In this paper we make observations on three distinct problems. In the first section, we show that the crossed product $R*G$ of a finite group $G$ is prime if and only if certain crossed products $R_p*G_p$ of the Sylow subgroups of $G$ are all prime. Furthermore, if $R$ is a Goldie ring, then we obtain a formula for the rank of $R*G$ in terms of the ranks of the rings $R_p*G_p$. In the second section, we consider prime skew group rings $RG$ for arbitrary $G$ and we determine the group theoretic structure of $W = G_{\text{inn}} \cap \Delta^+(G)$ when $R$ is a domain. This can be achieved because a certain twisted group algebra $C^t[W]$ is a division ring. Finally, in the third section, we study the relationship between a ring $R$ and its subring $R^G$ of fixed elements under a finite group $G$ of automorphisms. In particular, we introduce a simple mechanism for translating properties from $R$-modules to $R^G$-modules and using this we obtain quite elementary proofs of some known results as well as a good deal of additional information.

§1. Prime Crossed Products and Sylow Subgroups

In this section we study $R*G$ with $G$ finite and we consider the possibility that this crossed product is prime. In particular, we show that this occurs if and only if, for each prime divisor $p$ of $|G|$, $R_p*G_p$ is prime.
where $G_p$ is a Sylow $p$-subgroup of $G$ and $R^p * G_p$ is a certain crossed product of $G_p$ naturally obtained from $R * G_p$. Furthermore, if $R$ is a Goldie ring, then so is $R * G$ and we obtain the formula

$$\frac{\text{rank } R * G}{\text{rank } R} = \prod_p \frac{\text{rank } R_p * G_p}{\text{rank } R_p}$$

relating the respective Goldie ranks.

The former result is clearly related to well known properties of groups of central type ([5]) and extends the special case considered in [10]. On the other hand, the rank formula can be viewed as an extension of [10, Theorem II.7] (at least when $R = F$ in the notation of that result.)

Our proof proceeds in three steps depending upon the complexity of $R$. We first assume that $R$ is simple Artinian, then that $R$ is prime and finally that $R$ is $G$-prime. Observe that the latter is indeed the general case since if $R * G$ is prime then $R$ is surely $G$-prime. Furthermore, within each of these steps there are two parallel considerations, namely whether $R$ is a general ring or a Goldie ring. For general rings, we use the theory developed in [18] while for Goldie rings we use localization techniques to compute the ranks involved.

We now begin the first step in the argument. This actually concerns the relationship between a semisimple Artinian ring and certain nicely embedded subrings. However for the sake of simplicity we will only consider crossed products. In the next three lemmas we make the following assumptions:

1. $S = M_m(D)$ is the full $m \times m$ matrix ring over the division ring $D$.
2. $S * H$ is a crossed product of the finite group $H$ over $S$ and $S * H$ is semisimple.
3. $A$ is a finite group of automorphisms of $S * H$.

Let us observe a few basic properties of $S * H$ and introduce some notation. First, it is clear that $S * H$ is Artinian and indeed, as a right $D$-module, we have $\dim_D S * H = m^2 |H|$. Thus since $S * H$ is assumed to be semisimple, the Wedderburn theorem applies and

$$S * H = \bigoplus_1 M_{a_1}(D_1)$$
CROSSED PRODUCTS AND FIXED RINGS

is a direct sum of full matrices over division rings. As a consequence, we see that if \( \rho(H) \) denotes the right regular module of \( S \ast H \), then we have

\[
\rho(H) = \sum a_i V_i
\]

where \( V_i \) is the unique irreducible module of \( M_{a_i}(D_i) \). We call \( a_i \) the multiplicity of \( V_i \) in \( \rho(H) \) and this integer is uniquely determined by the Jordan-Holder theorem. Since \( D \subset S \ast H \), all \( V_i \) are right \( D \)-modules and computing dimensions yields

\[
m^2|H| = \dim_D S \ast H = \sum a_i \dim_D V_i.
\]

Furthermore, for the Goldie rank we have clearly

\[
\text{rank } S \ast H = \sum a_i.
\]

Now let \( K \) be a subgroup of \( H \) so that \( S \ast K \subset S \ast H \). We claim that \( S \ast K \) is also semisimple. Indeed we know that \( S \ast H \) is von Neumann regular and hence if \( \alpha \in S \ast K \) then there exists \( \alpha' \in S \ast H \) with \( \alpha \alpha' \alpha = \alpha \). But, applying the natural projection \( \pi_K : S \ast H \to S \ast K \) yields easily \( \alpha \pi_K(\alpha') = \alpha \) and hence we see that \( S \ast K \) is also von Neumann regular and therefore semisimple. If \( V \) is an \( S \ast H \)-module, then we let \( V_K \) denote its restriction to \( S \ast K \). Certainly \( \rho(K) = [H : K] \rho(K) \).

In the other direction, if \( W \) is an \( S \ast K \)-module, then \( W^H = W \otimes_{S \ast K} S \ast H \) is a right \( S \ast H \)-module. Clearly \( \dim_D W^H = [H : K] \dim_D W \) and \( \rho(K)^H = \rho(H) \).

Finally suppose \( \sigma \) is an automorphism of \( S \ast H \). Then \( \sigma \) permutes the modules of \( S \ast H \) and indeed if \( V \) is given, then \( V^\sigma \) is the module

\[
V^\sigma = \{ v^\sigma | v \in V \}
\]

with action defined by \( v^\sigma \alpha^\sigma = (v\alpha)^\sigma \) for all \( \alpha \in S \ast H \).

Suppose further that \( \sigma \) stabilizes \( S \ast K \). Then clearly \( (V^\sigma)_K = (V_K)^\sigma \).

Conversely if \( W \) is an \( S \ast K \)-module, then \( (W^H)^\sigma = (W^\sigma)^H \) since the map

\[
(W^H)^\sigma = (W \otimes_{S \ast K} S \ast H)^\sigma \to W^\sigma \otimes_{S \ast K} S \ast H = (W^\sigma)^H
\]

given by \( (w \otimes \alpha)^\sigma \to w^\sigma \otimes \alpha^\sigma \) is easily seen to be a module isomorphism.

**Lemma 1.1.** Let \( K \subset H \) and suppose that \( \rho(K) = kW \) for some module \( W \) and integer \( k \). Then
i. All multiplicities in $\rho(H)$ are divisible by $k$.

ii. If $W$ is irreducible and if $V$ is an $S \rtimes H$-module, then

$$\dim_D W \mid \dim_D V.$$ 

iii. In particular, $m$ divides all multiplicities in $\rho(H)$ and $m$ divides the dimensions of all $S \rtimes H$-modules.

**Proof.** (i) This is immediate since $\rho(H) = \rho(K)^H = kW^H$.

(ii) If $W$ is irreducible, then $W$ is the unique irreducible $S \rtimes K$-module.

Hence $V_k = cW$ for some integer $c$ and $\dim_D V = c(\dim_D W)$.

(iii) Now let $K = \langle 1 \rangle$. Then $S \rtimes K = S = M_m(D)$ so $\rho(K) = mU$ where $U$ is the unique irreducible module of $M_m(D)$. Since $\dim_D U = m$, the result follows from (i) and (ii) above.

We say that $S \rtimes H$ is $A$-simple if and only if $S \rtimes H$ has no nonzero $A$-invariant ideal. Since $A$ clearly permutes the simple factors of $S \rtimes H = \oplus \Sigma_i M_{a_i}(D_i)$, it therefore follows that $S \rtimes H$ is $A$-simple if and only if $A$ permutes these factors transitively. Observe that if $V_1$ is the unique irreducible module of $M_{a_1}(D_1)$ and if $\sigma \in A$, then $V_1^\sigma$ is surely the unique irreducible module of $M_{a_1}(D_1)^\sigma$. Thus we see that $S \rtimes H$ is $A$-simple if and only if there is precisely one orbit of irreducible $S \rtimes H$-modules under the action of $A$. Note that, in any case, all irreducible modules in a fixed $A$-orbit occur with the same multiplicity in $\rho(H)$. We now add one additional assumption which will apply in the next two lemmas.

4. $\rho$ is a prime, $H_p$ is a Sylow $p$-subgroup of $H$, $A_p$ is a Sylow $p$-subgroup of $A$ and $A_p$ stabilizes $S \rtimes H_p$.

If $n$ is an integer, we let $|n|_p$ denote the $p$-part of $n$.

**Lemma 1.2.** Assume that $S \rtimes H$ is $A$-simple. Then $S \rtimes H_p$ is $A_p$-simple and we can write $\rho(H) = aV$, $\rho(H_p) = bW$ where $V$ is a sum of distinct $A$-conjugate irreducible $S \rtimes H$-modules and $W$ is a sum of distinct $A_p$-conjugate $S \rtimes H_p$-modules. We then have
CROSSED PRODUCTS AND FIXED RINGS

i. \((a/m)(\dim_D V/m) = |H|\)

ii. \(b/m = |a/m|_p\)

iii. \(\dim_D W/m = |\dim_D V/m|_p\).

Proof. Recall that by Lemma 1.1(iii), applied to both \(S \ast H\) and \(S \ast H_p\), \(m\) divides all multiplicities and dimensions which occur. Since \(S \ast H\) is \(A\)-simple, we have \(\rho(H) = aV\), where \(V = V_1 + V_2 + \ldots + V_r\) is a sum of a complete orbit of distinct \(A\)-conjugate irreducible modules with \(a\) being their common multiplicity. Furthermore write \(\rho(H_p) = bW + U\), where \(W = W_1 + W_2 + \ldots + W_s\) is a sum of distinct \(A_p\)-conjugate irreducible modules with common multiplicity \(b\) and where \(U\) denotes the remaining terms which come from other \(A_p\)-orbits. Since

\[m^2 |H| = \dim_D S \ast H = a(\dim_D V)\]

part (i) follows.

Now

\[aV_{H_p} = \rho(H)H_p = [H:H_p]\rho(H_p) = [H:H_p](bW + U)\]

and therefore \(a[H:H_p]b\). Thus \((a/m)[H:H_p](b/m)\) and since \([H:H_p]\) is a \(p'\)-number we have \(|a/m|_p|b/m|\). In the other direction, since \(W\) is \(A_p\)-invariant so is \(W^H\). Thus if \(T\) is a right transversal for \(A_p\) in \(A\), then \(|T| = [A:A_p]\) and \(\sum_{\tau \in T}(W^H)^\tau\)

is an \(A\)-invariant \(S \ast H\)-module. Hence clearly \(\sum_{\tau \in T}(W^H)^\tau = cV\) for some integer \(c\) and by computing dimensions we have

\[c \dim_D V = |T| \dim_D W^H = [A:A_p][H:H_p] \dim_D W.\]

Thus \(\dim_D V/m\) divides \([A:A_p][H:H_p](\dim_D W/m)\) and since \([A:A_p]\) and \([H:H_p]\) are \(p'\)-numbers we conclude that \(|\dim_D V/m|_p\) divides \(\dim_D W/m\).

We have shown above that

\[|a/m|_p(b/m), \quad |\dim_D V/m|_p(\dim_D W/m).\]

Hence since

\[|a/m|_p \cdot |\dim_D V/m|_p = |H|_p = |H_p|\]
we see that \(|H_p| = (b/m)(\dim_D W/m)|\) and in particular that \(b \dim_p W = m^2 |H_p|\). On the other hand

\[b \dim_D W \leq b \dim_D W + \dim_D U = \dim_D \rho(H_p) = m^2 |H_p|\]

so we conclude that \(U = 0\) and that equality occurs throughout. Hence \(\rho(H_p) = b W\), \(S \ast H_p\) is \(A_p\)-simple and equations (ii) and (iii) are satisfied.

**Lemma 1.3.** Let \(\rho(H) = \alpha V + U\), where \(V\) is a sum of distinct \(A\)-conjugate irreducible \(S \ast H\)-modules with common multiplicity \(\alpha\) and where \(U\) denotes the remaining terms which come from other \(A\)-orbits. If \(S \ast H_p\) is \(A_p\)-simple, then \(|H_p| \mid (a/m)(\dim_D V/m)\).

**Proof.** By assumption, \(\rho(H_p) = b W\) where \(W\) is a sum of \(A_p\)-conjugate irreducible \(S \ast H_p\)-modules. Thus, by Lemma 1.1(i) with \(K = H_p\), we have \(b \mid \alpha\) and hence \((b/m) \mid (a/m)\). Furthermore, since \(V\) is \(A\)-invariant, \(V_{H_p}\) is surely \(A_p\)-invariant and \(V_{H_p} = c W\) for some integer \(c\). This shows that \(\dim_D W \mid \dim_D V\) so \((\dim_D W/m) \mid (\dim_D V/m)\).

Finally, by combining these we have

\[|H_p| = (b/m)(\dim_D W/m) \mid (a/m)(\dim_D V/m)\]

and the lemma is proved.

This completes the first step. Now suppose that \(R\) is a semiprime Goldie ring. If \(T\) denotes the set of regular elements of \(R\), then Goldie's theorem (see [23, Theorem 10.4.10]) asserts that \(R\) has a semisimple Artinian right quotient ring \(\Theta(R) = \text{RT}^{-1}\) and \(\text{rank } R = \text{rank } \Theta(R)\). Furthermore, if \(R \ast G\) is given, then \(T\) is easily seen to be a right divisor set of regular elements of this larger ring. Indeed, the elements of \(T\) are surely regular in \(R \ast G\) and if \(t \in T\), \(a = \Sigma r_X \bar{x} \in R \ast G\) then the fractions \((t^{-1} r_X) \bar{x} = (t^{-1})^{-1} r_X \bar{x} \in \Theta(R)\) can all be written with a common denominator. Hence, for all \(x\) in the support of \(a\), there exists \(s_x \in R\) and \(\bar{t} \in T\) with \((t^{-1} r_X) \bar{x} = s_x \bar{t}^{-1}\). Setting \(\beta = \Sigma \bar{x} s_x \in R \ast G\), it follows immediately that \(t \beta = a \bar{t}\) and \(T\) is indeed a right divisor set. We
conclude that \((R \ast G)T^{-1}\) exists and then we see easily that this ring is just \((RT^{-1}) \ast G = \mathcal{D}(R) \ast G\). In other words, \(R \ast G\) is an order in the Artinian ring \(\mathcal{D}(R) \ast G\) and from this it follows that \(R \ast G\) is Goldie and that \(\mathcal{D}(R \ast G) = \mathcal{D}(R) \ast G\).

**Proposition 1.4.** Let \(R \ast G\) be given with \(R\) a prime ring and with \(G\) finite and, for each prime \(p\), let \(G_p\) be a Sylow \(p\)-subgroup of \(G\). Then \(R \ast G\) is prime if and only if \(R \ast G_p\) is prime for all \(p\).

Furthermore, if this occurs and if \(R\) is a Goldie ring, then

1. \(R \ast G\) is a Goldie ring,
2. \(\frac{\text{rank } R \ast G}{\text{rank } R}\) is an integer dividing \(|G|\).
3. \(\frac{\text{rank } R \ast G}{\text{rank } R} = \prod_p \frac{\text{rank } R \ast G_p}{\text{rank } R}\).

**Proof.** Since \(R\) is prime, we can use the notation of [18, §2]. In particular, \(G\) has a normal subgroup \(H = G_{\text{inn}}\) and \(G\) acts as automorphisms on a certain twisted group algebra \(E = C^t[H]\). Furthermore, by [18, Theorem 2.5] the maps \(u\) and \(d\) yield a one-to-one correspondence between the prime ideals \(P\) of \(R \ast G\) with \(P \cap R = 0\) and the \(G\)-prime ideals of \(C^t[H]\). Hence, since \(0^d = 0\), as is easily checked from the definitions, we conclude that \(R \ast G\) is prime if and only if \(C^t[H]\) is \(G\)-prime (see also [21, Theorem 2.8]). Furthermore, for each prime \(p\), if \(G_p\) is a Sylow \(p\)-subgroup of \(G\), then \((G_p)_{\text{inn}} = G_p \cap H = H_p\) is a Sylow \(p\)-subgroup of \(H\). Thus the above considerations also show that \(R \ast G_p\) is prime if and only if \(C^t[H_p]\) is \(G_p\)-prime. In other words, for the first part of the theorem, we need to prove that \(C^t[H]\) is \(G\)-prime if and only if \(C^t[H_p]\) is \(G_p\)-prime for all \(p\).

We use the notation of the preceding lemmas with \(S = C\), \(S \ast H = C^t[H]\) and \(A = G\). In particular, \(m = 1\) and \(D = C\) in this case. Suppose first that \(C^t[H]\) is \(G\)-prime. Then \(C^t[H]\) is certainly semisimple so Lemma 1.2 applies and we conclude that \(C^t[H_p]\) is \(G_p\)-prime. Conversely, suppose that \(C^t[H_p]\) is \(G_p\)-prime for all \(p\). If \(\text{char } C = 0\), then \(C^t[H]\) is semisimple by [21, Lemma 3.1]. Furthermore, if
char $C = q > 0$, then since $C^t[H_q]$ is semisimple, it follows again from [21, Lemma 3.1] that $C^t[H]$ is semisimple. Thus Lemma 1.3 and its notation applies to $C^t[H] = S \ast H$ and we see that if $\rho(H) = aV + U$, then $|H_p| \mid a(\dim_D V)$ for all primes $p$. This implies that $|H| = \prod_p |H_p|$ divides $a(\dim_D V)$ so $|H| \leq a(\dim_D V)$. On the other hand,

$$a(\dim_D V) + \dim_D U = \dim_D \rho(H) = |H|$$

so we conclude that $U = 0$, $\rho(H) = aV$ and $C^t[H]$ is $G$-simple. This completes the first part of the proof.

Now we assume that $R \ast G$ is prime and that $R$ is a Goldie ring. Then $R$, being prime, has a classical right ring of quotients $\Omega(R) = M_m(D)$, which is a full matrix ring over a division ring $D$, and rank $R = m$. Furthermore as we observed above, $R \ast G$ is Goldie and $\Omega(R \ast G) = S \ast G$ where $S = \Omega(R) = M_m(D)$. Since $R \ast G$ is prime, $S \ast G$ is therefore simple. We now use the notation of the previous lemmas with $S = \Omega(R) = M_m(D)$, $H = G$ and $A = \{1\}$. In particular, Lemma 1.2 and its notation applies and we conclude from Lemma 1.2 (i) that

$$\frac{\text{rank } R \ast G}{\text{rank } R} = \frac{\text{rank } S \ast G}{\text{rank } S} = \frac{a}{m}$$

is an integer dividing $|G|$. Thus (ii) follows. Furthermore, for each prime $p$, Lemma 1.2 (ii) yields $|a/m|_p = b/m$ or equivalently

$$\frac{|\text{rank } R \ast G|_p}{\text{rank } R} = \frac{|\text{rank } S \ast G|_p}{\text{rank } S}.$$

The product formula (iii) is now clearly satisfied.

This completes the second step in the argument and we now begin the third. The following lemma is presumably well known.

**Lemma 1.5.** Let $R$ be a semiprime Goldie ring and let $N$ be an annihilator ideal of $R$. Then $R/N$ is a semiprime Goldie ring and the natural map $R \rightarrow R/N$ extends to an epimorphism $\Omega(R) \rightarrow \Omega(R/N)$ with kernel $N \Omega(R)$. Furthermore if $P_1, P_2, \ldots, P_n$ are the minimal prime ideals of $R$, then each partial intersection $\bigcap^m_1 P_1$ is an annihilator ideal of $R$. 
CROSSED PRODUCTS AND FIXED RINGS

Proof. Let \( N = \text{ann} \, A \), let \( - : R \to R/N \) denote the natural epimorphism and let \( T \) be the set of regular elements of \( R \). We first observe that \( T \) consists of regular elements of \( R \). Indeed if \( t \in T \), \( r \in R \) with \( tr = 0 \), then \( tr \in N \) so \( trA = 0 \). Thus \( rA = 0 \) since \( t \) is regular, so \( r \in \text{ann} \, A = N \) and \( T = 0 \). Similarly \( tr = 0 \) implies that \( T = 0 \). Furthermore, since \( T \) is a right divisor set in \( R \) and \( - \) is an epimorphism, it is clear that \( T \) is a right divisor set in \( R \). Hence the ring \( R \cdot T^{-1} \) exists. It is now trivial to verify that the map \( R \cdot T^{-1} \to R \cdot T^{-1} \) given by \( rT^{-1} \mapsto rt^{-1} \cdot T^{-1} \) is a well defined ring epimorphism extending the original map \( R \to R \). But \( R \cdot T^{-1} = \Omega(R) \) is a semisimple Artinian ring, so we see that \( R \) is an order in the semisimple Artinian ring \( R \cdot T^{-1} \). It follows immediately from this that \( R/N = \Omega \) is a semiprime Goldie ring and that \( R \cdot T^{-1} = \Omega(R) \). Since the kernel of the map \( \Omega(R) \to \Omega(R) \) is clearly \( NT^{-1} = N \cdot \Omega(R) \), the first part is proved.

Now if \( P_1, P_2, \ldots, P_n \) are the minimal primes of \( R \), then \( \bigcap_{i=1}^n P_i = 0 \). Set \( A = \bigcap_{i=1}^m P_i \) and \( B = \bigcap_{i=1}^m P_j \). We show that \( B = \text{ann} \, A \). Indeed, \( BA \subseteq \bigcap_{i=1}^n P_i = 0 \) so \( B \subseteq \text{ann} \, A \). Conversely, if \( j \leq m \), then since \( P_j \supseteq (\text{ann} \, A)A = 0 \) and \( P_j \nsubseteq A \), we have \( P_j \supseteq \text{ann} \, A \). Hence \( B = \bigcap_{i=1}^m P_j \supseteq \text{ann} \, A \) and the proof is complete.

Suppose \( R * G \) is given with \( G \) finite and with \( R \) a \( G \)-prime ring. Then by [18, Lemma 3.1(i)], \( R \) has a minimal prime \( Q \) such that \( \bigcap_{x \in G} Q^x = 0 \). Furthermore, the ideals \( Q^x \) are all the minimal primes of \( R \).

Proposition 1.6. Let \( R * G \) be a crossed product with \( G \) finite and with \( R \) a \( G \)-prime ring. Let \( Q \) be a minimal prime ideal of \( R \) and let \( H \) be the stabilizer of \( Q \) in \( G \). Then \( R * G \) is prime if and only if \( (R/Q) * H \) is prime. Furthermore, if this occurs and if \( R \) is a Goldie ring, then

1. \( R * G, R/Q \) and \( (R/Q) * H \) are Goldie rings
2. \( \text{rank} \, R = [G:H] \cdot \text{rank} \, R/Q \)
3. \( \text{rank} \, R * G = [G:H] \cdot \text{rank} \, (R/Q) * H \).
Proof. Since \( R \) is \( G \)-prime we can use the notation of [18, §3]. In particular, by [18, Theorem 3.6], the maps \( \kappa^{-1} \nu \) and \( \delta \kappa \) yield a one-to-one correspondence between the prime ideals of \( R \ast G \) disjoint from \( R \) and the prime ideals of \( (R/Q) \ast H \) disjoint from \( R/Q \). Hence since 
\[ 0^{\kappa^{-1} \nu} = 0 \quad \text{and} \quad 0^{\delta \kappa} = 0, \]
as is easily seen from the definitions, we conclude that \( R \ast G \) is prime if and only if \( (R/Q) \ast H \) is prime.

Now assume that the above occurs and that in addition \( R \) is a Goldie ring. Then \( R \) is a semiprime Goldie ring so Lemma 1.5 and Proposition 1.4 imply that \( R \ast G, \ R/Q \) and \( (R/Q) \ast H \) are also Goldie rings. It remains to compute the ranks which occur. Let \( U \) be the group of units of \( R \) and let
\[ G = \{ rX \mid r \in U, x \in G \} \]
be the group of trivial units in \( R \ast G \). Then \( G \) acts on \( R \) by conjugation and \( R \) is \( G \)-prime, so \( G \) acts on \( \mathcal{D}(R) \) and \( \mathcal{D}(R) \) is \( G \)-simple.

Let \( N = Q \) in Lemma 1.5 and let the ideal \( Q \mathcal{D}(R) \) of \( \mathcal{D}(R) \) be generated by the central idempotent \( 1 - e \). Then Lemma 1.5 asserts that \( e \mathcal{D}(R) = \mathcal{D}(R/Q) \) and the latter is a simple ring since \( R/Q \) is prime. In particular, we see that \( e \) is a centrally primitive idempotent of \( \mathcal{D}(R) \). Now \( G \) permutes the centrally primitive idempotents of \( \mathcal{D}(R) \) and, since \( \mathcal{D}(R) \) is \( G \)-simple, \( G \) must act transitively. Furthermore, the stabilizer of \( e \) is surely \( \mathcal{D} = \{ rX \mid r \in U, x \in H \}, \) since \( Q \mathcal{D}(R) \cap R = Q \) by Lemma 1.5. Thus it follows that \( \mathcal{D}(R) \) is a direct sum of \( [\mathcal{D} : \mathcal{D}] = [G : H] \) rings each isomorphic to \( \mathcal{D}(R/Q) \) and therefore

\[ \text{rank } R = \text{rank } \mathcal{D}(R) = [G : H] \text{ rank } \mathcal{D}(R/Q) = [G : H] \text{ rank } R/Q \]

so (ii) is proved.

Finally, since the centrally primitive idempotents of \( \mathcal{D}(R) \) yield an orthogonal decomposition of 1 in \( \mathcal{D}(R) \ast G \) and since these idempotents are permuted transitively by \( G \subseteq \mathcal{D}(R) \ast G \), [23, Lemma 6.1.6] implies that
\[ \mathcal{D}(R) \ast G = M_n(S) \quad \text{where} \quad n = [\mathcal{D} : \mathcal{D}] = [G : H] \quad \text{and} \quad S = e(\mathcal{D}(R) \ast G)e. \]
Furthermore, it is a fairly simple matter to describe the ring \( S \). Indeed if \( a = \sum_{x \in G} a_x x \in \mathcal{D}(R) \ast G \) with \( a_x \in \mathcal{D}(R) \), then
CROSSED PRODUCTS AND FIXED RINGS

\[ e \alpha e = \sum_{x \in G} a_x e^x = \sum_{x \in G} a_x e^{x^{-1}} \]

since \( e \) is orthogonal to its distinct \( G \)-conjugates. Hence it follows that \( S = e \mathbb{Z}(R) \cdot H \). Now observe that, by Lemma 1.5, the map

\[ R \cdot H \to (R \cdot H)/(Q \cdot H) = (R/Q) \cdot H \]

extends to a map \( \mathbb{Z}(R) \cdot H \to \mathbb{Z}(R/Q) \cdot H \) with kernel \( Q \mathbb{Z}(R) \cdot H = (1-e) \mathbb{Z}(R) \cdot H \).

Thus we see that \( S \) is naturally isomorphic to \( \mathbb{Z}(R/Q) \cdot H = \mathbb{Z}((R/Q) \cdot H) \).

In particular, since \( (R/Q) \cdot H \) is prime, \( S \) is a simple Artinian ring and

\[ \text{rank } S = \text{rank } \mathbb{Z}((R/Q) \cdot H) = \text{rank } (R/Q) \cdot H. \]

Therefore since \( \mathbb{Z}(R \cdot G) = \mathbb{Z}(R) \cdot G = M_n(S) \), we conclude that

\[ \text{rank } R \cdot G = \text{rank } \mathbb{Z}(R \cdot G) = n \text{ rank } S = [G:H] \text{ rank } (R/Q) \cdot H \]

and part (iii) is proved.

It is now a simple matter to combine Propositions 1.4 and 1.6 to obtain the main result of this section.

**Theorem 1.7.** Let \( R \cdot G \) be a crossed product with \( G \) finite and with \( R \) a \( G \)-prime ring. Suppose \( Q \) is a minimal prime ideal of \( R \) and define \( H \) to be its stabilizer in \( G \). For each prime \( p \), let \( H_p \) be a Sylow \( p \)-subgroup of \( H \), let \( G_p \) be a Sylow \( p \)-subgroup of \( G \) containing \( H_p \) and let

\[ R_p \cdot G_p = (R/Q) \cdot G_p \]

be the naturally obtained crossed product. Then \( R \cdot G \) is prime if and only if \( R_p \cdot G_p \) is a prime ring for each prime \( p \). Furthermore, if this occurs and if \( R \) is a Goldie ring, then

i. \( R \cdot G, R_p \) and \( R_p \cdot G_p \) are Goldie rings

ii. \( \frac{\text{rank } R \cdot G}{\text{rank } R} \) is an integer dividing \( |G| \)

iii. \( \frac{\text{rank } R \cdot G}{\text{rank } R} = \prod_p \frac{\text{rank } R_p \cdot G_p}{\text{rank } R_p} \).
Proof. By Proposition 1.6, we know that \( R \ast G \) is prime if and only if \( (R/Q) \ast H \) is prime. Similarly, since \( R_p \) is \( G_p \)-prime and since the stabilizer of \( Q/\cap_{x \in G_p} Q_x = Q_p \) in \( G_p \) is clearly \( G_p \cap H = H_p \), we see, from Proposition 1.6 again, that \( R_p \ast G_p \) is prime if and only if \( (R_p/Q_p) \ast H_p = (R/Q) \ast H_p \) is prime. Furthermore, Proposition 1.4 applied to \( (R/Q) \ast H \) asserts that \( (R/Q) \ast H \) is prime if and only if \( (R/Q) \ast H_p \) is prime for all \( p \). Therefore, combining all of these implications shows immediately that \( R \ast G \) is prime if and only if \( R_p \ast G_p \) is prime for all \( p \). We assume below that this occurs.

Now suppose that \( R \) is a Goldie ring. Then \( R \) is a semiprime Goldie ring and therefore so is \( R_p \) by Lemma 1.5. Hence \( R \ast G \) and \( R_p \ast G_p \) are Goldie by Proposition 1.6 (i) and part (i) is proved. Furthermore, by that proposition, applied to both \( G \) and \( G_p \) we have

\[
\frac{\text{rank } R \ast G}{\text{rank } R} = \frac{\text{rank } (R/Q) \ast H}{\text{rank } R/Q}
\]

and

\[
\frac{\text{rank } R_p \ast G_p}{\text{rank } R_p} = \frac{\text{rank } (R/Q) \ast H_p}{\text{rank } R/Q}.
\]

Thus, since \( |H| \) divides \( |G| \), (ii) and (iii) follow immediately from Proposition 1.4(ii)(iii) and the theorem is proved.

A special case of the above is the following known result which can be found in [16, page 293] and in an unpublished note of K. Brown. Observe that \( R \) is an Ore domain if and only if it is a prime Goldie ring of rank 1. Thus, by Proposition 1.4, we obtain immediately

**Corollary 1.8.** Let \( R \ast G \) be a crossed product with \( R \) an Ore domain and with \( G \) a finite group. For each prime \( p \), let \( G_p \) be a Sylow \( p \)-subgroup of \( G \). Then \( R \ast G \) is an Ore domain if and only if \( R \ast G_p \) is an Ore domain for all primes \( p \).

We remark that this corollary has a simple direct proof, as given in the above references, and we briefly sketch this for the sake of completeness. Let
D(R) be the division ring D. Then for each subgroup H of G, 
\( D(R \circ H) = D \circ H \) is Artinian and we need only show that \( D \circ G \) is a division ring if and only if each \( D \circ G_p \) is a division ring. One direction is of course trivial. Indeed suppose \( D \circ G \) is a division ring. Then for each \( p \), \( D \circ G_p \) is an Artinian ring without zero divisors and therefore surely a division ring. Conversely suppose that each \( D \circ G_p = D_p \) is a division ring and observe that as right modules \( \dim_D D_p = |G_p| \). Let I be a nonzero right ideal of \( D \circ G \). Then I is a right \( D_p \)-vector space, so clearly \( \dim_D I = (\dim_D D_p) (\dim_D D_p) \) and hence \( |G_p| \) divides \( \dim_D I \). Thus \( |G| = \prod_p |G_p| \) divides \( \dim_D I \) and, since \( \dim_D D \circ G = |G| \), we conclude that \( I = D \circ G \). Thus \( D \circ G \) has no nontrivial right ideals so it is a division ring and the corollary is proved.

§ 2. Prime Skew Group Rings

In this section we study prime skew group rings \( RG \) with \( G \) not necessarily finite but with \( R \) a prime ring. In particular, we determine the group theoretic structure of \( \Delta^+(G) \cap G_{\text{inn}} \) when \( R \) is a domain. The first three results below have already appeared in the literature (see [20] and [22]). However, the additional observation here concerning the \( G \)-action in Lemma 2.1 makes for more efficient proofs throughout.

We follow the notation of [21]. Thus let \( R \) be a prime ring and let \( S = Q_0(R) \) be its Martindale ring of quotients. Then the extended centroid \( C \) of \( R \) is, by definition, the center of \( S \) and \( C \) is a field which is in fact equal to the centralizer of \( R \) in \( S \). An automorphism \( \sigma \) of \( R \) is said to be \( X \)-inner if and only if it is induced by conjugation by a unit of \( S \). In other words, these automorphisms arise from those units \( s \in S \) with \( s^{-1}Rs = R \). Certainly, if \( s \) and \( t \) are two such units, then so is \( st \) and therefore [21, Lemma 2.1(iv)] implies that the set of all \( X \)-inner automorphisms of \( R \) is a normal subgroup of the group of all automorphisms of \( R \). Furthermore, for each \( X \)-inner automorphism \( \sigma \), the corresponding conjugating element \( s \in S \) is clearly unique up to multiplication by nonzero elements of \( C \).
Let \( G \) be a group acting as automorphisms on \( R \) and set
\[
G_{\text{inn}} = \{ x \in G \mid x \text{ is an } X\text{-inner automorphism of } R \}.
\]
If \( W \) is a subgroup of \( G_{\text{inn}} \), then the algebra of the group \( B(W) \) (see [13]) is the linear span of all units \( s \in S \) such that \( s^{-1}R_s = R \) and such that the conjugation map \( s \) agrees with \( w \) on \( R \) for some \( w \in W \).

It is trivial to see that \( B(W) \) is a \( C \)-subalgebra of \( S \). Furthermore \( G \) acts naturally on \( S \) and if \( W < G \), then \( B(W) \) is a \( G \)-stable subalgebra.

Again let \( G \) act on \( R \), let \( RG \) denote the skew group ring obtained and let \( SG \) denote the natural extension. If \( W \subset G_{\text{inn}} \), then it follows from [21, Lemma 2.3] that \( SW = S \otimes C E(W) \), where \( E(W) \) is the centralizer of \( S \) in \( SW \) and where \( E(W) \) is isomorphic to some twisted group algebra \( C^t[W] \). In addition, if \( W < G \), then \( G \) acts on \( E(W) \) by conjugation.

**Lemma 2.1.** Let \( RG \) be a skew group ring with \( R \) prime and let \( W \subset G_{\text{inn}} \). Then the augmentation map \( \varphi : E(W) \to B(W)^{\text{op}} \) given by
\[
\varphi \left( \sum_{w \in W} s_w \right) = \sum s_w
\]
is a \( C \)-algebra epimorphism. Furthermore, if \( W < G \), then \( \varphi \) commutes with the action of \( G \).

**Proof.** It is clear that \( E(W) \) is the set of all elements \( \sum_{w \in W} s_w \) such that each summand \( s_w \) centralizes \( S \). Moreover since \( w \) is an \( X \)-inner automorphism, it then follows immediately that each \( s_w \) is either zero or a unit in \( S \) acting like \( w^{-1} \) on \( R \). In other words, each \( s_w \in B(W) \), so \( \varphi(\sum s_{w}) = \sum s_{w} \) belongs to \( B(W) \) and hence can be thought of as an element of the opposite ring \( B(W)^{\text{op}} \). It is now trivial to see that \( \varphi : E(W) \to B(W)^{\text{op}} \) is a \( C \)-linear map which is onto.

Thus it remains to consider the properties of multiplication and of \( G \)-action if \( W < G \).
CROSSED PRODUCTS AND FIXED RINGS

\[ \alpha = \Sigma_v a_v v, \quad \beta = \Sigma_w b_w w \in E(W) \] and let * denote multiplication in \( B(W)^{OP}. \) Then

\[ \alpha \beta = \Sigma_{v,w} a_v b_w \cdot \Sigma_{v,w} a_v b_w * v w \]

since \( b_w \in S \) commutes with each \( a_v \) and hence

\[ \varphi(\alpha \beta) = \Sigma_{v,w} b_w a_v = (\Sigma_w b_w)(\Sigma_v a_v) \]
\[ = (\Sigma_v a_v) * (\Sigma_w b_w) = \varphi(\alpha) * \varphi(\beta). \]

Thus \( \varphi \) is a ring homomorphism. Finally if \( W \triangleleft G \) and if \( x \in G, \) then

\[ \alpha^x = \Sigma_v a_v^x v^x \]
so

\[ \varphi(\alpha^x) = \Sigma_{v,x} a_v^x = (\Sigma_v a_v)^x = \varphi(\alpha)^x \]
and the lemma is proved.

The following result is essentially \([22, \S 1, \text{Proposition 7}]\) and it is also implicit in \([20]\).

**Theorem 2.2.** Let \( RG \) be a skew group ring with \( R \) prime and set \( W = \Delta^+(G) \cap G_{\text{inn}}. \) Then \( RG \) is prime if and only if \( B(W) \) is \( G \)-simple and \( \varphi : E(W) \to B(W)^{OP} \) is an isomorphism.

**Proof.** Suppose \( B(W) \) is \( G \)-simple and \( \varphi \) is an isomorphism. Then certainly \( E(W) = C^+[W] \) is \( G \)-simple. Furthermore, if \( H \triangleleft G \) and \( H \subset W, \) then \( E(H) = C^+[H] \) is also \( G \)-simple since any \( G \)-invariant ideal of \( E(H) \) extends naturally to a \( G \)-invariant ideal of \( E(W). \) Thus it follows from \([21, \text{Theorem 2.8}]\) that \( RG \) is prime.

Conversely suppose \( RG \) is prime and let \( H \) be a finite normal subgroup of \( G \) contained in \( W. \) Then \( E(H) \) is \( G \)-prime, by \([21, \text{Theorem 2.8}], \) and hence \( G \)-simple since it is an Artinian ring. Furthermore, since \( W = \Delta^+(G) \cap G_{\text{inn}} \) is clearly generated by all such groups \( H, \) it follows that \( E(W) \) is also \( G \)-simple. But \( \varphi : E(W) \to B(W)^{OP} \) is a \( G \)-epimorphism, so we must have \( \ker \varphi = 0 \) and \( B(W) \cong E(W)^{OP} \) is also \( G \)-simple.
Note that we have also shown above that $RG$ is prime if and only if $E(W)$ is $G$-simple and in fact this holds for arbitrary crossed products over prime rings. Moreover there is an easy criterion for deciding when $\varphi$ is an isomorphism. Indeed if $b_w \in B(W)$ is a unit which acts on $R$ by conjugation in the same way $w \in W$ does, then $\varphi$ is certainly an isomorphism if and only if $\{b_w \mid w \in W\}$ is a $G$-basis for $B(W)$. The following simple example illustrates some of the above happenings.

**Example.** Let $F$ be a field of characteristic different from 2 which admits an automorphism $-\phi$ of order 2 and let $R = M_2(F)$. Then $R$ is a simple ring so $S = R$ and $C = F$. Let $a, b \in R$ be the matrices

$$a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and observe that $a^{-1}b a = -b$. We can now define an action of the fours group $G = \langle x \rangle \times \langle y \rangle$ on $R$ as follows. We let $y$ act via conjugation by $b$ and we let $x$ act via the composition of conjugation by $a$ followed by the field automorphism $-\phi$ naturally extended to $M_2(F)$. Since $a, b$ and $-\phi$ all have order 2 and since $a$ and $b$ commute modulo scalars, it is clear that this yields a well defined faithful action of $G$. Furthermore, we have $W = G_{\text{inn}} = \langle y \rangle$ and then $B(W) = F + Fb$ is the set of diagonal matrices in $R$.

Now $RW = R \otimes_F E(W)$ and $E(W)$, being spanned by 1 and $b$, is isomorphic to the ordinary group algebra $F[W]$ since $(by)^2 = 1$. Thus $RW \cong R \oplus R$. Furthermore, the map $\varphi : E(W) \to B(W)^{\text{op}} = B(W)$ is given by $\varphi(f_1 + f_2 b) = f_1 + f_2 b$ and this is certainly an isomorphism. Since $B(W)$ is clearly $G$-simple, due to the conjugation action of the matrix $a$, we conclude from Theorem 2.2 that $RG$ is prime. Indeed one can easily show that $RG \cong M_4(F)$. Moreover, although $RW$ is not a prime ring, it is $G$-prime since the action of $x \in G$ interchanges the two central idempotents $(1 + b y)/2$ and $(1 - b y)/2$. 

Downloaded by [ ] at 16:54 17 October 2015
Theorem 2.3. \([20]\). Let \(RG\) be a skew group ring with \(R\) a domain and set \(W = \Delta^+(G) \cap G_{\text{inn}}\). Then \(RG\) is prime if and only if \(E(W) = \mathbb{C}[W]\) is a division ring.

**Proof.** If \(E(W)\) is a division ring, then it is certainly \(G\)-simple and \(\phi: E(W) \to B(W)^{op}\) is certainly a one-to-one map. Thus, by Theorem 2.2, \(RG\) is prime. Conversely suppose \(RG\) is prime. Then, by Theorem 2.2 again, \(E(W) = B(W)^{op}\) and, by [20, Corollary 2], \(B(W)\) is a domain, since \(R\) is a domain and \(B(W)\) is contained in the normal closure of \(R\) in \(S\). Thus, since \(W\) is a locally finite group, \(E(W) = \mathbb{C}[W]\) is a domain algebraic over \(\mathbb{C}\) and hence we conclude that \(E(W)\) is a division ring.

This now motivates the following partial characterization of twisted group algebras which are division rings.

**Proposition 2.4.** Let \(F[G]\) be a twisted group algebra of the finite group \(G\). If \(F[G]\) is a division algebra, then we have either

i. \(G^t\) is cyclic and \(G\) is nilpotent; or

ii. \(\text{char } F = 0\), \(G^t \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times H\) where \(H\) is cyclic of order prime to 6, and \(G\) is either nilpotent or \([G: \mathbb{C}_G(Z_2 \times Z_2)] = 3\) and \(\mathbb{C}_G(Z_2 \times Z_2)\) is nilpotent.

**Proof.** Let \(G\) be the group of trivial units in \(F[G]\) so that

\[G = \{f \in F^* | f \in F \setminus \{0\}, \times, G\}.\]

Then \(F^t\) is a central subgroup of \(G\) of finite index with \(G/F^t = G\). Since \(G\) is center-by-finite, [23, Lemma 4.1.4] implies that \(W = G^t\) is finite. Moreover, if \(V = W \cap F^t\), then \(W/V \cong G^t\). Observe that \(W\) is a finite subgroup of a division ring, so the characterization due to Amitsur ([1]) can apply. However the situation here is actually much more special, so we will not require that work. We proceed in a series of steps.

**Step 1.** If \(W\) contains \(Q_8\), the quaternion group of order 8, then \(\text{char } F = 0\) and \(F\) does not contain a primitive cube root of 1.
Proof. If char \( F = p > 0 \), then \( GF(p)Q_8 \), the \( GF(p) \)-linear span of the elements of \( Q_8 \) is a finite subring of a division ring and hence is a division ring. But all finite division rings are commutative so this is a contradiction. Hence char \( F = 0 \).

Since \( Q_8 \subset F^*[G] \), the element of order 2 in \( Q_8 \) is \( -1 \) and we have elements \( i, j, k \in F^*[G] \) with the usual properties
\[
i^2 = j^2 = k^2 = -1, \quad ij = k, \quad jk = i, \quad ki = j,
\]
\[
ji = -k, \quad kj = -i, \quad ik = -j.
\]
Also it is easy to see that \( i, j, k \) are linearly independent over \( F \).

Suppose \( F \) contained \( \omega \), a primitive cube root of 1. Then, since
\[
\omega = (\sqrt[3]{-1} + \sqrt[3]{-1})/2, \quad \sqrt[3]{-1} \in F.
\]
Hence setting
\[
\alpha = \sqrt[3]{-1} + i + j + k \quad \text{and} \quad \overline{\alpha} = \sqrt[3]{-1} - i - j - k,
\]
then these are nonzero elements of \( F^*[G] \) with \( \alpha \overline{\alpha} = -3 + (1+1+1) = 0 \), a contradiction.

Step 2. If \( w \in W \) has prime order \( p \), then \( w \in V \) and hence is central in \( G \).

Proof. If \( w \not\in V \), then \( w = f^x \) for some \( f \in F^* \) and \( x \in G \) with \( x \) of order \( p \). But \( w \) has order \( p \) so
\[
(1-w)(1+w+w^2+\ldots+w^{p-1}) = 0
\]
and this yields nontrivial zero divisors in \( F^*[G] \), a contradiction.

Step 3. \( W \) is either (i) cyclic, or (ii) \( Q_8 \times C \) where \( C \) is cyclic of order prime to 6. Moreover the latter case can only occur if char \( F = 0 \).

Hence \( G' \) is abelian and in fact \( G' \) is either cyclic or \( G' = Z_2 \times Z_2 \times D \) where \( D \) is cyclic of order prime to 6.

Proof. Let \( P \not\in (1) \) be a Sylow \( p \)-subgroup of \( W \). Then by Step 2, all elements of \( P \) of order \( p \) are contained in \( F \). Hence \( P \) has at most one subgroup of order \( p \) and we conclude that either \( P \) is cyclic or \( p = 2 \) and \( P \) is quaternion (see [12, 8.2]). If \( P \) is cyclic, then since \( \Omega_1(P) \subset F \) we have \( \Omega_1(P) \) central in \( G \). It follows from this that \( \Omega_1(P) \) acts on \( P \) in such a way that it centralizes \( \Omega_1(P) \). Hence
$N_W(P)$ must act like a $p$-group and since $P$ is abelian we conclude that $N_W(P) = Z_w(P)$. By Burnside's transfer theorem ([12, IV.2.6]), $W$ has a normal $p$-complement.

Now suppose $P$ is quaternion. By Step 2, if $3 \mid |W|$, then $F$ contains a primitive cube root of 1 and this contradicts Step 1. Thus $3 \nmid |W|$ and also char $F = 0$. If $H$ is a subgroup of $P$, then $H$ is either cyclic or quaternion and thus $\operatorname{Aut} H$ is a $(2,3)$-group. But $3 \nmid |W|$ so $N_W(H)/C_W(H)$ is a 2-group for all such $H$. It now follows from Frobenius' transfer theorem ([12, IV.5.8(a)]) that $W$ has a normal $p = 2$-complement in this case also.

Hence $W$ has normal $p$-complements for all primes so $W$ is nilpotent.

It is now clear that $W$ is either (i) cyclic or (ii) $Q \times C$ where $Q$ is quaternion and $C$ is cyclic of order prime to 6. Also the latter can occur only for char $F = 0$. Suppose in (ii) that $Q$ is generalized quaternion so that $|Q| = 16$. Then $Q$ has a characteristic cyclic subgroup $D$ of index 2, and therefore $D$ is characteristic in $W$ and normal in $G$. But Aut $D$ is abelian, so this implies that $W = G'$ centralizes $D$, a contradiction since $D$ is not central in $Q$. Hence we can have only $Q = Q_8$.

Finally $W/V \cong G'$. Hence if $W$ is cyclic then certainly $G'$ is cyclic. On the other hand, if $W = Q_8 \times C$, then since the element of order 2 in $Q_8$ is contained in $V$, by Step 2, we conclude that $G' = W/V \cong Z_2 \times Z_2 \times (C/C \cap V)$ and the latter factor is cyclic of order prime to 6.

Step 4. In case (i), $G$ is nilpotent. In case (ii) either $G$ is nilpotent or $[G : G'(Z_2 \times Z_2)] = 3$ and $G'(Z_2 \times Z_2)$ is nilpotent.

Proof. Let $P$ be a Sylow $p$-subgroup of $W$. Then $P < W$ so $P < G$. Moreover if $P$ is cyclic, then since $\Omega_1(P)$ is central in $G$, by Step 2, $G$ acts like a $p$-group on $P$. It follows that $(P, G, G, \ldots, G) = (1)$ for some $n$ and hence that $P \subseteq \pi_n(G)$, the $n$th term of the upper central series of $G$. It therefore follows that if $W$ is cyclic, then $W \subseteq \pi_n(G)$.
for some $n$. But $W = \mathbb{C}^*$, so $\mathbb{C}$ is nilpotent and hence so is $G$.

In case (ii), with $W = Q_8 \times C$, we know at least that $C \leq Z_n(\mathbb{C})$. Furthermore, if $\mathbb{C}$ acts like a 2-group on $Q_8$, then also $Q_8 \leq Z_n(\mathbb{C})$ for some $n$, so again $\mathbb{C}$ and $G$ are nilpotent. Thus if $\mathbb{C}$ is not nilpotent, then $\mathbb{C}$ cannot act like a 2-group on $Q_8$. Observe that $\text{Aut} Q_8 \neq \text{Sym}_4$ with $Q_8$ acting on itself as the fours subgroup of $\text{Sym}_4$. Hence $\mathbb{C}$ acts as a group of order $4, 8, 12$ or $24$. But $4$ and $8$ are excluded since $\mathbb{C}$ does not act like a 2-group and $24$ is excluded since $\mathbb{C}/C(Q_8) = \text{Sym}_4$ and $\mathbb{C}$ has a normal subgroup $\mathfrak{h}$ of index $3$ with $|\mathfrak{h}/C(Q_8)| = 4$. It is now clear that $\mathfrak{h}$ is nilpotent, so $G$ has a normal subgroup $N$ of index $3$ which is nilpotent. Since $N$ is clearly $C_G(Z_2 \times Z_2)$, this step is proved and hence so is the proposition.

The above can presumably be sharpened further. However it is not clear that more detail would be at all useful or interesting. It is now a simple matter to combine the preceding two results to obtain.

**Theorem 2.5.** Let $RG$ be a skew group ring with $R$ a domain and set $W = \Delta^t(G) \cap C_{\text{inn}}$. If $RG$ is prime, then each $p$-subgroup of $W$ is nilpotent and we have either

1. $W'$ is locally cyclic and $W$ is locally nilpotent; or
2. $\text{char } R = 0$, $W' = Z_2 \times Z_2 \times H$ where $H$ is locally cyclic with no elements of order $2$ or $3$, and either $W$ is locally nilpotent or $[W : C_W(Z_2 \times Z_2)] = 3$ and $C_W(Z_2 \times Z_2)$ is locally nilpotent.

**Proof.** It follows from Theorem 2.3 that $E(W) = C^t[W]$ is a division ring. Thus if $L$ is any subgroup of $W$, then $C^t[L]$ is certainly a domain, and hence if $L$ is finite, then $C^t[L]$ is a division ring so Proposition 2.4 applies. Now using the fact that $W$ is locally finite, we see immediately that cases (i) and (ii) of Proposition 2.4 carry over to yield cases (i) and (ii) of this result. Finally, let $P$ be a $p$-subgroup of $W$. Then (i) and (ii)
show that either $P'$ is finite or $P' \cong \mathbb{Z}^\infty$, the Prüfer group. If the former occurs, then surely $P$ is nilpotent. On the other hand, if the latter occurs, then since $\mathbb{Z}^\infty$ has no proper subgroups of finite index and since $[P : \mathcal{C}_P(x)] < \infty$ for all $x \in P$, we conclude that $P'$ is central in $P$ and hence $P$ has class 2. In the above, we of course used the fact that $W \subset \Delta^+(G)$.

We now wish to construct some examples and, in this regard, part (ii) of the following lemma is particularly useful. The proof we offer is based on part (i) and hence on group ring techniques. Furthermore, this first part can clearly be generalized, following ideas of Formanek to yield a twisted group algebra analog of [23, Theorem 4.5.8]. (See [21, Theorem 3.11] for a brief discussion on a related topic.)

**Lemma 2.6.** Let $F^t[G]$ be a twisted group algebra of $G$ over the field $F$.

1. If $\Delta(G) = \{1\}$, then $F^t[G]$ is prime with extended centroid equal to $F$.

2. If $F^t[G]$ is a domain, then there exists a domain $R$ containing $F^t[G]$ such that $R$ is an $F$-algebra with extended centroid $F$.

**Proof.** (1) Let $\theta : F^t[G] \to F^t[\Delta(G)]$ denote the natural projection. Then, since $\Delta(G) = \{1\}$ here, we see that in this case $\theta$ is just the ordinary trace map $\theta : F^t[G] \to F$. Furthermore, it is well known that $\Delta(G) = \{1\}$ implies $F^t[G]$ is prime (see [21, Theorem 2.8] for example).

Now let $A$ be a nonzero ideal of $F^t[G]$ and let $f : A \to F^t[G]$ represent an element in the center of $Q_0(F^t[G])$. Then, by [2, Theorem 3], $f$ is in fact a bimodule homomorphism. Since $A \neq 0$, we can choose $\beta \in A$ with $\theta(\beta) = 1$ and let $\alpha \in A$ be arbitrary. We compute $f(\alpha \mathcal{X} \beta)$ for $x \in G$ in two different ways. Indeed since $\alpha, \beta \in A$ and $f$ is a bimodule map we have $f(\alpha \mathcal{X} \beta) = \alpha \mathcal{X} f(\beta)$ and $f(\alpha \mathcal{X} \beta) = f(\alpha \mathcal{X} \beta)$. Thus

$$f(\alpha \mathcal{X} \beta) = \alpha \mathcal{X} f(\beta)$$

for all $x \in G$ and [21, Lemma 3.8] yields

$$f(\alpha) \cdot \theta(\beta) = \alpha \cdot \theta(f(\beta)).$$
But \( \vartheta(\beta) = 1 \) so we have \( f(\alpha) = \alpha \cdot \vartheta(f(\beta)) \) and we see that \( f \) is just multiplication by the element \( \vartheta(f(\beta)) \in F \). It is now clear that \( F \) is the extended centroid of \( F^+[G] \).

(ii) Let \( F^+[G] \) be a domain. If \( G = \langle 1 \rangle \), we can take \( R = F = F^+[G] \) so assume now that \( G \neq \langle 1 \rangle \). Let \( Z \) be an infinite cyclic group and observe that the free product \( R = F^+[G] \ast F[Z] \) is isomorphic to \( F^+[G \ast Z] \), a certain twisted group algebra of the free product \( G \ast Z \) over \( F \). Since \( F^+[G] \) and \( F[Z] \) are domains, it follows from the Cohn-Lewin theorem ([23, Theorem 13.3.7]), which applies equally well to twisted group algebras, that \( F^+[G \ast Z] \) is also a domain. Finally since \( G \neq \langle 1 \rangle \), we have \( \Delta(G \ast Z) = \langle 1 \rangle \) and part (i) applied to \( F^+[G \ast Z] \) yields the result.

The goal now is to show that the possibilities listed for \( W \) in Theorem 2.5 can all occur. To this end, suppose that \( G \) is a group with \( G = \Delta^+(G) \) and such that \( F^+[G] \) is a twisted group algebra which is a division ring. By (ii) above we can find a domain \( R \) containing \( F^+[G] \) such that \( R \) is an \( F \)-algebra with extended centroid \( F \). Since \( F \) is central in \( R \), it is clear that conjugation yields a well defined action of \( G \) on \( R \) and we form the skew group ring \( RG \). Then certainly \( G = G_{\text{inn}} \cap \Delta^+(G) = G \). Moreover, since \( F = C \) is the extended centroid of \( R \), \( B(W) = F^+[G] \) is a division ring and the elements \( \{x \cdot R \mid x \in G\} \) are \( C \)-linearly independent. Thus the map \( \varphi \) of Lemma 2.1 is surely an isomorphism so \( E(W) = B(W)^{op} \) is a division ring. Theorem 2.3 now implies that \( RG \) is prime. In other words, twisted group algebras which are division rings give rise to suitable examples of prime skew group rings. We now construct appropriate twisted group algebras. Let \( Q \) denote the field of rational numbers.

**Example.** Let \( D = Q + Qi + Qj + Qk \) be the ordinary quaternion division algebra over \( Q \). Then \( D \) is clearly a twisted group algebra of the fours group \( Z_2 \times Z_2 \) over \( Q \). Note that \( D \) admits an automorphism \( \varphi \) of order 3 which cyclically permutes the generators \( 1, i, j, k \). Thus we can
CROSSED PRODUCTS AND FIXED RINGS

Let \( D[x] = D[x; \sigma] \) be the skew polynomial ring in \( x \) over \( D \) with \( x \) acting like \( \sigma \). Then \( D[x] \) is certainly a ring without zero divisors and \( Q[x^3] \) is certainly a central subring. It is therefore a trivial matter to form the ring of fractions \( E = (Q[x^3])^{-1}(D[x]) \). Note that \( E \) is an algebra over the field \( F = (Q[x^3])^{-1}(Q[x^3]) \) and that \( E \) has no zero divisors. Moreover since \( E \) has an \( F \)-basis consisting of the 12 elements \( x^5, ix^5, jx^5, kx^5 \) with \( s = 0, 1, 2 \), we see easily that \( E = F[G] \), some twisted group algebra of \( G = \text{Alt}_4 \) over \( F \). Since \( E \) is finite dimensional over \( F \), it is therefore a division ring.

**Example.** Let \( K = Q(\zeta) \) be the cyclotomic field extension of \( Q \) generated by \( \zeta \), a primitive \( p \)-th root of unity for some prime \( p \). Moreover let \( D = Q(\chi) \), where \( \chi \) is a primitive \( p^{n+1} \)-st root of unity. Then \( (D : K) = p^n \) and \( D \) is a \( K \)-algebra with basis \( 1, \chi, \chi^2, \ldots, \chi^{p^n-1} \). Thus \( D \) is a twisted group algebra of the cyclic group \( Z_{p^n} \) over the field \( K \). Note that \( D \) admits the field automorphism \( \sigma : x \to x^{1+p} \) which acts trivially on \( K \). We can therefore form the skew polynomial ring \( D[y] = D[y; \sigma] \) with \( y \) acting like \( \sigma \) on \( D \). Certainly \( D[y] \) is a ring without zero divisors containing the central subring \( K[y^{p_m}] \) where \( m \) is any fixed integer with \( m \geq n \). It is now a trivial matter to form the ring of fractions \( E = (K[y^{p_m}])^{-1}(D[y]) \). Then \( E \) has no zero divisors and \( E \) is an algebra over the field \( F = (K[y^{p_m}])^{-1}(K[y^{p_m}]) \). Furthermore, \( E \) has as an \( F \)-basis the \( p^{n+m} \) elements \( x^iy^j \) with \( 0 \leq i < p^n, 0 \leq j < p^m \). Hence \( E \) is easily seen to be \( F[G] \), some twisted group algebra of the group

\[
G = \langle a, b | a^{p^n} = 1, b^{p^m} = 1, b^{-1}ab = a^{1+p} \rangle
\]

of order \( p^{n+m} \). Finally since \( E \) is a finite dimensional algebra with no zero divisors, it must be a division ring. We remark that the above construction can also be achieved in characteristic \( q \neq 0 \) provided \( p \) and \( q \) are suitably related (see [23, Lemma 14.3.7]).

It is a simple matter to generalize this argument and obtain somewhat more interesting groups. Thus let \( K \) be generated over the rationals by \( p \)-th roots of unity for each prime \( p \) and let \( D \) be generated over \( K \) by \( p^{n+1} \)-st roots.
of unity $x_p^*$, where $n_p$ is an integer depending upon $p$. Then we form
the skew polynomial ring $D[y]$ where $y$ denotes an infinite number of
variables $y_p$, one for each $p$, and where $y_p$ acts on $D$ as the
Galois automorphism $x_p \mapsto x_p^{1+p}$, $x_q \mapsto x_q (q \not= p)$. Finally we localize
at $K[y^m]$, where the latter is the central polynomial ring generated by the
elements $y_p$ raised to the $m_p$-th power for fixed $m_p \equiv n_p$. Having
done this, we obtain a twisted group algebra of a group $G$ which is the weak
direct product of the finite $p$-groups as described above. Thus certainly
$G = \Delta^+(G)$ and $G$ is nilpotent if and only if the $n_p$'s are bounded.
Moreover, the twisted group algebra is certainly a domain and it is in fact a
division ring since $G$ is locally finite.

**Example.** Finally fix a prime $p$ and for each $n$ let $e_n$ denote a
primitive $p^n$-th root of unity over $Q$. Let $K = Q(e_1^p)$, $D = Q(e_1, e_2, \ldots)$
and form the ordinary polynomial ring $D[x]$ where $x$ denotes an infinite
number of variables $x_1, x_2, \ldots$. Furthermore, let $D[x][y]$ be the skew
polynomial ring, where $y$ denotes the variables $y_1, y_2, \ldots$ and $y_n$
acts on $D[x]$ by centralizing $D$ and by sending $x_n \mapsto e_n x_n$, $x_m \mapsto x_m (m \not= n)$
Observe that $D[x][y]$ is a domain containing the central subring $T$
generated by $K$, $x_n^{p^n}$ and $y_n^{p^n}$ for all $n$. Furthermore $E = T^{-1}(D[x][y])$
is easily seen to be a twisted group algebra of a certain $p$-group $G$ over the
field $F = T^{-1}T$. We can of course precisely write down the generators and
relations for $G$, but it suffices to say that $G'$ is a central subgroup
isomorphic to the Prufer group $\mathbb{Z}_p^\infty$, and $G/G'$ is isomorphic to the
weak direct product of two copies of $\mathbb{Z}_p$ for each $n$. Moreover $G = \Delta^+(G)$
and, since $G$ is locally finite and $F^+[G]$ is a domain, we conclude that
$F^+[G]$ is a division ring. Thus we see that all the structures described in
Proposition 2.4 and Theorem 2.5 do indeed occur.

§ 3. Modules over Fixed Subrings

Let $R$ be a ring and let $G$ be a finite group acting by automorphisms on
$R$. The goal of this final section is to present simple and unified proofs of some
CROSSED PRODUCTS AND FIXED RINGS

results relating the structure of $R$ to the structure of the fixed subring $R^G = \{ r \in R \mid r^g = r \text{ for all } g \in G \}$ of $R$. Some of these results were previously known, some are extensions of earlier results. Our proofs are based on a few elementary observations on module and bimodule correspondences along the lines of [17, Lemma 2.4].

We let $RG$ denote the skew group ring of $G$ over $R$ so that $RG$ is a crossed product with trivial factor set and with multiplication given by the rule $(rg)(sh) = rsg$ for $r, s \in R$ and $g, h \in G$. Throughout this section we assume that $|G|^{-1} R$ and we set \[
ed e = |G|^{-1} \sum_{g \in G} g \in RG \]
so that $eg = e = ge$ for all $g \in G$ and $e^2 = e$. Moreover, for any $r \in R$ we have $ere = (|G|^{-1} \sum_{g \in G} g^r)e = t_G(r)e$, where by definition $t_G(r) = |G|^{-1} \sum_{g \in G} g^r$, surely an element of $R^G$. In particular since $t_G(R^G) = R^G$ we have
\[
ed e R G e = t_G(R)e = R^G e. \]

We now consider modules over $R$, $RG$ and $R^G$ and for the most part we study the behaviour of a given right $R$-module $V$ under restriction to $R^G$. The main idea is to first pass from $V$ to the induced $RG$-module $V \otimes_R RG$ and then use the fact that $R^G$ is embedded in $RG$ via the isomorphism $R^G \cong R^G e = e RG e$. Standard idempotent techniques then yield information on $V_{RG}$. For later applications we state the following two lemmas in terms of bimodules. If $V$ is an $(A, S)$-bimodule for the two rings $A$ and $S$, then we let $\mathcal{L}(V_{AS})$ denote the lattice of $(A, S)$-subbimodules of $V$.

**Lemma 3.1.** Let $G$ be a finite group acting on a ring $R$ and assume that $|G|^{-1} R$. Let $A$ be any ring and let $V$ be an $(A, R)$-bimodule. Then the induced module $W = V \otimes_R RG$ is an $(A, RG)$-bimodule. Furthermore there exist inclusion preserving maps
\[
\sigma : \mathcal{L}(V_{AR}) \to \mathcal{L}(A_{WRG}) \]
and
\[
\tau : \mathcal{L}(A_{WRG}) \to \mathcal{L}(V_{AR}) \]
such that for $U \in \mathcal{F}(V_G)$ and $X_1, X_2 \in \mathcal{F}(A_W R_G)$ we have $U^{\sigma_T} = U$ and $(X_1 \oplus X_2)^T = X_1^T \oplus X_2^T$.

**Proof.** Each element of $W = V \oplus_R R_G$ can be uniquely written as $w = \sum_{g \in G} v g \otimes g$ with $v \in V$. We set $\text{tr}(w) = v \in V$ so that $\text{tr}: W \to V$ is certainly an $(A, R)$-bimodule map. Furthermore, we set $w^T = \text{tr}(we)$ for $w \in W$. Since $e$ commutes with the elements of $R^G$ it follows that $\tau$ is an $(A, R^G)$-bimodule map. Therefore, if $X \in \mathcal{F}(A_W R_G)$ then $X^T \in \mathcal{F}(A_W R_G)$ and if $X_1, X_2 \in \mathcal{F}(A_W R_G)$ then $(X_1 + X_2)^T = X_1^T + X_2^T$.

Moreover, if $X_1 \cap X_2 = 0$ then certainly $X_1 e \cap X_2 e = 0$ and since the elements of $W$ are easily seen to be of the form $w = G|\text{tr}(w) \otimes e$ we also have $\text{tr}(X_1 e) \cap \text{tr}(X_2 e) = 0$. Thus $(X_1 \oplus X_2)^T = X_1^T \oplus X_2^T$.

Moreover, $X_1 \subseteq X_2$ clearly implies that $X_1^T \subseteq X_2^T$.

Now let $U \in \mathcal{F}(V_G)$ and define $U^{\sigma} = (U \otimes e) R_G \subset W$.

Then $U^{\sigma} \in \mathcal{F}(A_W R_G)$ and $U_1 \subseteq U_2$ certainly implies that $U_1^{\sigma} \subseteq U_2^{\sigma}$ for $U_1, U_2 \in \mathcal{F}(V_G)$. Finally, $U^{\sigma} e = U \otimes e R_G e = U \otimes R^G e = U \otimes e$, since $U$ is a right $R^G$-module, and hence $U^{\sigma_T} = \text{tr}(U \otimes e) = |G|^{-1} U = U$.

The lemma is proved.

The following result is a version of the well known Maschke theorem. Although it is stated for bimodules and crossed products here, the classical proof still works in this situation. For the readers convenience we include the argument.

**Lemma 3.2.** Let $R \ast G$ be a crossed product with $G$ finite and $|G|^{-1} \in R$. Let $W$ be an $(A, R \ast G)$-bimodule, for any ring $A$, and let $V \in \mathcal{F}(A_W R_{\ast G})$. If $V$ has a complement in $\mathcal{F}(A_W R)$, then $V$ also has a complement in $\mathcal{F}(A_W R_{\ast G})$.

**Proof.** By assumption there exists $X \in \mathcal{F}(A_W R)$ with $V \oplus X = W$ and we let $\pi: W \to V$ be the projection onto $V$. Thus $\pi$ is an
\[(A, R)\)-bimodule map with \(\pi|_V = \text{id}_V\) and we define \(w^\lambda = |G|^{-1} \sum_{g \in G} (w\overline{g}) g^{-1}\) for \(w \in W\). Since \(V\) is stable under right multiplication by elements of \(R \circ G\), we certainly have \(W^\lambda \subseteq V\) and, since \((v\overline{g})^\tau = v\overline{g}\) for \(v \in V\), we have \(v^\lambda = |G|^{-1} \sum_{g \in G} (v\overline{g}) g^{-1} = v\). Thus \(\lambda|_V = \text{id}_V\). Furthermore, \(\lambda\) is clearly an \((A, R)\)-bimodule homomorphism. Now let \(h \in G\) and \(w \in W\). Then

\[
(w\overline{h})^\lambda = (|G|^{-1} \sum_{g \in G} (w\overline{h} g) g^{-1}) \overline{h}
\]

and since \(V\overline{g} = \overline{h} c\) for some unit \(c \in R\), we obtain

\[
(w\overline{h})^\lambda = (|G|^{-1} \sum_{g \in G} (w\overline{h} g c) c^{-1} \overline{h}^{-1}) \overline{h}
\]

Thus \(\lambda\) is an \((A, R \circ G)\)-bimodule projection onto \(V\) so \(Y = \ker \lambda\) is the desired complement for \(V\) in \(L(A, W_{R \circ G})\).

We now use the above two lemmas to reprove and slightly extend [17, Lemma 2.4]. The Krull-dimension of a right \(R\)-module \(V\) is a measure of the complexity of the lattice of submodules \(L(V_R)\). Thus for example \(K \dim V_R = 0\) means that \(V\) is nonzero and Artinian. We refer the reader to [9] for the precise definition in general. Two basic properties of Krull-dimension we require are as follows:

a) Let \(R\) and \(A\) be rings, let \(V\) and \(W\) be modules over \(R\) and \(A\) respectively and suppose there exists an inclusion preserving one-to-one map \(L(V_R) \rightarrow L(W_A)\). If \(K \dim W_A\) exists then \(K \dim V_R\) exists and \(K \dim V_R \leq K \dim W_A\). In particular, this always applies in the special case when \(V = W, A \subseteq R\) and where \(L(V_R) \rightarrow L(V_A)\) is given by restriction of operators to \(A\).

b) Let \(V\) be a submodule of the right \(R\)-module \(W\). Then \(K \dim W_R\) exists if and only if both \(K \dim V_R\) and \(K \dim (W/V)_R\) exist and in this case \(K \dim W_R = \sup\{K \dim V_R, K \dim (W/V)_R\}\).
Recall that the socle of $V$, $\text{soc} \ V_R$, is the sum of all simple submodules of $V$ and that the radical of $V$, $\text{rad} \ V_R$, is the intersection of all maximal submodules.

**Theorem 3.3.** Let $R$ be a ring and let $G$ be a finite group acting on $R$ such that $|G|^{-1} \in R$. If $V$ is a right $R$-module, then:

1. $K \dim V_R$ exists if and only if $K \dim V^G_R$ exists and in this case $K \dim V_R = K \dim V^G_R$.
2. $V_R$ is Noetherian if and only if $V^G_R$ is Noetherian.
3. If $V_R$ has finite length $n$, then $V^G_R$ has length $\leq |G| \cdot n$.
4. $\text{soc} \ V_R \subseteq \text{soc} \ V^G_R$ and $\text{rad} \ V_R \supseteq \text{rad} \ V^G_R$.

**Proof.** Set $W = V \otimes_R R$. Then $W_R = \bigoplus_{g \in G} V \otimes g$ is a finite direct sum of modules conjugate to $V$.

(i) By the remarks preceding the statement of this theorem, we know that if $K \dim V^G_R$ exists then so does $K \dim V_R$ and, moreover, $K \dim V_R = K \dim V^G_R$. Conversely, assume that $K \dim V_R$ exists. Since $\mathcal{L}(V^g_R) = \mathcal{L}(V_R)$ for all $g \in G$, we have $K \dim V_R = K \dim V^g_R$, by (a) above, and hence (b) implies that $K \dim W_R = K \dim V_R$. By (a) again, we conclude that $K \dim W^G_R$ exists and in fact $K \dim W^G_R = K \dim W_R = K \dim V_R$. Now Lemma 3.1 (with $A = \mathbb{Z}$) asserts that there exists a one-to-one order preserving map $\sigma : \mathcal{L}(V^G_R) \to \mathcal{L}(W^G_R)$. Again we deduce from this that $K \dim V^G_R$ exists and that $K \dim V^G_R = K \dim W^G_R \leq K \dim V_R$. This completes the proof of (i).

(ii) If $V^G_R$ is Noetherian, then clearly so is $V_R$. Conversely, if $V_R$ is Noetherian, then $W_R$ is Noetherian since each $(V \otimes g)_R = (V^g)_R$ is Noetherian. Thus $W^G_R$ is also Noetherian. Since $\sigma : \mathcal{L}(V^G_R) \to \mathcal{L}(W^G_R)$ is strictly increasing, we conclude that $V^G_R$ is Noetherian.

(iii) If $V_R$ has length $n$, then each $(V^g)_R$ has length $n$ and hence $W_R = \bigoplus_{g \in G} (V^g)_R$ clearly has length $|G| \cdot n$. Therefore, length $W^G_R \leq$ length $W_R = |G| \cdot n$. Since $\sigma : \mathcal{L}(V^G_R) \to \mathcal{L}(W^G_R)$ is strictly increasing, we see that length $V^G_R \leq$ length $W^G_R \leq |G| \cdot n$. 
We first show that if \( V_R \) is completely reducible, then so is \( V_{RG} \). Indeed, if \( V_R \) is completely reducible, then certainly \( W_R = \oplus g \in G(V_R) \) is also completely reducible and, by Lemma 3.2 (with \( A = \mathbb{Z} \)), we conclude that \( W_{RG} \) is completely reducible. Therefore, if \( U \in \mathcal{L}(V_{RG}) \) then \( U^G \in \mathcal{L}(W_{RG}) \) has a complement \( X \in \mathcal{L}(W_{RG}) \) with \( W = U^G \oplus X \).

Applying the map \( \tau \) of Lemma 3.1 now yields

\[
V = W^G = (U^G \oplus X)^G = U^G \oplus X^G = U \oplus X^G.
\]

Thus \( X^G \in \mathcal{L}(V_{RG}) \) is a complement for \( U \) and we have shown that \( V_{RG} \) is completely reducible.

It follows immediately from the foregoing that \( \text{soc} V_R \) is completely reducible as an \( R^G \)-module and hence is contained in \( \text{soc} V_{RG} \). Finally, let \( M \) be a maximal \( R \)-submodule of \( V \). Then \( V/M \) is a simple \( R \)-module and hence is completely reducible as a module over \( R^G \). In particular, \( M = \cap_i L_i \) for certain maximal \( R^G \)-submodules of \( V \). It follows that \( \text{rad} V_{RG} \cap \text{rad} V_{RG} \) and the theorem is proved.

We remark that part (iv) above leads to a simple proof of the equality

\[
J(R^G) = J(R) \cap R^G
\]

([19, Theorem 7]). We now apply the theorem to study \( R \) as a module over \( R^G \). The following result extends [6, Theorem 1] from semisimple Artinian rings to Noetherian rings.

**Corollary 3.4.** Let \( G \) be a finite group acting on a ring \( R \) such that \( |G|^{-1} \in R \). If \( R \) is right Noetherian, then \( R^G \) is right Noetherian and \( R \) is finitely generated as a right module over \( R^G \).

The proof is of course immediate from part (ii) of the theorem by taking \( V = R \). We remark that the result is false if the assumption \( |G|^{-1} \in R \) is weakened to "\( R \) has no \( |G| \)-torsion". Indeed, an example of Chuang and Lee [4] shows that there exists a commutative Noetherian domain \( R \) of characteristic 0 and an automorphism \( \varphi \) of order 2 such that \( R \) is not finitely generated over the fixed subring \( R(\varphi) \).

Part (i) of the next corollary extends [8, Theorem 3.5]. Part (ii)
is a variation on a theme of Farkas and Snider [6]. In the following, we write $K \dim R = K \dim R_R$.

**Corollary 3.5.** Let $G$ be a finite group acting on a ring $R$ with $|G|^{-1} \in R$.

1. If $R$ has Krull-dimension, then $R^G$ has Krull-dimension and in fact $K \dim R^G = K \dim R$.
2. If $R^G$ has Krull-dimension and $R$ is semiprime, then $R$ has Krull-dimension.

**Proof.** (i) Take $V = R$ in Theorem 3.3(i). Then it follows from this and property (b) of Krull-dimension that $K \dim R^G$ exists and

$$K \dim R^G \leq K \dim R = K \dim R_R = K \dim R.$$

On the other hand, by [9, Corollary 4.4], we now have $K \dim R^G \leq K \dim R^G$ so we must have equality throughout.

(ii) Assume that $R$ is semiprime and that $K \dim R^G$ exists. Then $R$ is semiprime Goldie, by [8, Theorem 2.10(ii)], and hence has a classical ring of quotients $\mathcal{Q}(R)$ which is semisimple Artinian. The action of $G$ on $R$ naturally extends to an action on $\mathcal{Q}(R)$ and from Corollary 3.4 it follows that $\mathcal{Q}(R)$ is finitely generated as a module over the fixed ring $\mathcal{Q}(R)^G$.

We now can copy the arguments given in [6, Proof of Theorem 2] and deduce that $R$ as a right $R^G$-module can be embedded in a finite direct sum of copies of $R^G$. Since the latter module has the same Krull-dimension as $R^G$, we conclude that $K \dim R$ exists.

Example 2 of [8] shows that part (ii) of the above corollary is false without the semiprimeness assumption on $R$. The case of rings of Krull-dimension $0$, that is of Artinian rings, is worthy special mention. It follows from part (i) of Corollary 3.5 that if $R$ is Artinian then so is $R^G$. This is an old result due to Levitzki [15]. Conversely, if $R^G$ is Artinian and if $R$ is semiprime, then $R$ is Artinian, by Corollary 3.5(ii), and we obtain a result due to Cohen and Montgomery [3]. In the case of an Artinian ring $R$, with $|G|^{-1} \in R$ or, equivalently, with no $|G|$-torsion, Theorem 3.3(iii) yields a bound on
the number of generators needed to generate \( R \) over \( R^G \). Indeed, if \( R \) has length \( n \), then \( R^G \) has length \( \leq |G| \cdot n \) and hence can be generated by \( \leq |G| \cdot n \) elements. The following example shows that even in the case of a simple Artinian ring this bound cannot be appreciably improved. (Compare with [11, Theorem 6]).

**Example.** Let \( R = M_n(K) \) be the \( n \times n \)-matrix ring over the field \( K \) of characteristic \( \neq 2 \) and let \( \varphi \) be the inner automorphism of \( R \) induced by the diagonal matrix \( \text{diag}(-1, 1, 1, \ldots, 1) \in R \). Then \( \varphi \) has order 2 and the fixed subring \( R(\varphi) \) consists of all matrices in the block diagonal form

\[
\begin{pmatrix}
\ast & 0 \\
0 & \varphi
\end{pmatrix}^{n-1}
\]

In particular, \( R(\varphi) = K \oplus M_{n-1}(K) \) and, as a right module over \( R(\varphi) \), \( R \) can be written as \( R = C_1 \oplus C_{n-1} \), where \( C_1 \) denotes the first column and \( C_{n-1} \) stands for the remaining \( n-1 \) columns. Moreover, the lower \( M_{n-1}(K) \)-block of \( R(\varphi) \) annihilates \( C_1 \). So \( R(\varphi) \) acts on \( C_1 \) as multiplication by field elements. This shows that \( n \) elements are required to generate \( C_1 \) over \( R(\varphi) \) and therefore at least \( n \) elements are required to generate \( R \) as a right module over \( R(\varphi) \). It is easy to check that \( n \) elements do in fact suffice.

Suppose that in addition \( H \) is a finite Galois group of automorphisms of \( K \). Then \( H \) also acts on \( M_n(K) \) and this action commutes with the action of \( \varphi \). Therefore \( G = \langle \varphi \rangle \times H \) acts on \( M_n(K) \), and the fixed subring consists of all matrices of the above described form with entries in the fixed field \( F = K^H \). Since \( \dim_F K = |H| \), we now see that \( |H| \cdot n \) elements are required to generate \( C_1 \) over \( R^G \). Therefore \( |H| \cdot n = |G| \cdot n/2 \) elements are required to generate \( R \) over \( R^G \).

For additional applications of this technique, we now return to Lemmas 3.1 and 3.2 and use the bimodule information to obtain the following two results.

**Lemma 3.6.** Let \( G \) be a finite group acting on the ring \( R \), let \( H \) be a finite group acting on the ring \( S \) and assume that \( |G|^{-1} \in R \),
If $V$ is an $(S, R)$-bimodule, then the induced module $W = SH \otimes_S V \otimes_R RG$ is an $(SH, RG)$-bimodule. Furthermore, there exist inclusion preserving maps

$$\sigma : \mathcal{L}(SHV^G) \to \mathcal{L}(SHWRG)$$

and

$$\tau : \mathcal{L}(SHWRG) \to \mathcal{L}(SHV^G)$$

such that for $U \in \mathcal{L}(SHV^G)$ and $X_1, X_2 \in \mathcal{L}(SHWRG)$ we have $U \circ \tau = U$ and $(X_1 \oplus X_2)^\tau = X_1^\tau \oplus X_2^\tau$.

**Proof.** First set $A = SH$ in Lemma 3.1 and let $M = V \otimes_R RG$. Then by that lemma $M$ is an $(S, RG)$-bimodule and there exist inclusion preserving maps

$$\sigma_1 : \mathcal{L}(SHV^G) \to \mathcal{L}(SHM^{RG})$$

and

$$\tau_1 : \mathcal{L}(SHM^{RG}) \to \mathcal{L}(SHV^G)$$

such that $\sigma_1 \tau_1 = \text{id}$ and $\tau_1$ preserves direct sums. Similarly, since $W = SH \otimes_S M$, we can now apply the left analog of Lemma 3.1 with $A = RG$. We deduce that there exist inclusion preserving maps

$$\sigma_2 : \mathcal{L}(SHM^{RG}) \to \mathcal{L}(SHWRG)$$

and

$$\tau_2 : \mathcal{L}(SHWRG) \to \mathcal{L}(SHM^{RG})$$

such that $\sigma_2 \tau_2 = \text{id}$ and $\tau_2$ preserves direct sums. It is now clear that $\sigma = \sigma_1 \sigma_2$ and $\tau = \tau_2 \tau_1$ have the appropriate properties.

**Lemma 3.7.** Let $R \ast G$ and $S \ast H$ be crossed products with $G$ and $H$ finite and with $|G|^{-1} \in R$, $|H|^{-1} \in S$. Let $W$ be an $(S \ast H, R \ast G)$-bimodule and let $V \in \mathcal{L}(S \ast HWRG)$. If $V$ has a complement in $\mathcal{L}(SW_R)$, then it has a complement in $\mathcal{L}(S \ast HWRG)$.

**Proof.** Let $V$ and $W$ be as above. By Lemma 3.2, with $A = S$,
we deduce that $V$ has a complement in $\mathcal{L}(S^W_{R \rtimes G})$. Now by the left analog of Lemma 3.2, with $A = R \rtimes G$, we conclude that $V$ has a complement in $\mathcal{L}(S^W_{R \rtimes G})$.

It is now an easy matter to obtain

**Theorem 3.8.** Let $G$ be a finite group acting on $R$, let $H$ be a finite group acting on $S$ and assume that $|G|^{-1} \in R$, $|H|^{-1} \in S$. If $V$ is an $(S, R)$-bimodule, then:

1. $K \dim S^V_R$ exists iff $K \dim S^V_{R^G}$ exists and in this case
   \[ K \dim S^V_R = K \dim S^V_{R^G}. \]
2. $S^V_R$ is Noetherian iff $S^V_{R^G}$ is Noetherian.
3. If $S^V_R$ has finite length $n$, then $S^V_{R^G}$ has length $\leq |H| \cdot |G| \cdot n$.
4. $\text{soc } S^V_R \subseteq \text{soc } S^V_{R^G}$ and $\text{rad } S^V_R \supseteq \text{rad } S^V_{R^G}$.

**Proof.** Let $W = SH \otimes_S V \otimes_R R^G$. Then $S^W_R = \bigoplus_{h \in H, g \in G} h \otimes V \otimes g$ is a finite direct sum of $|H| \cdot |G|$ subbimodules each conjugate to $V$. In view of the preceding two lemmas the proof of Theorem 3.3 immediately goes over to yield the result.

Using this we can now translate properties of the lattice of two sided ideals of $R$ to the corresponding lattice for $R^G$ (see [7, Corollary 2.4]).

**Corollary 3.9.** Let $G$ be a finite group acting on $R$ and assume that $|G|^{-1} \in R$.

1. If $R$ satisfies the minimal condition on two sided ideals, then so does $R^G$.
2. If $R$ satisfies the maximal condition on two sided ideals, then so does $R^G$ and $R$ is a finitely generated $(R^G, R^G)$-bimodule.
3. If the chains of two sided ideals of $R$ have length $\leq n$,
   then the chains of two sided ideals of $R^G$ have length $\leq n \cdot |G|^2$. 
Proof. Take $R = S$, $G = H$ and $V = R$ in Theorem 3.8. Since 
$R^G R^G \subseteq R^G V R^G$, parts (i), (ii) and (iii) above follow immediately from the corresponding parts of Theorem 3.8.

In the course of proving (iii) above, one actually shows that the bimodule $R^G R^G$ has length $\leq n \cdot |G|^2$. The following example shows that the bound in this case is reasonably sharp.

Example. Let $K$ be a field containing $m$ distinct $m$-th roots of unity $\epsilon_1, \epsilon_2, \ldots, \epsilon_m$. Let $R = M_m(K)$ and let $\varphi$ be the inner automorphism of $R$ induced by the diagonal matrix $\text{diag}(\epsilon_1, \epsilon_2, \ldots, \epsilon_m)$. If $G = \langle \varphi \rangle$, then $|G| = m$ and $R^G$ consists of the diagonal matrices in $R$. Since $R$ is simple, $R^G R^G$ has length 1 so $n = 1$ in the above. On the other hand,

$$R^G R^G = \oplus_{i,j} \Delta_{ij} K \epsilon_{ij}$$

is a decomposition of the bimodule as a direct sum of $m^2 = |G|^2$ irreducible subbimodules, so the length of $R^G R^G$ is $|G|^2 = n |G|^2$ in this case.

Finally we consider the completely reducible aspect of the two-sided ideal structure. Part (ii) of the following result is originally due to Kharchenko ([14]), while the bound $n \cdot |G|$ given here was first obtained by Osterburg ([22, §2, Theorem 8]). Part (i) has also been observed by J. Fisher.

Corollary 3.10. Let $R$ be a ring which is a direct sum of $n$ simple rings and let $G$ be a finite group. Assume that $R$ has no $|G|$-torsion.

i. If $R \ast G$ is a crossed product, then $R \ast G$ is a direct sum of at most $n \cdot |G|$ simple rings.

ii. If $G$ acts on $R$, then $R^G$ is a direct sum of at most $n \cdot |G|$ simple rings.

Proof. The structure of $R$ implies immediately that $|G|^{-1} \subset R$.

(i) Take $W = R \ast G$, $R = S$ and $G = H$ in Lemma 3.7. Then

$$R^W R^G = \oplus_{g \in G} R^G$$

is a direct sum of $|G|$ subbimodules each conjugate to...
It follows that $R^W_R$ is completely reducible and hence, by Lemma 3.7, so is $R^G W_{R^G}$. Thus $R^G$ is a direct sum of simple subrings and this direct sum is necessarily finite. In fact, since $R^W_R$ is a direct sum of $n \cdot |G|$ simple subbimodules, we see that $R^G$ is a direct sum of at most $n \cdot |G|$ simple rings.

(ii) By (i) above, the skew group ring $RG$ is a direct sum of at most $n \cdot |G|$ simple rings. Since $R^G = e RG e$, it follows that the same is true of $R^G$.

Acknowledgment

The first author's research was supported by Deutsche Forschungsgemeinschaft Grant No. Lo 261/1. The second author's research was partially supported by NSF Grant No. MCS 77-01775 A01.

References

2. S. A. Amitsur, On rings of quotients, Symposia Mathematica, 8 (1972) 149-164.
10. D. Handelman, Algèbres simples de groupes à gauche, original manuscript.
11. D. Handelman and G. Renault, Actions de groupes, original manuscript.


Received: March 1979