5. Crossed Products of Finite Groups

Let $R$ be a ring and let $G$ be a group. To start with, a crossed product $R \rtimes G$ is a generalized group ring. It has as an $R$-basis the set $G$ which is a copy of $G$, so that each element of $R \rtimes G$ is uniquely a finite sum $\sum_{x \in G} r_x x$ with $r_x \in R$. Addition is as expected, but multiplication has two new wrinkles, a twisting and an action. Specifically, for $x, y \in G$, we have

\[ x \cdot y = t(x, y) x y \]

where $t : G \times G \to U = U(R)$, the group of units of $R$. Furthermore, for $x \in G$ and $r \in R$, we have

\[ r x = x r \]

where $x \in \text{Aut } R$. The twisting and action are interrelated by conditions precisely equivalent to $R \rtimes G$ being associative. Note that we can and will assume that $1 = 1$. It follows that $R$ is naturally embedded in the crossed product via $r \mapsto r 1$. On the other hand, $G$ is in general not contained in $R \rtimes G$. Nevertheless, each $x$ is a unit in the ring, $\mathcal{G} = \{u^{-1} x u | u \in U, x \in G\}$ is the group of so-called trivial units of $R \rtimes G$ and $\mathcal{G} / U \simeq G$.

We study crossed products because they occur naturally. We do not merely go around constructing them. For example

**Lemma.** Let $N \triangleleft H$. Then $K[H] = K[N] \rtimes (H/N)$.

**Proof.** Set $R = K[N]$ and $G = H / N$. For each $x \in G$ let $x \in H$ be a fixed inverse image. Then $H = \bigcup_x N x$ implies that

\[ K[H] = \bigoplus_x K[N] x = \bigoplus x R x \]

so $G$ is an $R$-basis for $K[H]$.

Since $N \triangleleft H$, $x^{-1} N x = N$ so $x^{-1} K[N] x = K[N]$ and $x$ induces a conjugation automorphism on $R$. In particular, if $x \in G$ and $r \in R$, then

\[ r x = x^{-1} x r = x r x \]

and we see that an action occurs. Note that the action is trivial if $N$ is central in $H$. 

29
Next, for \( x, y \in G \) we have \( N\bar{x} \cdot N\bar{y} = N\bar{xy} \) so \( \bar{x} \bar{y} = t(x, y)\bar{xy} \) for some \( t(x, y) \in N \subseteq U(R) \). Furthermore, this twisting is trivial if we can choose a consistent set of coset representatives, that is, if \( H = N \rtimes G \). Finally we observe that \( K[H] \) is certainly associative.

Several remarks are in order. (1) Finite index problems occur frequently in the study of group rings. Namely, suppose we know information about \( K[N] \) with \( N \) a normal subgroup of \( H \) of finite index. The goal is to lift this information to \( K[H] \). Since \( K[H] = K[N] \rtimes (H/N) \), the structure of crossed products of finite groups can sometimes help. We will offer a nice example of this. (2) Suppose \( I \triangleleft K[H] \) is controlled by \( N \) so that \( I = L \cdot K[H] \) with \( L = I \cap K[N] \). It then follows easily that \( K[H]/I = (K[N]/L) \rtimes (H/N) \). (3) Finally, the same argument shows that if we are given \( R \rtimes H \) and \( N \triangleleft H \), then \( R \rtimes H \supseteq R \rtimes N \) and \( R \rtimes H = (R \rtimes N) \rtimes (H/N) \). Thus we do not leave the family of crossed products.

Certain special cases of crossed products have their own names. If there is no action or twisting, then \( R \rtimes G = R[G] \) is an ordinary group ring. If the action is trivial, then \( R \rtimes G = R^t[G] \) is a twisted group ring. Finally, if the twisting is trivial, then \( R \rtimes G = RG \) is a skew group ring. We frequently construct the latter.

**Lemma 2.** Let \( G \to \text{Aut} R \) be a group homomorphism and define \( RG \) as above. Then this skew group ring is associative.

Note that since the twisting is trivial in \( RG \) we have \( \bar{x} \bar{y} = \bar{xy} \). Thus we can drop the overbars here and assume that \( RG \supseteq G \). The skew group ring is a useful tool in the Galois theory of rings. We will discuss this later on.

Historically, crossed products arose in the study of division rings. Let \( K \) be a field and let \( D \) be a division algebra finite-dimensional over its center \( K \). If \( F \) is a maximal subfield of \( D \), then \( \dim_K D = (\dim_K F)^2 \). Suppose that \( F/K \) is normal, although this is not always true. If \( x \in \text{Gal}(F/K) = G \), then the Skolem-Noether theorem implies that there exists \( \bar{x} \in D \setminus 0 \) with \( \bar{x}^{-1}fx = f\bar{x} \) for all \( f \in F \). Furthermore, \( \bar{x} \bar{y} \) and \( \bar{xy} \) agree in their action on \( F \) so \( \bar{x} \bar{y} \bar{x}^{-1} \bar{y}^{-1} \in C_D(F) = F \). Once we show that the elements \( \bar{x} \) for \( x \in G \) are linearly independent over \( F \), then we conclude by computing dimensions that \( D = \oplus \sum_{x \in G} F\bar{x} = F \rtimes G \).

More generally we say that \( A \) is central simple over \( K \), if \( A \) is a finite-dimensional simple algebra over its center \( K \). Thus \( A = M_n(D) \) for some \( n \) and division ring \( D \) with \( \mathcal{Z}(D) = K \). Two such algebras \( A \) and \( B \) are equivalent if they have the same \( D \). The equivalence classes then form a group under tensor product \( \otimes_K \), the Brauer group. Now given \( A \), one can show that there exists \( B \sim A \) with \( B = F \rtimes G \). But \( F \rtimes G \) is determined by the twisting function \( t: G \times G \to F \), a 2-cocycle. Thus, in this way we obtain the homological characterization of the Brauer group as the 2nd cohomology group.

We now begin to consider the ring theoretic properties of \( R \rtimes G \) with \( G \) finite. We start with the essential version of Maschke's theorem (see [7]).
THEOREM 3. Given \( R \ast G \) with \( G \) finite. Let \( W \subseteq V \) be \( R \ast G \)-modules with no \( |G| \)-torsion. Then \( W \text{ess}_R V \) if and only if \( W \text{ess}_{R \ast G} V \).

PROOF. We need only show that \( W \text{ess}_{R \ast G} V \) implies that \( W \text{ess}_R V \) since the other implication is obvious.

Case 1. Suppose \( V = W \oplus U \) where \( U \) is a complementary \( R \)-submodule. Then for all \( x \in G, V = Wx \oplus Ux = W \oplus Ux \) and we let \( \pi_x: V \to W \) be the \( R \)-homomorphism determined by this decomposition. Note that if \( v = w + ux \), then \( v\overline{y} = w\overline{y} + ux\overline{y} \), so clearly

\[
\pi_{xy}(v\overline{y}) = w\overline{y} = \pi_x(v)\overline{y}.
\]

It follows that \( \pi = \sum_x \pi_x \) is an \( R \ast G \)-homomorphism from \( V \) to \( W \) since

\[
\pi(v\overline{y}) = \sum_x \pi_x(v\overline{y}) = \sum \pi_{xy}(v\overline{y}) = \sum_x \pi_x(v)\overline{y} = \pi(v)\overline{y}.
\]

Furthermore, we have \( \pi(w) = |G|w \) so \( \ker \pi \cap W = 0 \) since \( V \) has no \( |G| \)-torsion, and hence, \( \ker \pi = 0 \) since \( W \text{ess}_{R \ast G} V \). Finally, let \( u \in U \) and set \( w = \pi(u) \).

Then \( |G|u - w \in \ker \pi \) so \( |G|u \in W \cap U = 0 \) and \( u = 0 \).

Case 2. Now for the general case. Choose \( U_R \subseteq V \) maximal with \( U_R \cap W = 0 \). Then \( W \oplus U \text{ess}_R V \) and set \( E = \bigcap_x (W \oplus U)x \). It follows that \( E \text{ess}_R V \) and that \( E \) is an \( R \ast G \)-submodule. Furthermore, \( W \subseteq E \subseteq W \oplus U \) so \( E = W \oplus (U \cap E) \). By Case 1, \( W = E \) so \( W \text{ess}_R V \).

THEOREM 4 [2]. Let \( R \) be a semiprime ring with no \( |G| \)-torsion. Then \( R \ast G \) is semiprime.

PROOF. Let \( N \triangleleft R \ast G \) with \( N^2 = 0 \). If \( L = l_{R \ast G}(N) \), then \( L \triangleleft R \ast G \) and \( L \text{ess}_{R \ast G} R \ast G \) as right ideals. Maschke’s theorem now implies that \( L \text{ess}_R R \ast G \) so \( (L \cap R) \text{ess}_R R \). Since \( R \) is semiprime, we conclude that \( L \cap R = 0 \) and then \( N \subseteq l_{R \ast G}(L \cap R) = 0 \), by the freeness of \( R \ast G \) over \( R \).

The proof given above is from [7] but the original techniques are still needed for the following generalization.

THEOREM 5 [8]. Given \( R \ast G \) with \( G \) finite.

(i) If \( R \ast G \) is semiprime and \( H \subseteq G \), then \( R \ast H \) is semiprime.

(ii) Assume that \( R \ast P \) is semiprime for \( P = 1 \) and all elementary abelian \( p \)-subgroups \( P \subseteq G \) such that \( R \) has \( p \)-torsion. Then \( R \ast G \) is semiprime.

Now let us study the prime ideals in \( R \ast G \) with \( G \) finite. Note that \( G \) permutes the ideals of \( R \) by conjugation. If \( A \triangleleft R \ast G \), then \( A \cap R \) is a \( G \)-invariant ideal of \( R \). Conversely, if \( I \) is a \( G \)-invariant ideal of \( R \), then \( I \ast G = I(R \ast G) \) is an ideal of \( R \) with \( (I \ast G) \cap R = I \). Moreover, \( (R \ast G)/(I \ast G) = (R/I) \ast G \).

To study the prime ideals \( P \) of \( R \ast G \) we might as well mod out by \( (P \cap R) \ast G \) and assume that \( P \cap R = 0 \). This forces \( R \) to be \( G \)-prime, a condition somewhat
weaker than being prime. Indeed for $G$ finite it means that there exists a prime ideal $Q$ of $R$ with $\bigcap_{x \in G} Q^x = 0$. Note that $\{Q^x| x \in G\}$ is the set of minimal primes of $R$ and hence is uniquely determined by $R$. There are two cases to consider according to whether $R$ is prime or not. We start with the latter situation.

Let $H$ be a subgroup of $G$ and let $I \triangleleft R \ast H$. Then $I(R \ast G)$ is a right ideal of $R \ast G$ and we denote by $I^G$ the unique largest two-sided ideal it contains. In other words, the induced ideal $I^G$ is given by

$$I^G = \text{Id}(I(R \ast G)) = \bigcap_{x \in G} (I(R \ast G))^x.$$

If $J$ is a second ideal of $R \ast H$, then $I^G J^G \triangleleft R \ast G$ and

$$I^G J^G \subseteq I(R \ast G) J^G \subseteq IJ^G \subseteq IJ(R \ast G).$$

Thus, induction satisfies the submultiplicative formula $I^G J^G \subseteq (IJ)^G$. Note that $H \triangleleft G$ implies that

$$I^G = \left( \bigcap_{x \in G} I^x \right) (R \ast G)$$

and $H$ controls $I^G$. The first main result on primes is

**Theorem 6 [5].** Given $R \ast G$ with $G$ finite and suppose $Q$ is a prime ideal of $R$ with $\bigcap_{x \in G} Q^x = 0$. Let $H$ be the stabilizer of $Q$ in $G$. Then the map $T \mapsto T^G$ yields a one-to-one correspondence between the primes $T$ of $R \ast H$ with $T \cap R = Q$ and the prime ideals $P$ of $R \ast G$ with $P \cap R = 0$.

Note that there is an obvious one-to-one correspondence between the primes $T$ of $R \ast H$ with $T \cap R = Q$ and the prime ideals $\bar{T}$ of $(R \ast H)/(Q \ast H) = (R/Q) \ast H$ with $\bar{T} \cap (R/Q) = 0$. This, therefore, reduces considerations to the prime case.

Now suppose that $R$ is prime and consider all $R$-module homomorphisms $f: RA \to R \ast R$ where $A$ runs over all nonzero two-sided ideals of $R$. We say that $f \sim g$ if and only if $f$ and $g$ agree on their common domain and we let $\hat{f}$ denote the equivalence class of $f$. Then $Q_l(R)$, the set of all such equivalence classes, becomes a ring under function addition and composition. Furthermore, $R$ embeds in $Q_l(R)$ via $r \mapsto$ right multiplication by $r$. $Q_l(R)$ is called the (left) Martindale ring of quotients of $R$.

We will discuss $S = Q_l$ in more detail later on. For now it suffices to know that $C = Z(S)$ is a field called the extended centroid of $R$. Also, any automorphism $\sigma$ of $R$ extends uniquely to one of $S$. We say that $\sigma$ is $X$-inner if it becomes inner on $S$.

Given $R \ast G$, there exists a unique extension to a crossed product $S \ast G$. We let $G_{\text{inn}} = \{x \in G| x^x \text{ is } X\text{-inner on } R\}$. Then $G_{\text{inn}} \triangleleft G$ and the second main result on primes is

**Theorem 7 [5].** Let $R \ast G$ be a crossed product with $G$ finite and $R$ prime. Set $S = Q_l(R)$ and let $E = C_{S \ast G}(S)$.
(i) $E = C^t[G_{\text{inn}}]$ is a twisted group algebra of $G_{\text{inn}}$ over the field $C$, the extended centroid of $R$.

(ii) Conjugation by each $\overline{z} \in R \ast G \subseteq S \ast G$ yields an action of $G$ on $E$.

(iii) There exists a one-to-one correspondence between the prime ideals $P$ of $R \ast G$ with $P \cap R = 0$ and the $G$-orbits of primes of $E$.

To be precise, the $G$-orbit $\{T^\overline{z}\}$ of primes of $E$ corresponds to

$$P = \left( \bigcap_{z \in G} T^\overline{z} \right) \cdot (S \ast G) \cap (R \ast G).$$

By combining the above two results we see that for $R$ a $G$-prime ring, the primes $P$ of $R \ast G$ with $P \cap R = 0$ correspond to the $H$-orbits of primes of $E = C^t[H_{\text{inn}}]$ where $C$ is the extended centroid of $R/Q$. Since $E$ is a finite-dimensional $C$-algebra, this implies that there are only finitely many primes $P$ and indeed we have

**Corollary 8.** Given $R \ast G$ with $G$ finite and $R$ a $G$-prime ring.

(i) If $P$ is a prime ideal of $R \ast G$, then $P$ is a minimal prime if and only if $P \cap R = 0$.

(ii) There exist only finitely many minimal primes $P_1, P_2, \ldots, P_n$ and $n \leq |G|$.

(iii) If $J = P_1 \cap P_2 \cap \cdots \cap P_n$, then $J$ is the unique largest nilpotent ideal of $R \ast G$ and $J^{[G]} = 0$.

This result is now a special case of properties of finite normalizing extensions. But more information is available here. For example, in the notation of Theorem 6, the number of primes $P$ with $P \cap R = 0$ is at most equal to the number of conjugacy classes of $H$ (not of $G$). Furthermore, if $\text{char} C = p > 0$, then only the $p$-regular classes matter. In particular, if $H_{\text{inn}}$ is a $p$-group, then there exists a unique prime $P$ with $P \cap R = 0$.

We can also use these results to describe when $R \ast G$ is prime. It reduces to the twisted group algebra case which is still unsolved.

The above material was developed to study prime ideals in group rings of polycyclic-by-finite groups. For example, if $G$ is such a group, then $G$ has a normal subgroup $G_0$ of finite index which is orbitally sound, and hence, we essentially know the primes of $K[G_0]$. Furthermore, $K[G] = K[G_0] \ast (G/G_0)$ so the preceding results can apply. Indeed, Theorem 6 translates almost directly as follows. Let $P$ be a prime ideal of $K[G]$ and let $Q$ be a prime of $K[G_0]$ minimal over $P \cap K[G_0]$. If $H$ is the stabilizer of $Q$ in $G$, then $G \supseteq H \supseteq G_0$ and there exists a prime $T$ of $R \ast (H/G_0) = K[H]$ with

$$P = T^G = \bigcap_{z \in G} (T \cdot K[G])^z.$$

It remains to consider $T$ and, in an attempt to apply Theorem 7 directly, Lorenz and I computed $X$-inner automorphisms using $\Delta$-methods. It turned out that yet another variant of the $\Delta$-method was the missing ingredient, namely
Proposition 9 [4]. Let $G$ be a polycyclic-by-finite group and let $I$ be an ideal of $K[G]$ with $I = (I \cap K[\Delta]) \cdot K[G]$ and $I \cap K[\Delta] = Q_1 \cap Q_2 \cap \cdots \cap Q_n$, an intersection of almost faithful primes. If $A, B \leq K[G]$ with $AB \subseteq I$, then $\theta(A)\theta(B) \subseteq \theta(I) = I \cap K[\Delta]$. In particular, $I$ is a semiprime ideal and if all $Q_i$ are $G$-conjugate, then $I$ is a (standard) prime.

This was sufficient to show that $T$ above is image standard. Thus, to start with, if $P$ is a prime ideal of $K[G]$, then $P = T^G$ for $T$ an image standard prime of $K[H]$ with $|G : H| < \infty$. This sounds like a complete solution but it does leave a number of questions unanswered. Most notably we ask what are the possibilities for $H$ and how unique is the situation. For this we need some additional definitions.

Let $N$ be a subgroup of $G$. Then $N$ is orbital if and only if it has a finite number of $G$-conjugates, that is, $|G : \mathcal{N}_G(N)| < \infty$. $N$ is said to be an isolated orbital if it is orbital and for any larger orbital $N_1 > N$ we have $|N_1 : N| = \infty$. Finally, $G$ is orbitally sound if all isolated orbitals are normal. Note that any finite orbital subgroup of $G$ is contained in $\Delta^+(G)$ and that $\Delta^+$ is an isolated orbital. The answer to the first question is that $H$ can be taken to be the normalizer of an isolated orbital subgroup. Thus if $G$ is orbitally sound, then $H = G$. Next, if $H = \mathcal{N}_G(N)$, then what is $N$? Again we need some more definitions.

If $I < K[G]$, then we let $I^\dagger = \{x \in G | x - 1 \in I\}$. Then $I^\dagger$ is the kernel of the homomorphism $G \to K[G]/I$ and $I^\dagger < G$. We can now state that $H = \mathcal{N}_G(T^\dagger)$ and, more properly, $H$ is the normalizer of the unique isolated orbital subgroup of finite index above $T^\dagger$.

Note that any standard prime is induced from a prime ideal of $K[\Delta]$. This leads to our last definition. Let $N \subseteq G$ and set $H = \mathcal{N}_G(N)$. Then we let $\mathcal{N}_G(N)$ be the subgroup of $G$ with $H \supseteq \mathcal{N}_G(N) \supseteq N$ and $\mathcal{N}_G(N)/N = \Delta(H/N)$. We can now state the following three results of [6]. The first of course is based on the work of [9].

Theorem 10 (Existence) [6, 9]. Let $G$ be polycyclic-by-finite and let $P$ be a prime ideal of $K[G]$. Then there exists an isolated orbital subgroup $N$ of $G$ and a prime $L$ of $K[\mathcal{N}_G(N)]$ with $|N : L^\dagger| < \infty$ and $P = L^G$.

Note that $\mathcal{N}_G(N)/N$ is torsion-free abelian so $\mathcal{N}_G(N)/L^\dagger$ is finite-by-abelian (and center-by-finite). Thus $L$ is essentially a prime of a commutative group algebra. We call $N$ above a vertex of $P$ and $L$ a source.

Theorem 11 (Uniqueness) [6]. Let $G$ be polycyclic-by-finite and let $P$ be a prime of $K[G]$. Then the vertices of $P$ are unique up to conjugation in $G$. Furthermore, if $N$ is a vertex, then the sources for this $N$ are unique up to conjugation by $\mathcal{N}_G(N)$.

Theorem 12 (Converse) [6]. Let $N$ be an isolated orbital subgroup of the polycyclic-by-finite group $G$. If $L$ is a prime ideal of $K[\mathcal{N}_G(N)]$ with $|N : L^\dagger| < \infty$, then $L^G$ is prime.
It is a consequence of the last result that every isolated orbital subgroup is a vertex. Thus if all primes are image standard, then all isolated orbitals are normal and $G$ is orbitally sound. The above has been extended to

**COROLLARY 13 [1].** Let $N$ be an isolated orbital subgroup of the polycyclic-by-finite group $G$. If $L$ is a prime ideal of $K[N]$ having only finitely many conjugates under $N_G(N)$, then $L^G$ is prime.

In closing we briefly mention the beautiful results on finite normalizing extensions. These deserve a much more detailed discussion than we can offer here. Let $S \supseteq R$ be rings with the same 1. Then $S$ is a finite normalizing extension of $R$ if there exist $s_1, s_2, \ldots, s_n \in S$ with $S = \sum_1^n Rs_i$ and $s_i R = Rs_i$ for all $i$. For example, we could have $S = R * G$ with $G$ a finite group or $S$ could be a finite centralizing extension where each $s_i$ centralizes $R$. The following result was contributed to by a number of people. But by far the most difficult part is the incomparability due to Heinicke and Robson. So we credit all of it to their paper.

**THEOREM 14 [3].** Let $S = \sum_1^n Rs_i$ be a finite normalizing extension of $R$.

(i) (Cutting Down) If $P$ is a prime ideal of $S$, then $P \cap R = Q_1 \cap Q_2 \cap \cdots \cap Q_t$ is an intersection of $t \leq n$ minimal covering primes of $R$. Furthermore, all $R/Q_i$ are isomorphic.

(ii) (Lying Over) Let $Q$ be a prime ideal of $R$. Then there exist primes $P_1, P_2, \ldots, P_s$ of $S$ with $1 \leq s \leq n$ such that $Q$ is minimal over each $P_i \cap R$.

(iii) (Incomparability) Let $P$ be a prime ideal of $S$ and let $I \triangleleft S$ with $I \supset P$. Then $I \cap R > P \cap R$.

A continuation of [3] considers nilpotent ideals of $S$. Furthermore, the authors study intermediate extensions, that is, rings $T$ contained between $R$ and $S$. They obtain a strong relationship between the primes of $R$ and those of $T$. However, they are less successful relating those of $S$ and $T$. We remark that not every finite extension of interest is an intermediate extension. For example, let $R$ be a local commutative algebra of characteristic $p > 0$ with $J = JR \neq 0$ and suppose $\delta$ is a derivation of $R$ with $\delta^p = 0$ and $\delta J \not\subseteq J$. Then $R[x; \delta|x^p = 0]$ is not an intermediate extension of $R$.

**References**


