text{ ess } R_R$ , hence  $I \cap R \neq 0$ , and
- (ii) if  $R$  is semiprime, then  $r_{R^*G}(I) = \ell_{R^*G}(I) = 0$ .

PROOF. By Lemma 1.2 (ii) we have  $I_R \text{ ess } (R_{R^*G})_R$  and hence  $(I \cap R)_R \text{ ess } R_R$ . In addition, if  $R$  is semiprime then the latter implies that  $\text{ann}_R(I \cap R) = 0$ . Thus clearly  $\ell_{R^*G}(I \cap R) = r_{R^*G}(I \cap R) = 0$  and, since  $I \supseteq I \cap R$ , the result follows.

We now come to the Fisher-Montgomery theorem [4]. This is known to be "essentially Maschke's theorem". We now see why.

THEOREM 2.2. *Let  $R$  be a semiprime ring with no  $|G|$ -torsion. Then  $R^*G$  is semiprime.*

PROOF. Let  $N$  be a nilpotent ideal of  $R^*G$  and set  $I = \ell_{R^*G}(N)$ . Then

$I \triangleleft R * G$  and  $I_{R * G}$  ess  $(R * G)_{R * G}$ . For the latter observe that if  $X$  is a nonzero right ideal of  $R * G$  and if  $k$  is maximal with  $XN^k \neq 0$ , then  $XN^k \subseteq X \cap I$ . Now Lemma 2.1 (ii) applies and we conclude that  $N \subseteq r_{R * G}(I) = 0$ .

An ideal  $P$  of  $R$  is prime, written  $P \triangleleft' R$ , if for all  $A, B \triangleleft R$  the inclusion  $AB \subseteq P$  implies  $A \subseteq P$  or  $B \subseteq P$ . Then, as is well known,  $R$  is semiprime if and only if the intersection of all its prime ideals is zero or equivalently if and only if the intersection of all its minimal primes is zero.

We now study  $R$  as an  $(R, R)$ -bimodule with an eye towards computing rank  ${}_R R_R$ . Observe that the submodules of  ${}_R R_R$  are precisely the ideals of  $R$  and that  $0 \neq U \triangleleft R$  is uniform if and only if for all nonzero ideals  $A, B \subseteq U$  we have  $A \cap B \neq 0$ .

LEMMA 2.3. *Let  $R$  be a semiprime ring, let  $P \triangleleft' R$  and let  $U \triangleleft R$  be uniform.*

- (i)  $I \triangleleft R$  and  $I > P$  implies that  $\text{ann } I = 0$ .
- (ii)  $\text{ann } P$  is either zero or uniform.
- (iii)  $\text{ann } U$  is a minimal prime of  $R$ .
- (iv) If  $P_1, P_2, \dots, P_n$  are all the minimal primes of  $R$ , then  $\text{ann } P_j = \bigcap_{i \neq j} P_i \neq 0$  and  $\text{ann}(\text{ann } P_j) = P_j$ .

PROOF. (i)  $I \cdot \text{ann } I = 0 \subseteq P$  and  $I \not\subseteq P$  implies that  $\text{ann } I \subseteq P < I$ . Thus  $\text{ann } I = 0$ .

(ii) Suppose  $A, B \triangleleft R$  with  $A, B \subseteq \text{ann } P$  and  $A \cap B = 0$ . Then  $AB = 0 \subseteq P$  so, say,  $A \subseteq P \cap \text{ann } P = 0$ .

(iii) Let  $A, B \triangleleft R$  with  $AB \subseteq \text{ann } U$ . Then  $(AU) \cdot (BU) = 0$  so  $AU \cap BU = 0$ . Since  $U$  is uniform, this implies, say,  $AU = 0$  and  $A \subseteq \text{ann } U$ . Thus  $\text{ann } U$  is prime and, by (i), it must be minimal since  $U \neq 0$ .

(iv) If  $i \neq j$  then  $P_i \supseteq 0 = P_j \cdot \text{ann } P_j$  so  $P_i \supseteq \text{ann } P_j$ . Thus  $\bigcap_{i \neq j} P_i \supseteq \text{ann } P_j$  and equality must hold, since  $R$  semiprime implies  $\bigcap_i P_i = 0$ . Moreover the intersection  $\bigcap_i P_i = 0$  is irredundant so  $\text{ann } P_j$  is nonzero. Finally  $\text{ann}(\text{ann } P_j) \supseteq P_j$  and, by (i), equality must hold.

As a consequence we obtain the following characterization of the bimodule Goldie rank.

LEMMA 2.4. *Let  $R$  be a semiprime ring. Then  $R$  has finitely many minimal primes if and only if  $\text{rank } {}_R R_R < \infty$ . Furthermore, when this occurs the number of minimal primes is precisely equal to  $\text{rank } {}_R R_R$ .*

PROOF. Assume that  $R$  has  $n < \infty$  minimal primes  $P_1, P_2, \dots, P_n$ . Since  $\bigcap_1^n P_i = 0$ ,  $R$  embeds isomorphically in  $(R/P_1) \oplus (R/P_2) \oplus \dots \oplus (R/P_n)$ . But each  $R/P_i$ , being a prime ring, is surely uniform as an  $(R, R)$ -bimodule. Thus  $k = \text{rank } {}_R R_R \leq n$ .

Conversely let  $\text{rank } {}_R R_R = k < \infty$  and let  $U_1, U_2, \dots, U_k$  be uniform ideals with  $E = U_1 \oplus U_2 \oplus \dots \oplus U_k$  essential as an  $(R, R)$ -bimodule. Since  $R$  is semiprime, the latter implies that  $\text{ann } E = 0$  and hence that

$\bigcap_1^k \text{ann } U_i = 0$ . But each  $\text{ann } U_i$  is a minimal prime by Lemma 2.3 (ii) so  $R$  has  $n \leq k$  minimal primes and the result follows.

REMARKS. Other proofs of Theorem 2.2 appear in the original Fisher-Montgomery paper as well as in [21] and [28]. However the proof offered here is considerably easier than all of these. Lemma 2.4 is an extremely useful result due to Heinicke and Robson [9].

**3. Prime ideals in  $R*G$ .** We now use the results of the preceding section to study the primes of  $R*G$ . Recall that  $\mathcal{G} = \{u\bar{x}|u \in U(R), x \in G\}$  is a group of units in  $R*G$  which acts on  $R$  by conjugation. Hence  $\mathcal{G}$  permutes the ideals of  $R$  and clearly  $U(R)$  acts trivially. Thus  $G \cong \mathcal{G}/U(R)$  permutes these ideals. Observe that, if  $A$  is a  $G$ -invariant ideal of  $R$ , then  $A*G = A(R*G)$  is an ideal of  $R*G$  and clearly  $(R*G)/(A*G) = (R/A)*G$  where the latter is a suitable crossed product of  $G$  over  $R/A$ .

We say that  $R$  is  $G$ -prime if for all nonzero  $G$ -invariant ideals  $A, B$  of  $R$  we have  $AB \neq 0$ . Furthermore if  $A \triangleleft R$  is  $G$ -invariant, then  $A$  is said to be  $G$ -prime if and only if  $R/A$  is a  $G$ -prime ring. These ideals are of interest because of the following Lying Over result.

LEMMA 3.1. *Given  $R*G$ .*

- (i) *If  $P \triangleleft' R*G$ , then  $P \cap R$  is a  $G$ -prime ideal of  $R$ .*
- (ii) *If  $A$  is a  $G$ -prime ideal of  $R$ , then there exists  $P \triangleleft' R*G$  with  $P \cap R = A$ .*

PROOF. (i) Since any ideal of  $R*G$  is  $G$ -invariant, it is clear that  $P \cap R$  is a  $G$ -invariant ideal of  $R$ . Now let  $A, B \triangleleft R$  be  $G$ -invariant with  $AB \subseteq P \cap R$ . Then  $A*G, B*G \triangleleft R*G$  with  $(A*G)(B*G) = AB*G \subseteq P$ . Thus if, say,  $A*G \subseteq P$ , then  $A \subseteq P \cap R$ .

(ii) There exists an ideal  $I$  of  $R*G$ , namely  $A*G$ , with  $I \cap R = A$ . We now choose  $P \triangleleft R*G$  maximal with this property. It follows easily that  $P$  is prime.

The next argument is analogous to that of Lemma 1.3.

LEMMA 3.2. *The ring  $R$  is  $G$ -prime if and only if there exists  $Q \triangleleft' R$  with  $\bigcap_{x \in G} Q^x = 0$ . Furthermore, when this occurs,  $R$  is semiprime and the ideals  $Q^x$  are precisely all the minimal primes of  $R$ .*

PROOF. If  $Q \triangleleft' R$  with  $\bigcap_{x \in G} Q^x = 0$ , then it is trivial to verify that  $R$  is  $G$ -prime. Conversely assume that  $R$  is  $G$ -prime and, by Zorn's lemma, choose  $Q \triangleleft R$  maximal with respect to the property that  $\bigcap_{x \in G} Q^x = 0$ . It follows easily that  $Q$  and all its conjugates  $Q^x$  are prime. Furthermore the minimal primes of  $R$  are the minimal members of  $\{Q^x | x \in G\}$ . But if  $Q$  is a minimal prime, then surely so is  $Q^x$  so these are all minimal primes.

We now fix some notation. Let the crossed product  $R*G$  be given and

assume that  $R$  is  $G$ -prime. Let  $Q$  be a minimal prime of  $R$ , as described above, and define  $H = \text{stab}_G Q = \{x \in G \mid Q^x = Q\}$  and  $N = \text{ann}_R Q$ . By Lemmas 3.2 and 2.3 (iv) we have  $\text{ann}_R N = Q$  and  $N = \bigcap_{x \notin H} Q^x$ .

LEMMA 3.3. *Let  $0 \neq I \triangleleft R * G$ . Then  $0 \neq NIN \subseteq N * H \subseteq R * H$ .*

PROOF. Since  $H$  is the stabilizer of  $Q$  in  $G$  it is clear that  $H$  stabilizes  $N$ . Conversely any element of  $G$  stabilizing  $N$  will also stabilize  $\text{ann}_R N = Q$ . Thus  $\text{stab}_G N = H$  and it follows from Lemma 2.3 (iv) that  $N^x N = 0$  for  $x \notin H$  and hence that  $N \bar{x} N = 0$ . This yields

$$N(R * G)N = \sum_{x \in G} N \bar{x} N = \sum_{x \in H} N \bar{x} N \subseteq N * H$$

and thus  $NIN \subseteq N * H$ .

Finally let  $J$  be the set of identity coefficients of elements of  $I$  so that  $J = \{r \in R \mid \sum_{x \in G^r} x \bar{x} \in I \text{ and } r = r_1\}$ . Then  $J$  is a nonzero  $G$ -invariant ideal of  $R$  and hence  $\text{ann}_R J = 0$ . In particular,  $JN \neq 0$  and, since  $R$  is semiprime, we have  $(JN)^2 \neq 0$  so  $NJN \neq 0$ . Thus  $NIN \neq 0$ .

The following is a special case of a result of Lorenz and Passman [18].

THEOREM 3.4. *Let  $R$  have no  $|G|$ -torsion and let  $R * G$  be given. Suppose that  $R$  is  $G$ -prime, let  $Q$  be a minimal prime of  $R$  and set  $H = \text{stab}_G Q$ . Then  $R * G$  has at most  $|H|$  minimal primes. Furthermore if  $P \triangleleft' R * G$ , then  $P$  is minimal if and only if  $P \cap R = 0$ .*

PROOF. By Theorem 2.2,  $S = R * G$  is semiprime and we begin by studying  $S$  as an  $(R, R)$ -bimodule. By Lemma 2.3 (ii),  $N = \text{ann}_R Q$  is uniform and hence clearly  $\text{rank}_R(N * H)_R = |H|$ . Now we compute  $\text{rank}_S S_S$ . Suppose  $I_1, I_2, \dots, I_k$  are nonzero ideals of  $S$  with  $\sum_i I_i$  a direct sum. Then, by the preceding lemma,  $NI_i N \neq 0$  and  $\sum_i NI_i N$  is a direct sum of  $(R, R)$ -subbimodules of  $N * H$ . Thus  $k \leq \text{rank}_R(N * H)_R = |H|$  and  $\text{rank}_S S_S \leq |H|$ . It now follows from Lemma 2.4 that  $S$  has  $n \leq |H|$  minimal primes.

Let  $P \triangleleft' R * G$ . If  $P$  is minimal, then by Lemma 2.3 (iv)  $\text{ann}_{R * G} P \neq 0$  and hence  $\text{ann}_R(P \cap R) \neq 0$ . But  $P \cap R$  is a  $G$ -invariant ideal of the  $G$ -prime ring  $R$  so we must have  $P \cap R = 0$ . Conversely suppose  $P$  is not minimal. Then  $\text{ann}_S P = 0$ , by Lemma 2.3 (i) and hence  $P_S \text{ess } S_S$ . Lemma 2.1 (i) yields  $P \cap R \neq 0$  and the theorem is proved.

COROLLARY 3.5. *Let  $R * G$  be given with  $|G|^{-1} \in R$  and let  $A$  be a  $G$ -prime ideal of  $R$ . Then  $A * G = P_1 \cap P_2 \cap \dots \cap P_n$  an intersection of  $n \leq |G|$  minimal covering primes. Furthermore, if  $P \triangleleft' R * G$ , then  $P = P_i$  for some  $i$  if and only if  $P \cap R = A$ .*

PROOF. Let  $\sim : R * G \rightarrow (R * G)/(A * G) = (R/A) * G$  denote the natural epimorphism. Then  $\bar{R} = R/A$  is a  $G$ -prime ring with no  $|G|$ -

torsion since  $|G|^{-1} \in R$ . Then by Theorems 2.2 and 3.4 we see that  $\tilde{R} * G$  has  $n \leq |G|$  minimal primes which intersect to zero and hence, if  $P_1, P_2, \dots, P_n$  are their complete inverse images in  $R * G$ , then  $P_i \triangleleft' R * G$  and  $\bigcap_1^n P_i = A * G$ . Finally if  $P \triangleleft' R * G$  then, by Theorem 3.4,  $P = P_i$  for some  $i$  if and only if  $P \cong A * G$  and  $\tilde{P} \cap \tilde{R} = 0$ . Since the latter conditions are easily seen to be equivalent to  $P \cap R = A$ , the result follows.

**REMARKS.** The result of Lorenz and Passman [18] is a good deal more general than Theorem 3.4. Indeed the no  $|G|$ -torsion assumption is not required and the result actually offers a reasonably useful description of the primes. As a consequence one sees that the number of minimal primes of  $R * G$  is actually at most equal to the number of conjugacy classes of  $H$  (not of  $G$ ). Corollary 3.5 is then also a special case of the correspondence between the  $G$ -prime ideals of  $R$  and the prime ideals of  $R * G$  obtained in [18] [19]. In those papers the basic Krull relations of Going Up, Going Down and Incomparability are proved without the assumption on  $|G|^{-1}$ .

This latter correspondence, in turn, is a special case of the more recent correspondence developed for prime ideals in finite normalizing extensions in [9] and [16]. From these papers we see that general incomparability, at present, appears to be exceedingly difficult to prove. But in our case, it is actually quite trivial. It turns up in Theorem 3.4 as the assertion that if  $P$  is a nonminimal prime of  $R * G$  then  $P \cap R \neq 0$ , and this is immediate from Lemma 1.2 (ii) the essential version of Maschke's theorem.

**4. Group actions and fixed points.** We now begin our applications to Galois theory. Let  $G$  be a finite group acting on the ring  $R$ . More precisely, this means that we have a homomorphism of  $G$  into  $\text{Aut } R$ . We are of course concerned with the relationship between  $R$  and the fixed subring  $R^G = \{r \in R \mid r^g = r \text{ for all } g \in G\}$ . Define the trace map on  $R$  by

$$\text{tr}_G(r) = \sum_{x \in G} r^x.$$

The following basic properties are trivial to check.

**LEMMA 4.1.** *Let  $G$  act on  $R$ .*

- (i)  $\text{tr}_G$  is an  $(R^G, R^G)$ -bimodule homomorphism from  $R$  to  $R^G$ .
- (ii) If  $A$  is a right ideal of  $R^G$ , then  $|G| \cdot A \cong |G| \cdot (AR)^G \cong \text{tr}(AR) \cong A$ .

Given the action of  $G$  on  $R$  we now form the skew group ring  $RG$ . This is easily seen to be an associative ring and indeed a special case of a crossed product. However since  $G$  is contained isomorphically in this ring, we do not use the overbar notation. Define  $\hat{G} = \sum_{x \in G} x \in RG$  and observe that for all  $g \in G$  we have  $\hat{G}g = g\hat{G} = g\hat{G}$ .



LEMMA 4.2. Let  $\hat{G} \in RG$  be as above.

(i)  $\hat{G}(RG) = \hat{G}R \cong R$  as  $RG$ -modules. Here  $R$  acts on  $R$  by right multiplication and  $G$  acts in the given manner.

(ii) If  $r \in R$ , then  $\hat{G}r\hat{G} = \hat{G} \cdot \text{tr } r$ . Hence  $\hat{G}(RG)\hat{G} = \hat{G} \cdot \text{tr } R \subseteq \hat{G} \cdot R^G$ .

(iii) If  $I$  is a  $G$ -invariant right ideal of  $R$ , then  $R\hat{G}I \triangleleft RG$  and for all  $n \geq 0$   $(R\hat{G}I)^{n+1} = R\hat{G}(\text{tr } I)^n I$ .

PROOF. (i) Since  $RG = GR$  we have  $\hat{G}(RG) = \hat{G}(GR) = \hat{G}R \cong R$  where the latter isomorphism is given by  $\theta(\hat{G}r) = r$ . This is certainly a right  $R$ -module map and for  $g \in G$  we have  $\theta(\hat{G}rg) = \theta(\hat{G}g^{-1}rg) = r^g = \theta(\hat{G}r)^g$ .

(ii) This is clear since

$$\hat{G}r\hat{G} = \sum_{x \in G} \hat{G}rx = \sum_{x \in G} \hat{G}x^{-1}rx = \hat{G} \cdot \text{tr } r.$$

(iii)  $R\hat{G}I$  is surely an  $(R, R)$ -bimodule. Furthermore since both  $R$  and  $I$  are  $G$ -invariant and since  $\hat{G}$  absorbs factors from  $G$  we have  $R\hat{G}I \triangleleft RG$ . Now by induction  $(R\hat{G}I)^{n+1} = R\hat{G}I \cdot R\hat{G}(\text{tr } I)^n I$ . But  $\hat{G}I\hat{G} = \hat{G}I\hat{G} = \hat{G} \cdot \text{tr } I$  from (ii) above, so the result follows.

We now obtain the extremely important theorem of Bergman and Isaacs [1].

THEOREM 4.3. Let  $G$  act on  $R$  and suppose that  $R$  is semiprime with no  $|G|$ -torsion.

(i) If  $I \neq 0$  is a  $G$ -invariant right or left ideal of  $R$ , then  $I^G \neq 0$  and  $\text{tr } I \neq 0$ .

(ii)  $R^G$  is semiprime.

PROOF. Let  $0 \neq I$  be a  $G$ -invariant right ideal of  $R$  and consider the nonzero ideal  $R\hat{G}I$  of  $RG$ . By Theorem 2.2,  $RG$  is semiprime so  $R\hat{G}I$  is not nilpotent. Thus, by Lemma 4.2 (ii),  $\text{tr } I$  is not nilpotent. In particular,  $\text{tr } I \neq 0$  and (i) is proved. For (ii) let  $A$  be a nonzero right ideal of  $R^G$  and set  $I = AR$ . Then  $\text{tr } I \subseteq A$  and  $\text{tr } I$  is not nilpotent so  $R^G$  is surely semiprime.

The following is a special case of the Bergman-Isaacs result [1] on the existence of fixed points. While we do not need it here, it is interesting to see how close these methods come to proving the general result.

THEOREM 4.4. Let  $G$  act on  $R$  a ring with no  $|G|$ -torsion, and suppose that  $0 \neq I \triangleleft R$  is  $G$ -invariant. If  $\text{tr } I$  is nilpotent, then  $I \cap r_R(I) \neq 0$ .

PROOF. By Lemma 4.2 (iii),  $R\hat{G}I$  is a nilpotent ideal of  $RG$ . Therefore  $J = r_{RG}(R\hat{G}I)$  is an ideal of  $RG$ , essential as a left ideal. Hence, by the left analog of Lemma 2.1 (i) we have  ${}_R(J \cap R) \text{ ess } {}_R R$ . But surely  $J \cap R = r_R(I)$  so, since  $I \neq 0$  we have  $I \cap r_R(I) \neq 0$ .

REMARKS. The proof given above for Theorem 4.3 was shown to me by Montgomery and appears in [24]. The work of Bergman and Isaacs [1] goes well beyond Theorem 4.4. Indeed, their main result asserts that, with the hypothesis as given,  $I$  is nilpotent of degree bounded by a function of  $|G|$  and of the nilpotence degree of  $\text{tr } I$ . This is proved by a subtle combinatorial argument, best understood in the context of skew group rings. It does follow from Theorem 4.4, with a little work, that  $I$  is nilpotent. However, we obtain no bound for its nilpotence degree in this manner.

**5. Goldie rings.** Here we continue our application of skew group rings to Galois theory. The following lemma shows that there exists a nice relationship between the essential right ideals of  $R$  and those of  $R^G$ . In part (i), the  $RG$ -module structure of  $R$  is as described in Lemma 4.2 (i).

LEMMA 5.1. *Let  $G$  act on  $R$ , a semiprime ring with no  $|G|$ -torsion.*

- (i)  $\text{rank } R^G = \text{rank } R_{RG}$ .
- (ii)  $\text{rank } R^G \leq \text{rank } R_R \leq |G| \cdot \text{rank } R^G$ .
- (iii) *If  $E$  is an essential right ideal of  $R$ , then  $(E \cap R^G) \text{ ess } R^G$ .*
- (iv) *If  $A$  is an essential right ideal of  $R^G$ , then  $AR \text{ ess } R$ .*

PROOF. We will freely use Lemma 4.1 (ii) and Theorem 4.3 (i).

(i) If  $I_1 \oplus I_2 \oplus \dots \oplus I_k$  is a direct sum of nonzero  $RG$ -submodules of  $R$ , then  $I_1^G \oplus I_2^G \oplus \dots \oplus I_k^G$  is a direct sum of nonzero right ideals of  $R^G$ . Conversely if  $A_1 \oplus A_2 \oplus \dots \oplus A_k$  is a direct sum of nonzero right ideals of  $R^G$ , then  $A_1R \oplus A_2R \oplus \dots \oplus A_kR$  is a direct sum of nonzero  $RG$ -submodules of  $R$ . Indeed, the latter sum is direct since, for each  $i$ ,  $B_i = (A_1R + \dots + A_{i-1}R) \cap A_iR$  is a  $G$ -invariant right ideal of  $R$  with  $\text{tr } B_i \subseteq (A_1 + \dots + A_{i-1}) \cap A_i = 0$ . Thus  $B_i = 0$  and the ranks are clearly equal.

(ii) This is immediate from (i) above and Lemma 1.3.

(iii) If  $E \text{ ess } R$ , then since  $G$  is finite we see that  $(\bigcap_{x \in G} E^x) \text{ ess } R$  and this intersection is  $G$ -invariant. Thus we may assume  $E$  is  $G$ -invariant. Now suppose  $X$  is a nonzero right ideal of  $R^G$ . Then  $E \cap XR \neq 0$  and hence  $0 \neq \text{tr}(E \cap XR) \subseteq (E \cap R^G) \cap X$ .

(iv) If  $A \text{ ess } R^G$ , then it is clear that  $AR_{RG} \text{ ess } R_{RG}$ . Indeed if  $X$  is a nonzero  $G$ -invariant right ideal of  $R$ , then  $0 \neq X^G$  so  $A \cap X^G \neq 0$  and hence  $AR \cap X \neq 0$ . But then Lemma 1.2 (ii) yields  $AR_R \text{ ess } R_R$ .

As a consequence we obtain the lovely result of Levitzki [15] and Cohen-Montgomery [3]. This follows almost immediately since a ring  $R$  is semi-simple Artinian if and only if it has no proper essential right ideal.

THEOREM 5.2. *Let  $G$  act on  $R$  and suppose that  $R$  is semiprime with no  $|G|$ -torsion. Then  $R$  is semisimple Artinian if and only if  $R^G$  is.*

PROOF. If  $R^G$  is semisimple Artinian and if  $E \text{ ess } R$ , then  $(E \cap R^G) \text{ ess}$

$R^G$ , by Lemma 5.1 (iii), so  $1 \in E \cap R^G$  and  $E = R$ .

Conversely if  $R$  is semisimple Artinian, then the center of  $R$  is a sum of fields so  $|G|^{-1} \in R$ . If  $A \text{ ess } R^G$ , then  $AR \text{ ess } R$ , by Lemma 5.1 (iv), so  $1 \in AR$ . Thus  $|G| = \text{tr } 1 \in \text{tr } AR \subseteq A$ , by Lemma 4.1 (ii), and hence  $A = R^G$ . In view of the above remarks, the theorem is proved.

$R$  is said to be a Goldie ring if and only if  $\text{rank } R_R < \infty$  and  $R$  satisfies the maximum condition on right annihilators of subsets of  $R$ . Goldie's theorem [8, Theorem 1.37] asserts that a ring  $R$  has a classical right quotient ring  $Q(R)$  which is semisimple Artinian if and only if  $R$  is a semiprime Goldie ring. These rings can also be characterized in terms of their essential right ideals and therefore a correspondence analogous to the above theorem is to be expected. For convenience we quote the following lemma which merely isolates the last few steps in the proof of Goldie's theorem.

LEMMA 5.3. *Let  $T$  be a multiplicatively closed subset of regular elements of  $R$  and suppose that*

- (i)  $t \in T$  implies  $tR \text{ ess } R$ , and
- (ii)  $E \text{ ess } R$  implies  $E \cap T \neq \emptyset$ .

*Then  $T$  is a right divisor set in  $R$ ,  $RT^{-1}$  is a semisimple Artinian ring and  $R$  is a semiprime Goldie ring with classical quotient ring  $Q(R) = RT^{-1}$ .*

With this, we can now prove the following theorem of Kharchenko [14], discovered independently by Cohen [2] and by Fisher and Osterburg [6].

THEOREM 5.4. *Let  $G$  act on the ring  $R$  and suppose that  $R$  is semiprime with no  $|G|$ -torsion. Then  $R$  is Goldie if and only if  $R^G$  is. Furthermore when this occurs then  $Q(R) = RT^{-1}$  where  $T$  is the set of regular elements of  $R^G$  and  $Q(R)^G = Q(R^G)$ .*

PROOF. Observe that  $R^G$  is semiprime, by Theorem 4.1 (ii).

Suppose first that  $R$  is Goldie. Then  $R^G \subseteq R \subseteq Q(R)$  and  $Q(R)$  is Artinian so  $R^G$  surely satisfies the maximum condition on right annihilators of subsets. Furthermore  $\text{rank } R^G$  is finite, by Lemma 5.1 (ii), and hence  $R^G$  is semiprime Goldie.

Conversely suppose that  $R^G$  is Goldie and hence that  $Q(R^G) = R^G T^{-1}$  exists, where  $T$  is the set of regular elements of  $R^G$ . Certainly  $T$  is a multiplicatively closed subset of  $R$ . Furthermore, if  $t \in T$  and if  $X$  is either the right or left annihilator of  $t$  in  $R$ , then  $X$  is a  $G$ -invariant right or left ideal of  $R$  with  $X \cap R^G = 0$ . Hence, by Theorem 4.3 (i),  $X = 0$  and  $T$  consists of regular elements of  $R$ . We show now that  $T$  satisfies (i) and (ii) of Lemma 5.3. Indeed if  $t \in T$ , then  $tR^G \text{ ess } R^G$  since  $R^G$  is a Goldie ring. But then, by Lemma 5.1 (iv),  $tR = (tR^G)R$  is essential in  $R$ . On the other hand, if  $E \text{ ess } R$ , then  $(E \cap R^G) \text{ ess } R^G$ , by Lemma 5.1 (iii),

and hence since  $R^G$  is a semiprime Goldie ring we conclude that  $E \cap T = (E \cap R^G) \cap T \neq \emptyset$ . Lemma 5.3 now asserts that  $R$  is a semiprime Goldie ring with  $Q(R) = RT^{-1}$ . Finally, since  $T \cong R^G$  we see immediately that  $Q(R)^G = (RT^{-1})^G = R^G T^{-1} = Q(R^G)$  and the result follows.

We close this section by proving a special case of the additivity principle of Joseph and Small [13]. If  $e, f$  are idempotents of  $R$  we write  $e \sim f$  if and only if  $eR_R \cong fR_R$ . As is well known, this occurs if and only if there exist elements  $u, v \in R$  with  $e = uv$  and  $f = vu$ .

**LEMMA 5.5.** *Let  $S \cong R$  be rings with  $S$  semisimple Artinian and write  $S = \bigoplus \sum_1^k S_i$ , a direct sum of simple rings. If  $f_i$  is a primitive idempotent in  $S_i$ , then  $\text{rank } R = \sum_1^k (\text{rank } S_i)(\text{rank } f_i R)$ .*

**PROOF.** We know that  $S_i \cong M_{n_i}(D_i)$ , a full matrix ring over a division ring, and we let  $\{f_{i1}, f_{i2}, \dots, f_{in_i}\}$  be a family of orthogonal idempotents summing to the identity of  $S_i$ . Then  $1 = \sum_{ij} f_{ij}$  is an orthogonal decomposition of  $1 \in S \cong R$  and hence  $R = \bigoplus \sum_{ij} f_{ij}R$ . Observe that  $f_{ij} \sim f_i$  in  $S$  and hence in  $R$  so  $f_{ij}R \cong f_iR$ . Thus computing ranks yields  $\text{rank } R = \sum_1^k n_i \cdot \text{rank } f_i R$  and the lemma is proved since  $n_i = \text{rank } S_i$ .

**Remarks.** The inequality in Lemma 5.1 (ii) is due to Fisher and Osterburg [6]. The key relationship in Lemma 5.1 (iii) can be found in [2] and [6]. Part (iv), the converse of (iii), appears in [21] and is another application of Maschke's theorem. The proof given here of Theorem 5.4 follows the presentation in [21].

**6. Prime ideals in  $R^G$ .** Perhaps the most interesting application of skew group ring methods to Galois theory is the correspondence that is obtained between the prime ideals of  $R$  and of  $R^G$ . For this we need to assume that  $|G|^{-1} \in R$  and we define  $e \in RG$  by

$$e = |G|^{-1} \hat{G} = |G|^{-1} \sum_{x \in G} x.$$

**LEMMA 6.1.** *Let  $G$  act on  $R$  with  $|G|^{-1} \in R$ . Then  $e = |G|^{-1} \hat{G}$  is an idempotent of  $RG$  with*

- (i)  $e(AG)e = eA^G$  for any  $G$ -invariant ideal  $A$  of  $R$ , and
- (ii)  $e(RG)e = eR^G \cong R^G$  where the latter is a ring isomorphism.

**PROOF.** Since  $g\hat{G} = \hat{G}$  it follows that  $(\hat{G})^2 = |G| \cdot \hat{G}$  and hence that  $e$  is an idempotent. Now let  $A$  be a  $G$ -invariant ideal of  $R$ . Then  $A^G = \text{tr } A$  since  $|G|^{-1} \in R$  so (i) is immediate from Lemma 4.2 (ii). Furthermore, since  $R^G$  clearly commutes with  $e$ , the isomorphism  $eR^G \cong R^G$  does indeed preserve the ring structure.

In view of part (ii) above, the following lemma is surely of interest.

LEMMA 6.2. *Let  $e$  be a nonzero idempotent in a ring  $R$  and define  $\varphi$ , a map from ideals of  $R$  to those of  $eRe$ , by  $I^\varphi = eIe = I \cap (eRe)$ . Then  $\varphi$  yields a one-to-one correspondence between the set of prime ideals of  $R$  not containing  $e$  and all the primes of  $eRe$ . Moreover if  $P_1, P_2$  are primes of  $R$  not containing  $e$ , then  $P_1 \subseteq P_2$  if and only if  $P_1^\varphi \subseteq P_2^\varphi$ .*

PROOF. Observe that if  $I \triangleleft R$ , then  $eIe = I \cap (eRe)$  and that this is a proper ideal of  $eRe$  if  $e \notin I$ . Furthermore if  $A \triangleleft eRe$ , then  $RAR \triangleleft R$  and, since  $A = eAe$ , we have  $(RAR)^\varphi = eR(eAe)Re = A$ . From this it follows easily that if  $P \triangleleft' R$ , then  $P^\varphi \triangleleft' eRe$ .

Now suppose  $P, I \triangleleft R$  with  $P$  prime and  $e \notin P$ . If  $I^\varphi \subseteq P^\varphi$ , then  $eIe = I^\varphi \subseteq P$  and  $(ReR)I(ReR) \subseteq P$ . But  $P$  is prime and  $e \notin P$ , so this yields  $I \subseteq P$ . We conclude from this that  $\varphi$  is one-to-one on the set of primes of  $R$  not containing  $e$  and it remains to show that  $\varphi$  is onto.

Let  $Q \triangleleft' eRe$ . Since  $(RQR)^\varphi = Q$  we can now choose, by Zorn's lemma, an ideal  $P$  of  $R$  maximal with  $P^\varphi = Q$ . Then  $e \notin P$  and since  $P$  is easily seen to be prime, the lemma is proved.

We now combine the above two results. More precisely we study  $e \in RG$  as given in Lemma 6.1 and we let  $\varphi$  denote the map from ideals of  $RG$  to ideals of  $eRGe = eR^G \cong R^G$ . Thus if  $I \triangleleft RG$ , then  $I^\varphi = eJ$  for some  $J \triangleleft R^G$ .

LEMMA 6.3. *Let  $G$  act on  $R$  with  $|G|^{-1} \in R$  and let  $A$  be a  $G$ -prime ideal of  $R$ . Then  $A^G = Q_1 \cap Q_2 \cap \cdots \cap Q_k$ , a finite intersection of  $k \leq |G|$  minimal covering primes. Furthermore if  $Q \triangleleft' R^G$ , then  $Q = Q_i$  for some  $i$  if and only if  $eQ = P^\varphi$  for some prime  $P$  of  $RG$  with  $P \cap R = A$ .*

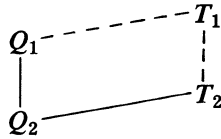
PROOF. By Corollary 3.5 we have  $AG = P_1 \cap P_2 \cap \cdots \cap P_n$  with  $n \leq |G|$ . Thus if  $P_i^\varphi = eQ_i$ , then Lemma 6.1 (i) yields

$$eA^G = (AG)^\varphi = P_1^\varphi \cap P_2^\varphi \cap \cdots \cap P_n^\varphi = eQ_1 \cap eQ_2 \cap \cdots \cap eQ_n$$

and hence  $A^G = Q_1 \cap Q_2 \cap \cdots \cap Q_n$ . We can of course delete those  $Q_i$ 's equal to  $R^G$  or equivalently we delete those  $P_i$ 's containing  $e$ . When this is done and the primes suitably labeled, we then have, by Lemma 6.2,  $A^G = Q_1 \cap Q_2 \cap \cdots \cap Q_k$  an intersection of  $k \leq n \leq |G|$  primes. Furthermore since the  $P_i$ 's are incomparable so are the  $Q_i$ 's by Lemma 6.2 and hence  $Q_1, Q_2, \dots, Q_k$  are precisely the minimal covering primes of  $A^G$ .

Finally if  $Q \triangleleft' R^G$ , write  $eQ = P^\varphi$  for some  $P \triangleleft' RG$ . Then  $Q = Q_i$  if and only if  $P = P_i$ , by Lemma 6.2 again, and hence if and only if  $P \cap R = A$ . Note  $P$  necessarily satisfies  $e \notin P$ .

If  $T \triangleleft' R$  and  $Q \triangleleft' R^G$ , we say that  $T$  lies over  $Q$  if  $Q$  is a minimal covering prime of  $T \cap R^G$ . For simplicity we will describe certain Going Up and Going Down statements diagrammatically. Thus for example



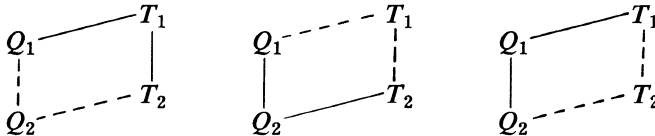
is read as follows. Given  $Q_1 \cong Q_2$  primes of  $R^G$  and  $T_2$  a prime of  $R$  lying over  $Q_2$ , there exists  $T_1$  a prime of  $R$  such that  $T_1$  lies over  $Q_1$  and  $T_1 \cong T_2$ . We can now obtain a key result due to Montgomery [26].

**THEOREM 6.4.** *Let  $G$  act on  $R$  and suppose that  $|G|^{-1} \in R$ .*

(i) *If  $T \triangleleft' R$ , then  $T \cap R^G = Q_1 \cap Q_2 \cap \cdots \cap Q_k$  an intersection of  $k \leq |G|$  minimal covering primes. Thus  $T$  lies over finitely many primes of  $R^G$ .*

(ii) *If  $Q \triangleleft' R^G$ , then there exists a prime  $T$  of  $R$ , unique up to  $G$ -conjugation, such that  $T$  lies over  $Q$ .*

(iii) *The following three versions of Going Up and Going Down hold.*



**PROOF.** (i) Let  $T \triangleleft' R$  and observe that for  $x \in G$  we have  $T^x \cap R^G = (T \cap R^G)^x = T \cap R^G$ . Hence if  $A = \bigcap_{x \in G} T^x$ , then  $A$  is a  $G$ -prime ideal of  $R$  and  $A^G = A \cap R^G = T \cap R^G$ . Now apply Lemma 6.3.

(ii) Let  $Q \triangleleft' R^G$  and define  $P \triangleleft' RG$  and  $A \triangleleft R$  by  $P^\varphi = eQ$  and  $A = P \cap R$ . Then  $A$  is a  $G$ -prime ideal of  $R$  so  $A = \bigcap_{x \in G} T^x$  for some  $T \triangleleft' R$ , by Lemma 3.2. Since  $T \cap R^G = A^G$  we see from Lemma 6.3 that  $T$  lies over  $Q$ . Furthermore that lemma shows that  $A$  is the unique  $G$ -prime ideal of  $R$  with  $Q$  minimal over  $A^G$ . Hence if  $T_1$  also lies over  $Q$  and if  $A_1 = \bigcap_{x \in G} T_1^x$ , then we must have  $A_1 = A$  and  $T_1 = T^x$  for some  $x \in G$ .

(iii) The first relation is obvious. We have  $Q_1 \cong T_1 \cap R^G \cong T_2 \cap R^G$  so  $Q_1$  contains a minimal covering prime  $Q_2$  of  $T_2 \cap R^G$ . For the second and third define  $P_i \triangleleft' RG$  and  $A_i \triangleleft R$  by  $P_i^\varphi = eQ_i$  and  $A_i = P_i \cap R$ . Then  $Q_1 \cong Q_2$  implies, by Lemma 6.2, that  $P_1 \cong P_2$  and hence that  $A_1 \cong A_2$ . It is now a simple matter to compare the corresponding  $T_i$ 's.

The missing Going Up relation in (iii) above does not in fact hold. Even though Going Up holds in  $RG$ , the primes determined may contain  $e$  and hence would not correspond to primes of  $R^G$ . The following result due to Lorenz, Montgomery and Small [17] is the additivity principle applied to Galois theory.

**THEOREM 6.5.** *Let  $G$  act on  $R$ , a ring with no  $|G|$ -torsion, and suppose*

that  $R$  is  $G$ -prime and Goldie. If  $T$  is a minimal prime of  $R$  with  $H = \text{stab}_G T$  and if  $Q_1, Q_2, \dots, Q_k$  are the minimal primes of  $R^G$ , then  $\text{rank}(R/T) = \sum_1^k z_i \cdot \text{rank}(R^G/Q_i)$  for suitable integers  $z_i$  satisfying  $1 \leq z_i \leq |H|$ .

PROOF. Since  $R$  is  $G$ -prime, it is semiprime and Theorem 5.4 applies. In particular,  $R^G$  is also semiprime Goldie and  $Q(R^G) = Q(R)^G$ . Furthermore, it is known (see [8]) that the minimal primes of  $R$  correspond in a one-to-one manner with the primes of  $Q(R)$  and indeed that their factor rings have equal Goldie rank. In view of these remarks, we may now clearly replace  $R$  by  $Q(R)$  and assume that both  $R$  and  $R^G$  are semisimple Artinian. Observe that  $|G|$  is now invertible in  $R$ .

Write  $R = R_1 \oplus R_2 \oplus \dots \oplus R_j$ , a direct sum of simple rings and, say,  $T = R_2 \oplus \dots \oplus R_j$ . Since  $R$  is  $G$ -prime, these factors are permuted transitively by  $G$  and hence it is clear that  $R^G \cong R_1^H$ . Thus since  $R_1 \cong R/T$ , we may clearly replace  $R$  by  $R_1$  and  $G$  by  $H$  and then assume that  $T = 0$ .

Finally write  $R^G = S = S_1 \oplus S_2 \oplus \dots \oplus S_k$  as in Lemma 5.5. Then by that lemma we have  $\text{rank}(R/T) = \text{rank} R = \sum_1^k (\text{rank } S_i)(\text{rank } f_i R)$ . Since  $S_i = R^G/Q_i$  and  $z_i = \text{rank } f_i R$  is a positive integer, it remains to bound these integers. To this end, we see from Lemma 4.1 that  $(f_i R)^G = f_i R^G$  is an  $R^G$ -module of rank 1. Hence Theorem 4.3 (i) implies that  $f_i R$  is an  $RG$ -module of rank 1 and Lemma 1.3 yields the result.

REMARKS. Lemma 6.2 is well known and can be found in [11]. Using this and Corollary 3.5, Lorenz and Passman were able to show in [18] that the prime lengths of  $R$  and of  $R^G$  are equal. However this work did not specifically look at the primes of  $R^G$  so Theorem 6.4 is a significant improvement. The special case with  $R^G$  central was considered earlier in [6]. Theorem 6.5 appears in [17] without an upper bound for the integers  $z_i$ . The result, in any case, is just a slight sharpening of the inequality obtainable from Lemma 5.1 (ii). We should mention that most of these correspondences and in particular those of Lemma 6.2 and Theorem 6.4 preserve the property of being a primitive ideal. In addition, it is shown in [26] that the correspondence of Theorem 6.4 is actually a homeomorphism between the appropriate quotient spaces of  $\text{Spec } R$  and  $\text{Spec } R^G$  endowed with the quotient Zariski topology.

**7. The Jacobson radical.** Since Maschke's theorem is so intimately related to semisimplicity considerations, it seems appropriate, in this final brief section, to discuss the Jacobson radical of crossed products and fixed rings. We start with a result of Villamayor [29]. Unlike the material considered earlier, the work here is "really Maschke's theorem".

**THEOREM 7.1.** *Let  $R * G$  be a crossed product with  $|G|^{-1} \in R$ . Then  $J(R * G) = J(R) * G$ .*

PROOF. There are two inclusions to prove here and the first does not require the assumption on  $|G|$ . Let  $V$  be an irreducible  $R * G$ -module. Then  $V$  is a cyclic  $R * G$ -module and hence  $V_R$  is finitely generated. It follows from Nakayama's lemma that  $VJ(R) \neq V$ . But  $VJ(R)$  is easily seen to be an  $R * G$ -submodule so  $VJ(R) = 0$ . We conclude that  $J(R) \subseteq J(R * G)$  and hence that  $J(R) * G \subseteq J(R * G)$ .

In the other direction, let  $V$  be an irreducible  $R$ -module and form the induced  $R * G$ -module  $V * G = V \otimes_R (R * G)$ . Then  $V * G = \bigoplus_{x \in G} V \otimes \bar{x}$  and each such  $V \otimes \bar{x}$  is an irreducible  $R$ -submodule conjugate to  $V$ . Thus  $(V * G)_R$  is completely reducible and Maschke's theorem, Lemma 1.1, implies that  $(V * G)_{R * G}$  is completely reducible. In particular  $(V * G) \cdot J(R * G) = 0$ . Finally, let  $\alpha = \sum_{g \in G} r_g \bar{g} \in J(R * G)$ . Then for any  $v \in V$ ,  $0 = (v \otimes \bar{1}) \alpha = \sum v r_g \otimes \bar{g}$  so  $v r_g = 0$  and  $V r_g = 0$ . Since this is true for all such  $V$  we deduce that  $r_g \in J(R)$  and therefore that  $J(R * G) \subseteq J(R) * G$ .

To transfer this information to fixed rings we use the well known fact that if  $e$  is a nonzero idempotent of  $R$ , then  $J(eRe) = eJ(R)e$ . As a consequence we obtain Montgomery's theorem [23].

**THEOREM 7.2.** *Let  $G$  act on  $R$  with  $|G|^{-1} \in R$ . Then  $J(R^G) = J(R) \cap R^G = J(R)^G$ .*

PROOF. Form  $RG$  and let  $e = |G|^{-1} \hat{G}$ . Then by Lemma 6.1 (i) (ii) and the preceding result we have

$$eJ(R^G) = e(J(R * G))e = e(J(R) * G)e = eJ(R)^G.$$

Thus we see that  $J(R^G) = J(R)^G$ .

REMARKS. The relationship between  $R$ - and  $R * G$ -modules considered in the proof of Theorem 7.1 is part of a general Clifford theory. There are numerous proofs of Theorem 7.2 in the literature, all of them of course using some version of Maschke's theorem. Analogous results for the prime radical follow immediately from Theorems 2.2 and 6.4.

CONCLUDING REMARKS. Skew group rings have proved to be an extremely useful tool in dealing with certain aspects of Galois theory. For example, much of the classical theory for fields and division rings can be developed quite nicely in this manner using the Jacobson-Bourbaki correspondence (see [11], [12]). In addition, the early papers of Zaleskii and Neroslavskii [30] and Fisher and Osterburg [5] on the Galois theory of noncommutative rings took a decidedly skew group ring approach. More recent successes include the prime ideal correspondence discussed here as well as a mechanism, due to Lorenz [20], for studying the restriction of  $R$ -modules to  $R^G$ .



Finally we mention two extremely interesting open problems which might be amenable to skew group ring methods. The first is a sharpening of the Bergman-Isaacs bound. Let  $G$  act on  $R$ , a ring with no  $|G|$ -torsion, and let  $I$  be a  $G$ -invariant ideal. If  $I^G = 0$ , then  $I$  is nilpotent of degree bounded by an extremely unpleasant function of  $|G|$ . If  $G$  is solvable, then it is known [1] that  $I^{|G|} = 0$  and it is conjectured that  $|G|$  is indeed the best possible bound in general. The second problem requires  $|G|^{-1} \in R$  and we ask whether  $R$  is integral, in some reasonable sense, over  $R^G$ . This is known to be true at least when  $G$  is abelian [27].

## REFERENCES

1. G.M. Bergman and I.M. Isaacs, *Rings with fixed-point-free group actions*, Proc. London Math. Soc. **27** (1973), 69–87.
2. M. Cohen, *Semiprime Goldie centralizers*, Israel J. Math. **20** (1975), 37–45, (addendum **24** (1976), 89–93).
3. ——— and S. Montgomery, *Semisimple Artinian rings of fixed points*, Canadian Math. Bull. **18** (1975), 189–190.
4. J. Fisher and S. Montgomery, *Semiprime skew group rings*, J. Algebra **52** (1978), 241–247.
5. J. Fisher and J. Osterburg, *Some results on rings with finite group actions*, in *Ring Theory*, Lecture Notes in Math., Vol. **25**, Marcel Dekker, New York, 1976, 95–112.
6. ———, *Semiprime ideals in rings with finite group actions*, J. Algebra **50** (1978), 488–502.
7. ———, *Finite group actions on noncommutative rings: a survey since 1970*, in *Ring Theory and Algebra III*, Marcel Dekker, New York, 1980, 357–393.
8. A.W. Goldie, *The structure of Noetherian rings*, in Springer Lecture Notes, No. **246**, Springer, Berlin, 1972.
9. A.G. Heinicke and J.C. Robson, *Normalizing extensions: prime ideals and incomparability*, J. Algebra **72** (1981), 237–268.
10. D.G. Higman, *Modules with a group of operators*, Duke Math. J. **21** (1954), 369–376.
11. N. Jacobson, *Structure of Rings*, Colloquium Publications, Vol. **37**, American Math. Soc., Providence, 1964.
12. ———, *Theory of Fields and Galois Theory*, Lectures in Abstract Algebra, Vol. **III**, Van Nostrand, Princeton, 1964.
13. A. Joseph and L.W. Small, *An additivity principle for Goldie rank*, Israel J. Math. **31** (1978), 105–114.
14. V.K. Kharchenko, *Galois extensions and quotient rings*, Algebra and Logic **13** (1975), 265–281.
15. J. Levitzki, *On automorphisms of certain rings*, Annals of Math. **36** (1935), 984–992.
16. M. Lorenz, *Finite normalizing extensions of rings*, Math. Zeit. **176** (1981), 447–484.
17. ———, S. Montgomery and L.W. Small, *Prime ideals in fixed rings II*, Comm. in Algebra **10** (1982), 449–456.
18. M. Lorenz and D.S. Passman, *Prime ideals in crossed products of finite groups*, Israel J. Math. **33** (1979), 89–132.

19. ———, *Integrality and normalizing extensions of rings*, J. Algebra **61** (1979), 289–297.
20. ———, *Observations on crossed products and fixed rings*, Comm. in Algebra **8** (1980), 743–779.
21. ———, *Two applications of Maschke's theorem*, Comm. in Algebra **8** (1980), 1853–1866.
22. H. Maschke, *Über den arithmetischen Character der Coefficienten der Substitutionem endlicher linearer Substitutionsgruppen*, Math. Ann. **50** (1898), 482–498.
23. S. Montgomery, *The Jacobson radical and fixed rings of automorphisms*, Comm. in Algebra **4** (1976), 459–465.
24. ———, *Outer automorphisms of semiprime rings*, J. London Math. Soc. **18** (1978), 209–221.
25. ———, *Fixed Rings of Finite Automorphism Groups of Associative Rings*, Lecture Notes in Math., No. **818**, Springer, Berlin, 1980.
26. ———, *Prime ideals in fixed rings*, Comm. in Algebra **9** (1981), 423–449.
27. D.S. Passman, *Fixed rings and integrality*, J. Algebra **68** (1981), 510–519.
28. ———, *Prime ideals in normalizing extensions*, J. Algebra **73** (1981), 556–572.
29. O.E. Villamayor, *On the semisimplicity of group algebras*, Proc. AMS **9** (1958), 621–627.
30. A.E. Zalesskii and O.M. Neroslavskii, *On simple Noetherian rings*, Proc. Akad. Sciences Bylorussia S.S.R. (1975), 38–42, (in Russian).

UNIVERSITY OF WISCONSIN-MADISON, MADISON, WI 53706