8. Galois Theory and Crossed Products

Let $G$ act on the ring $R$ so that we have a group homomorphism $G \to \text{Aut } R$. Then we can form the skew group ring $RG$ which is associative and contains $R, G$ and the fixed ring $R^G$. In other words, $RG$ contains all the ingredients for the study of the Galois theory of rings. Thus we might hope to use crossed product results to obtain Galois theoretic information. Indeed there exist such applications, but perhaps not an overwhelming amount for the following reasons.

First, it seems necessary for us to assume $G$ is finite. The reason is that only certain classes of infinite groups are allowed (discussed in the next section) and their description does not readily translate into crossed product terms. Second, the structure of $RG$ is best understood when $R$ has no $|G|$-torsion. Thus the route through crossed products usually requires that assumption. Third, certain natural Galois theory questions may not translate to natural questions about $RG$ and vice versa.

In this section we will discuss skew group ring applications and we will always assume $G$ to be finite here. We start with the existence of fixed points. Let $G$ act on $R$ and let $I$ be a nonzero $G$-invariant ideal of $R$. The question is whether $I^G = I \cap R^G$ must necessarily be nonzero. The answer is yes and no. For no we have the following example of Bergman.

Let $S = K\langle x, y \rangle$ be the free algebra on $x, y$ over the field $K$ of characteristic $p > 2$ and let $R = M_2(S)$ be the ring of $2 \times 2$ matrices over $S$. Now let $G$ be the group of units of $R$ generated by the matrices

\[
\begin{bmatrix}
-1 & 0 \\
0 & 1
\end{bmatrix}, \quad \begin{bmatrix}
1 & x \\
0 & 1
\end{bmatrix}, \quad \begin{bmatrix}
1 & y \\
0 & 1
\end{bmatrix}.
\]

Then $|G| = 2p^2$, $G$ acts on $R$ by conjugation, and hence $R^G = C_R(G)$. To compute the latter, first note that the centralizer of $\begin{bmatrix}
-1 & 0 \\
0 & 1
\end{bmatrix}$ is precisely the set of diagonal matrices, since char $K \neq 2$. It then follows easily that $R^G = K$. But there is a natural homomorphism $S \to K$ obtained by mapping $x, y \to 0$ and this extends to a map $R \to M_2(K)$ with kernel $I \neq 0$. Since $I \triangleleft R$, $I$ is $G$-invariant, but $I \cap R^G = I \cap K = 0$.

We note three properties of this example. (1) $R$ is a prime ring but not a domain (and hence has nontrivial nilpotent elements). (2) $G$ is inner on $R$. (3) $R$ has $|G|$-torsion.
As we will see, each of these three properties is in some sense a necessary ingredient of the example. We start with a fairly easy result. In the skew group ring $R\hat{G}$, set $\hat{G} = \sum_{x \in G} x$. Then $y\hat{G} = \hat{G}y = \hat{G}$ for $y \in G$ so $(\hat{G})^2 = |G|\hat{G}$. Also, if $r \in R$ we have
\[
\hat{G}r\hat{G} = \hat{G} \sum_{x \in G} rx = \hat{G} \sum_{x \in G} xr = \hat{G} \sum_{x \in G} r^x.
\]
Thus if we define
\[
\tilde{t}_{\hat{G}}(r) = \sum_{x \in G} r^x,
\]
then $\tilde{t}_{\hat{G}}: R \to R^G$ is an $R^G$-bimodule homomorphism and
\[
\hat{G}r\hat{G} = \hat{G}\tilde{t}_{\hat{G}}(r) = \tilde{t}_{\hat{G}}(r)\hat{G}.
\]

**Proposition 1.** Let $G$ act on the ring $R$. Then any of the following implies the existence of fixed points in nonzero $G$-invariant one-sided ideals of $R$.

(i) $RG$ is semiprime.

(ii) $R$ is semiprime with no $|G|$-torsion.

(iii) $R$ is prime and $G$ is $X$-outer.

(iv) $R$ has characteristic $p > 0$ and $|G| = p$.

**Proof.** (i) Let $I$ be a nonzero $G$-invariant left ideal of $R$. Then $I\hat{G}$ is a left ideal of $RG$. Since $RG$ is semiprime, this implies that $I\hat{G}\hat{G} \neq 0$ so $I\tilde{t}_{\hat{G}}(I)\hat{G} \neq 0$. Thus $0 \neq \tilde{t}_{\hat{G}}(I) \subseteq I^G$.

(ii) and (iii) certainly imply (i).

(iv) Say $G = \langle g \rangle$ with $g^p = 1$ and let $I$ be as above. Then $g$ acts as a linear transformation on $I$ and char $R = p$ so $(g - 1)^p = 0$. Now note that the nilpotent transformation $g - 1$ has a nonzero kernel.

We remark that (iv) is in fact true for any finite $p$-group $G$. This covers properties (2) and (3) of the example, but what about (1)?

**Theorem 2 [2].** Let $G$ act on the domain $R$.

(i) If $G$ is $X$-inner and faithful, then $R$ has no $|G'|$-torsion.

(ii) If $I$ is a nonzero $G$-invariant one-sided ideal of $R$, then $I^G \neq 0$.

**Proof.** (i) Say char $R = p > 0$ and let
\[
H = \{q|q \text{ is a unit of } Q_s(R) \text{ which acts like some } g \in G \text{ on } R\}.
\]
Then $H$ is a multiplicative group which contains $C^*$, the set of nonzero elements of the extended centroid $C$ of $R$. Since $G$ is both $X$-inner and faithful we have $H/C^* \simeq G$. Therefore $H$ is center-by-finite and this implies that the commutator subgroup $H'$ of $H$ is finite. Now let $q \in H'$ and suppose $q^p = 1$. Then $(q - 1)^p = 0$ so $q = 1$ since $Q_s(R)$ is a domain. It follows that $p|H'|$ and hence $p|G'$ since $H'$ maps onto $G'$.

(ii) Since a subring of a domain is a domain, this easily reduces to the situation where $G$ is simple and acts faithfully on $R$. Since $G_{\text{inn}} \trianglelefteq G$, there are three cases
to consider:

a. $G$ is $X$-outer.

b. $G$ is $X$-inner and abelian.

c. $G$ is $X$-inner and nonabelian.

Case (a) is already done and for (b) we must have $|G| = p$ for some prime $p$. Here the result follows if either char $R = p$ or not. Finally, for (c) we have $G = G'$ so (i) implies that $R$ has no $|G|$-torsion and again fixed points exist.

Kharchenko in fact proved the stronger result: If $R$ has no nilpotent elements, then fixed points exist. Thus we are able to finesse $|G|$-torsion in this case. Now what can we get with the additional assumption that $R$ has no $|G|$-torsion? We actually get the premier result on this question. First note that the augmentation map $\rho: RG \to R$ is given by $\rho(\sum g r g) = \sum g r g$. For $\alpha \in RG, x \in G$ and $r \in R$ we have $\rho(\alpha x) = \rho(\alpha), \rho(x^{-1} \alpha) = \rho(\alpha)^x$ and $\rho(r \alpha) = r \rho(\alpha)$.

**Theorem 3 [1].** Let $G$ act on $R$ and let $I$ be a $G$-invariant one-sided ideal of $R$ with no $|G|$-torsion. Then either $I^G \neq 0$ or $I$ is nilpotent of bounded degree (depending on $|G|$).

**Proof (Sketch).** Assume the $I$ is a left ideal, form $RG$ and let

$$IG = \left\{ \sum g r g \in RG | r_g \in I \text{ for all } g \in G \right\}.$$

Then $IG$ is a left ideal of $RG$ and we set

$$A = \{ \alpha \in IG | \rho(\alpha I G) = \rho(\alpha I) = 0 \}.$$ 

We have $(RG) A \subseteq A$, $A(IG) \subseteq A$ and $A \subseteq IG$ so $\rho(A^2) = 0$. The goal is to show that $\rho(A)$ is nilpotent of bounded degree.

Define $A_i$ to be the linear span of all elements of $A$ of support size at most $i$. Then $A_0 = 0$ so $\rho(A_0) = 0$. Thus it suffices to show that $\rho(A_i)^{k_i} \subseteq \rho(A_{i-1})$ for all $i$ and suitable integers $k_i$. For example, suppose $\alpha, \beta \in A$ both have the same support $X$ with $|X| = i \geq 1$ and write $\alpha = \sum_{x \in X} a_x x$, $\beta = \sum_{x \in X} b_x x$. For each $x \in X$ form $\gamma_x = a_x \beta - a \beta x$. Then $\gamma_x \in A$ and $\text{Supp } \gamma_x \subseteq X - \{x\}$ so $\gamma_x \in A_{i-1}$. Since $\alpha \in A$ and $b_x \in I$ we have $\rho(\gamma_x) = a_x \rho(\beta)$ so $a_x \rho(\beta) \in \rho(A_{i-1})$. Adding over all $x \in X$ then yields $\rho(\alpha) \rho(\beta) \in \rho(A_{i-1})$. It now follows from a pigeon hole argument that $\rho(A_i)^{k_i} \subseteq \rho(A_{i-1})$ with $k_i = \binom{|G|}{i} + 1$. Thus we have proved that $\rho(A)^n = 0$ with $n = k_1 k_2 \cdots k_{|G|}$.

Finally, suppose that $I^G = 0$ so that $\tilde{\text{tr}}_G(I) = 0$. We claim that $I \tilde{G} \subseteq A$. Indeed, if $a, b \in I$, then $a \tilde{G} b = \sum_x a b x^{-1}$ so $\rho(a \tilde{G} b) = a \tilde{\text{tr}}_G(b) = 0$. Using $\rho(A)^n = 0$ and $\rho(I \tilde{G}) = I \cdot |G|$ we conclude that $I^n \cdot |G|^n = 0$ and hence that $I^n = 0$ since $I$ has no $|G|$-torsion.

It is an open problem to obtain the sharp bound for the degree of nilpotence of $I$ in the above. It is conjectured that this bound should be $|G|$. We remark that less computational proofs of Theorem 3 can be given following the argument of
Proposition 1 or via the completely different approach of [6]. In either case, one proves that \( f \) is nilpotent but obtains no bound at all for the nilpotence degree. We briefly discuss the proof in [6]. To start with it requires

**Lemma 4.** Let \( I \triangleleft R \) and let \( L_1 \) and \( L_2 \) be right ideals of \( R \) with \( I + L_1 = I + L_2 = L_1 + L_2 = R \). Then \( I + (L_1 \cap L_2) = R \).

**Proof.** First \( I = RI = (L_1 + L_2)I \) so \( I = (I \cap L_1) + (I \cap L_2) \). Next, since \( I + L_1 = R \) we see that \( L_1 + (I \cap L_2) = R \) and hence \( L_2 = (L_1 \cap L_2) + (I \cap L_2) \). Finally, using \( I + L_2 = R \) and the above we obtain \( I + (L_1 \cap L_2) = R \).

**Lemma 5.** Let \( G \) act on \( R \) and let \( I \) be a \( G \)-invariant ideal of \( R \) with \( I^G = 0 \). Then \( |G| \cdot I \subseteq JR \).

**Proof.** Let \( M \) be a maximal right ideal of \( R \). We show that either \( I \subseteq M \) or \( |G| \in M \). To this end, suppose that \( I \notin M \). Then \( I + M = R \) and hence, for all \( g \in G \), \( I + M^g = R \). The previous lemma now shows that \( I + \overline{M} = R \) where \( \overline{M} \) is the \( G \)-invariant right ideal \( \overline{M} = \bigcap_{g} M^g \). Thus there exists \( i \in I \) with \( 1 - i \in \overline{M} \). Furthermore for all \( g \in G \), \( 1 - i^g \in \overline{M} \), so summing over \( g \) yields \( |G| \cdot \overline{tr}(i) \in \overline{M} \). But \( \overline{tr}(i) = 0 \) so \( |G| \in \overline{M} \subseteq M \). We conclude that \( |G| \cdot I \) is contained in all such \( M \).

Here is a sketch of the remainder of the argument. Form a suitable polynomial power series ring over \( R \). Then \( G \) acts on \( R[[X]] \) and \( I[[X]] \) is a \( G \)-invariant ideal. Furthermore, if \( I^G = 0 \), then \( I[[X]]^G = 0 \) and \( |G| \cdot I[[X]] \subseteq J(R[[X]]) \). But \( J(R[[X]]) \) is nilpotent, if this extension is chosen properly, so \( |G| \cdot I \) is nilpotent and hence so is \( I \).

A natural generalization of the existence of fixed points is integrality. Namely, we ask whether \( I \) is integral in some reasonable sense over \( I^G \). We will discuss this question in the final section. Now we move on to other skew group ring applications. For these we need \( |G|^{-1} \in R \). With this assumption we can set \( e = |G|^{-1} \hat{G} \in RG \). It follows easily that \( e \) is an idempotent and that

\[
 eRGe = eR^G = R^G e \simeq R^G.
\]

This then yields an alternate route from \( R \) to its subring \( R^G \). Namely, we can go from \( R \) to \( RG \) and then from \( RG \) to \( eRGe \simeq R^G \). Since both of these steps are fairly well understood, we are able to obtain nice results in this roundabout fashion. We will discuss two of these applications below.

The first one concerns the restriction of \( R \)-modules to \( R^G \). If \( V_R \) is a right \( R \)-module, let \( \mathcal{L}(V_R) \) denote the lattice of its \( R \)-submodules. Given \( V \) we can also form the induced \( RG \)-module \( W = V \otimes_R RG \) and then \( We \) is a module for \( eRGe \simeq R^G \).

**Theorem 6 [3].** Let \( G \) act on the ring \( R \) with \( |G|^{-1} \in R \) and let \( V_R \) be a right \( R \)-module. If \( W = V \otimes_R RG \) is the induced \( RG \)-module, then there exist order preserving maps

\[
 \sigma: \mathcal{L}(V_R^G) \rightarrow \mathcal{L}(W_{RG}), \quad \tau: \mathcal{L}(W_{RG}) \rightarrow \mathcal{L}(V_R^G)
\]
such that
   (i) $\sigma \tau = 1$ so $\sigma$ is one-to-one and $\tau$ is onto, and
   (ii) $\tau$ preserves direct sums.

Proof. Set $S = RG$ and define $\sigma : \mathcal{L}(\text{We}eS_e) \to \mathcal{L}(WS)$ and $\tau$ in the other
direction by $A' = AS$ and $B' = Be$. It is a standard, easy result that (i) and
(ii) are satisfied. Thus it suffices to show that $\text{We}eS_e \simeq V_{RG}$. But this is clear
since $W = \sum_{x \in G} V \otimes x$ implies that the map $v \to \sum_{x} v \otimes x$ gives the necessary
$R^G$-isomorphism.

We can now apply known results on induced modules, including Maschke’s
theorem, to obtain numerous consequences. We list a sample of these. Part (iv)
uses the fact that this machinery also applies to bimodules.

Corollary 7. Let $G$ act on $R$ with $|G|^{-1} \in R$ and let $V_R$ be a right $R$
module.
   (i) If $V_R$ is Noetherian or Artinian, then so is $V_{RG}$.
   (ii) If $R$ is right Noetherian, then $R$ is a finitely generated $R^G$-module and
   $R^G$ is right Noetherian.
   (iii) If $V_R$ is completely reducible of composition length $n$, then $V_{RG}$ is
   completely reducible of composition length $\leq n \cdot |G|$.
   (iv) If $R$ is a direct sum of $n$ simple rings, then $R^G$ is a direct sum of at most
   $n \cdot |G|$ simple rings.

Part (ii) above is not true in general without the assumption that $|G|^{-1} \in R$.
But the counterexample is not a group ring. Therefore we pose the following
problem. Let $H$ be a polycyclic-by-finite group and let $G$ be a finite group of
automorphisms of $H$. Then $G$ acts on the Noetherian group rings $K[H]$ and
$Z[H]$. Are the fixed subrings necessarily Noetherian?

Here is how to construct a counterexample. Let $N \triangleleft H$ with $\overline{H} = H/N$ infinite
cyclic and let $G = \mathbb{Z}_p$ act on $H$ normalizing $N$. Assume that $C_H(G) \subseteq N$ and
that $G$ acts trivially on $\overline{H}$. Now the fixed points of $G$ on $Z[H]$ are spanned by
the $G$-class sums of $H$ and, since $|G| = p$, these class sums have size $1$ or $p$.
Suppose $h \in H \setminus N$. Then the class sum of $h$ has size $p$ since $C_H(G) \subseteq N$ and all
$G$-conjugates of $h$ are congruent mod $N$ since $G$ acts trivially on $\overline{H}$. Thus, under
the homomorphism $Z[H] \to Z[\overline{H}]$ we see that $Z[H]^G$ maps onto $R = Z + pZ[\overline{H}]$.
But $R$ is not a Noetherian ring since $pZ[\overline{H}]/p^2Z[\overline{H}]$ is a quotient of ideals of $R$
which has infinite $R$-rank.

Fortunately, such automorphisms of polycyclic-by-finite groups do not exist.
Indeed we have

Lemma 8. Let $H$ be a polycyclic-by-finite group and let $G$ be a finite group
of automorphisms of $H$. Then $[H,G] \cdot C_H(G)$ has finite index in $H$.

Proof. Set $W = H \times G$ so that $W$ is also polycyclic-by-finite. Now it is a
standard group theoretic fact that $[H,G] \triangleleft \langle H, G \rangle = W$ and thus we see that
$N = [H,G] \cdot G \triangleleft W$. Since $N$ is polycyclic-by-finite, it has only finitely many
conjugacy classes of finite subgroups, and say these are represented by \( G = G_1, G_2, \ldots, G_k \). We now apply the Frattini argument. To this end let us assume that \( G_1, G_2, \ldots, G_s \) are the groups in this list which are conjugate to \( G \) in \( W \) and say \( G_1 = G^{w_1} \). Then if \( w \in W \), we have \( G^w \subseteq N \) so \( G^w \) is \( N \)-conjugate to one of these \( G_i \), and hence \( G^w = G_i^x = G^{w_i x} \) for some \( x \in N \). This implies that \( w \in N_W(G)w_i, N = N_W(G) \cdot N w_i \) so we see that \( W = \bigcup_{i \leq s} N_W(G) \cdot N w_i \). Hence \( |W : N_W(G) \cdot N| \leq s < \infty \) and the result now follows quite easily.

The final and perhaps most successful skew group ring application to Galois theory concerns the behavior of prime ideals. It is based on the earlier study of primes in \( RG \) along with the following classical fact.

**Lemma 9.** Let \( e \neq 0 \) be an idempotent in the ring \( R \) and let \( \varphi \) map the ideals of \( R \) to those of \( eRe \) by \( I^e = eIe \). Then \( \varphi \) determines a one-to-one correspondence between the primes of \( R \) not containing \( e \) and the primes of \( eRe \). Furthermore, if \( P_1 \) and \( P_2 \) are primes of \( R \) not containing \( e \), then \( P_1 \subseteq P_2 \) if and only if \( P_1^e \subseteq P_2^e \).

We remark that if \( \bar{P} \) is a prime ideal of \( eRe \), then its correspondent in \( R \) is the unique largest ideal \( P \) of \( R \) with \( ePe = \bar{P} \).

Now suppose that \( G \) acts on \( R \) with \( |G|^{-1} \in R \). Let \( T \) be a prime ideal of \( R \) and set \( A = \bigcap_{x \in G} T^x \) so that \( A \) is a \( G \)-prime ideal. Since \( RG/AG \cong (R/A)G \) and the latter ring is semiprime, it follows that \( AG = P_1 \cap P_2 \cap \cdots \cap P_n \) is an intersection of \( n \leq |G| \) minimal covering primes. We then get primes \( P_1^e, P_2^e, \ldots, P_n^e \) of \( eRG \). This idea was originally used by Lorenz and me to compare the prime lengths of \( R \) and of \( R^G \). It was then carried to its completion by Montgomery who obtained

**Theorem 10 [4].** Let \( G \) act on \( R \) with \( |G|^{-1} \in R \).

(i) If \( T \) is a prime ideal of \( R \), then \( T \cap R^G = Q_1 \cap Q_2 \cap \cdots \cap Q_k \) is an intersection of \( k \leq |G| \) minimal covering primes. Thus \( T \) lies over finitely many primes of \( R^G \).

(ii) If \( Q \) is a prime ideal of \( R^G \), then there exists a prime ideal \( T \) of \( R \), unique up to \( G \)-conjugation, such that \( T \) lies over \( Q \).

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

![Diagram](image)

The first diagram reads as follows: Let \( T_1 \supseteq T_2 \) be primes of \( R \) and assume that \( T_1 \) lies over the prime \( Q_1 \) of \( R^G \). Then there exists a prime ideal \( Q_2 \) of \( R^G \) with \( Q_1 \supseteq Q_2 \) and such that \( T_2 \) lies over \( Q_2 \). The other diagrams read similarly. We remark that an efficient proof of this result can now be found in [5].
Galois Theory and Crossed Products

We close with two relevant examples. First let \( R = M_n(C) \) be the ring of \( n \times n \) matrices over the complex numbers \( C \), and for each \( 1 \leq i \leq n - 1 \) let \( d_i \) be the diagonal matrix \( d_i = \text{diag}(1, 1, \ldots, -1, 1, \ldots, 1) \) with \(-1\) in the \( i\)th entry and ones elsewhere. Let \( G \) be the group of automorphisms of \( R \) generated by \( g_1, g_2, \ldots, g_{n-1} \) where each \( g_i \) acts like conjugation by \( d_i \). Then \( |G| = 2^{n-1} \) and \( G \) is inner on \( R \). The latter implies that \( RG = R \otimes_C E \) where \( E = C^k[G] \). But \( E \) is semiprime and is generated by the commuting elements \( d_i g_i \), so \( E \simeq \bigoplus |G| C \), a direct sum of \( |G| \) copies of \( C \). Thus \( RG \simeq \bigoplus |G| R \) and therefore \( RG \) has \( |G| = 2^{n-1} \) minimal primes. On the other hand, \( R^G \) is the subring of diagonal matrices of \( R \) so \( R^G \) has precisely \( n \) minimal primes. For \( n \geq 3 \) we see that there are primes lost under the \( \varphi \) map; that is, there are primes containing \( e \).

Finally, let \( A \) be a simple domain over the field \( K \) and assume that \( A \) is not a division ring. Then we can choose \( I \) to be a nonzero left ideal. For example, we could take \( A \) to be the Weyl algebra \( A_1(K) = K[x,y| xy - yx = 1] \) with \( \text{char} \: K = 0 \) and \( I = Ax \). Now define \( R = [K + I \ A] \subseteq M_2(A) \). It follows easily that \( R \) is prime so \( T_2 = 0 \) is a prime ideal of \( R \). Also observe that \( T_1 = [I \ A] \) is a maximal two-sided ideal of \( R \) with \( R/T_1 = K \). Let \( G \) be the group of automorphisms of \( R \) generated by conjugation by \( \text{diag}(1, -1) \). We assume of course that \( \text{char} \: K \neq 2 \). Then \( |G| = 2 \) and \( RG = \text{diag}(K + I, A) \). Thus \( RG \) has two minimal primes one of which is \( Q_2 = \text{diag}(K + I, 0) \). But \( R^G / Q_2 \simeq A \) so \( Q_2 \) is also maximal. Thus we see that there exists no prime \( Q_1 \) of \( R^G \) which completes the diagram below. In other words, the missing Going Up result does indeed fail. It does not fail in \( RG \), but the prime we get may contain \( e \) and, hence, may not correspond to a prime of \( R^G \).

References