Problem 2
Homework 4

C. Blakestad, M. Hartman

Let G be a group with identity e, K a field, and $\sigma : G \to Aut(K)$ a homomorphism. Discover and prove conditions on G, F and σ that are necessary and sufficient for the skew group ring $K[G;\sigma]$ to be semisimple.

The skew group ring $K[G;\sigma]$ consists of formal sums $\sum a_i g_i$ with $a_i \in K$ and $g_i \in G$, where elements of K commute with elements of G under the twist σ, that is $ag \cdot bh = a\sigma(g)(b) \cdot gh$.

Proposition. *If G is finite, $H = \ker(\sigma)$ and $|H|$ is a unit in K, then $K[G;\sigma]$ is semisimple.*

Proof. Let V be a left $K[G;\sigma]$-module and W an left $K[G;\sigma]$-submodule. Acting by elements of the form $a \cdot e$ on elements of V, we have that V is a K vector space and W a K subspace, so $V = W \oplus W'$ as K-vector spaces, for some K vector space W'. Hence there is a K-linear map $f : V \to W$ with $f|_W$ the identity on W (projection onto W).

We will use f to define a new function from V to W which is also the identity on W, but which is a $K[G;\sigma]$-module homomorphism. Define $z_a : V \to V$ by

$$z_a(v) = \sum_{g \in G} ga \cdot f(g^{-1}v)$$

where a is an element of K. Note this sum is well-defined because G is finite. If $w \in W$, then $g^{-1}w \in W$, hence is fixed by f, so

$$gaf(g^{-1}w) = \sigma(g)(a)gf(g^{-1}w) = \sigma(g)(a)gg^{-1}w = \sigma(g)(a)w,$$

hence

$$z_a(w) = \sum_{g \in G} \sigma(g)(a)w = \left(\sum_{g \in G} \sigma(g)(a)\right) w = \left(|H| \sum_{g \in T} \sigma(g)(a)\right) w,$$

where T is a subset of G which contains exactly one member from each coset of G/H. The last equality holds because σ sends all members of the coset gH to the same automorphism of K. Since the image A of σ is precisely G/H, the image of each coset is a distinct member of A and each member of A arises in such a fashion. Hence

$$\sum_{g \in T} \sigma(g)(a) = \sum_{\bar{g} \in G/H} \bar{\sigma}(\bar{g})(a)$$

where $\bar{g}$ is the image of g in G/H under the quotient map and $\bar{\sigma}$ is the map induced by σ from G/H to the automorphisms of K. The right hand sum is precisely the trace of a from K down to the fixed field F of the action of A. Hence combining the last two equation lines, we have $z_a(w) = \left(|H| Tr_F^K(a)\right) w$. Thus if there is an element b of K with trace $|H|^{-1}$, we will have z_b be the identity on W.

It suffices to know that $Tr_F^K : K \to F$ is surjective since any automorphism of K must fix all multiples of 1, including $|H|$, hence it must also fix $|H|^{-1}$, so $|H|^{-1}$ is an element of F. Since Tr_F^K is F-linear, it is enough for the trace to not be the zero map. But by Dedekind's Theorem on linear independence of characters, the trace map $Tr : K \to F$ is never the zero map for finite Galois extensions K/F.

Defining z as z_b from above, we have that z acts as the identity on W. On the other hand, since f maps V to W and G fixes W, for any $v \in V$, we have $z(v) \in W$. It remains to show that z is a $K[G;\sigma]$-module homomorphism. Since the action of G on V is $\mathbb{Z}$-linear as is f, then z is also $\mathbb{Z}$-linear. Thus it suffices to show that the action of z commutes with multiplication by an element of the form $a \cdot g$ for $a \in K$ and $h \in G$. For $v \in V$, we have:

$$\begin{aligned}
z(ahv) &= \sum_{g \in G} gbf(g^{-1}ahv) \\
&= \sum_{g \in G} gbf(\sigma(g^{-1})(a)g^{-1}hv) \\
&= \sum_{g \in G} g\sigma(g^{-1})(a)bf(g^{-1}hv) \\
&= \sum_{g \in G} \sigma(g)(\sigma(g^{-1})(a))gbf(g^{-1}hv) \\
&= \sum_{g \in G} \sigma^{-1}(g^{-1})(\sigma(g^{-1})(a))gbf(g^{-1}hv) \\
&= \sum_{g \in G} agbf(g^{-1}hv) \\
&= a \sum_{g \in G} gbf(g^{-1}hv).
\end{aligned}$$

Setting $g' = h^{-1}g$, we have $hg' = hh^{-1}g = g$ and $g'^{-1} = g^{-1}h$ with the g' still running over all of G, so

$$\begin{aligned} z(ahv) &= a\sum_{g\in G} gbf(g^{-1}hv) \\ &= a\sum_{g'\in G} hg'bf(g'^{-1}v) \\ &= ah\sum_{g'\in G} g'bf(g'^{-1}v) \\ &= ah\cdot z(v). \end{aligned}$$

Hence $z : V \to W$ is a $k[G;\sigma]$-module homomorphism which is the identity on W hence $V = W \oplus \ker(z)$. Thus any submodule of an arbitrary module is complemented, so $K[G;\sigma]$ is semisimple.

□

Lemma. *If $K[G;\sigma]$ is semisimple then G is finite.*

Proof. We will show independently that both H and G/H are finite.

To show H is finite, we note that σ can be extended to a map $\varepsilon : K[G;\sigma] \to K[G/H;\bar{\sigma}]$ which is the identity on K and acts as σ on G, where $\bar{\sigma}$ is the induced map of σ on G/H into the automorphism group of K. Let I be the ideal of $K[G;\sigma]$ sent to zero under ε. Since $K[G;\sigma]$ is semisimple, there is an ideal J such that $K[G;\sigma] = I \oplus J$. Hence there are nonzero idempotents e and f such that $I = K[G;\sigma]e$, $J = K[G;\sigma]f$, $e + f = 1$, and $ef = 0$. by exercise 1.7 in Lam. For any α in H, we have $\varepsilon(\alpha - 1) = 0$, so $\alpha - 1$ is in I. Then $I \cdot f = K[G;\sigma]e \cdot f = 0$ so in particular $(\alpha - 1)f = 0$, hence $\alpha f = f$ for any $\alpha \in H$. We have $f = \sum_{\beta\in G} a_\beta\beta$ for some $a_\beta \in K$, all but finitely many zero. If $\gamma \in G$ appears in f with a nonzero coefficient, then

$$f = \alpha f = \alpha\sum_{\beta\in G} a_\beta\beta = \sum_{\beta\in G} \sigma(\alpha)(a_\beta)\alpha\beta$$

and $\sigma(\alpha)(a_\gamma) \neq 0$, so the coefficient of $\alpha\gamma$ is nonzero, for all $\alpha \in H$. If H were infinite, then f would not be an element of $K[G;\sigma]$, so H must be finite.

Since G/H is precisely the image of σ, it is the Galois group of K/F. Hence if G/H were infinite, then K/F would be an infinite degree extension and K would be an infinite dimensional vector space over F. We will show that when $K[G;\sigma]$ is semisimple, this cannot be the case.

We will show the multiplication of $K[G;\sigma]$ is defined precisely in such a way that K can be made into a left $K[G;\sigma]$-module under the action

$$\left(\sum_{g\in G} a_g g\right)\cdot k = \sum_{g\in G} a_g\sigma(g)(k).$$

This multiplication is clearly additive in $K[G;\sigma]$ and K, and 1 in $K[G;\sigma]$ acts as the identity on K. It remains only to check associativity:

$$\begin{aligned}
\left(\sum_{g\in G} a_g g\right)\cdot\left(\sum_{h\in G} b_h h\cdot k\right) &= \left(\sum_{g\in G} a_g g\right)\cdot\sum_{h\in G} b_h\sigma(h)(k)\\
&= \sum_{g\in G} a_g\sigma(g)\left(\sum_{h\in G} b_h\sigma(h)(k)\right)\\
&= \sum_{g\in G}\sum_{h\in G} a_g\sigma(g)\left(b_h\sigma(h)(k)\right)\\
&= \sum_{g\in G}\sum_{h\in G} a_g\sigma(g)(b_h)\sigma(g)(\sigma(h)(k))\\
&= \sum_{g\in G}\sum_{h\in G} a_g\sigma(g)(b_h)\sigma(gh)(k)\\
&= \left(\sum_{g\in G}\sum_{h\in G} a_g\sigma(g)(b_h)gh\right)\cdot k\\
&= \left(\sum_{g\in G}\sum_{h\in G} a_g g b_h h\right)\cdot k\\
&= \left(\sum_{g\in G} a_g g\sum_{h\in G} b_h h\right)\cdot k
\end{aligned}$$

hence this multiplication does make K into a left $K[G;\sigma]$-module.

Restricting the scalars to just K, this action is already transitive, so K must be a simple $K[G;\sigma]$-module. Hence the endomorphism ring E must be a division ring. Since any element of E is $K[G;\sigma]$-linear and, in particular, K-linear, elements of E are uniquely determined by where they send 1 and can be viewed as right multiplication by where 1 is sent, ie if e_a is the endomorphism sending 1 to a, then $e_a(k) = ka$ for all $k \in K$. The e_a which are allowable are precisely those which associate with multiplication by elements of $K[G;\sigma]$. Certainly all elements of F will be allowed because

$$\left(\sum_{g\in G} a_g g\right)\cdot kf = \sum_{g\in G} a_g\sigma(g)(fk) = f\sum_{g\in G} a_g\sigma(g)(k) = f\left(\sum_{g\in G} a_g g\cdot k\right) = \left(\sum_{g\in G} a_g g\cdot k\right) f.$$

It remains to show that these are the only allowable elements of K.

If e_f is an left $K[G;\sigma]$-module endomorphism of K and g an element of G, then $e_f(g\cdot 1) = g\cdot e_f(1)$ hence $(g\cdot 1)f = g\cdot(1f)$. For the left hand side, we have $(g\cdot 1)f = \sigma(g)(1)f =$

$1f = f$, and for the right hand side we have $g \cdot (1f) = g \cdot f = \sigma(g)(f)$, hence $\sigma(g)(f) = f$ for all g in G, so f must be in the fixed field of K under G, which is exactly F. Thus E is right multiplication by elements of F. Certainly K is a vector space over F, but since $K[G;\sigma]$ is semisimple and $End_{K[G;\sigma]}(K) = F$, it must be that K is a finite dimensional vector space over F, hence $[K : F]$ is finite. □

Proposition. *If $K[G;\sigma]$ is semisimple, then $|H|$ is a unit in K.*

Proof. It suffices to show that any prime dividing $|H|$ is a unit in K. Let p be a prime dividing $|H|$. By Cauchy's Theorem, there is an element g in H of order p. Since $K[G;\sigma]$ is semisimiple, by Corollary 4.24 in Lam, $K[G;\sigma]$ is von Neumann regular, so there is an element $\alpha \in K[G;\sigma]$ such that $1-g = (1-g)\alpha(1-g)$, and hence $[1-(1-g)\alpha]\cdot(1-g) = 0$. By the following lemma, we have $[1-(1-g)\alpha] \in K[G;\sigma]\cdot(1+h+\cdots+h^{p-1})$, so $[1-(1-g)\alpha] = \beta\cdot(1+g+\cdots+g^{p-1})$, for some $\beta \in K[G;\sigma]$. Applying ε, we have $1 = \varepsilon(\beta)\cdot p$, hence p is a unit in $K[G/H;\bar{\sigma}]$ so cannot be zero in K. □

Lemma. *Let $r \in K[G;\sigma]$, $h \in H = \ker(\sigma)$ an element of order p such that $r\cdot(1-h) = 0$, then $r \in K[G;\sigma]\cdot(1+h+\cdots+h^{p-1})$*

Proof. We will induct on the number n of nonzero terms in $r = \sum_{g\in G} r_g g$, where the $r_g \in K$. If $n = 0$, then $r = 0$ and the result is trivial. If $n \geq 0$, then let $\tau \in G$ be an element with nonzero coefficient in r, then since $r = r\cdot h$ by asumption, $\tau\cdot h^a$ must occur with the same coefficent as τ in r for each integer a. Hence

$$r = r_\tau(\tau + \tau h + \cdots + \tau h^{p-1}) + r' = r_\tau\tau(1+h+\cdots+h^{p-1}) + r',$$

where $r' \in K[G;\sigma]$ with nonzero coefficents only on the elements of G which r had nonzero coefficents, but also with zero coefficients for $\tau, \tau h, \ldots, \tau h^{p-1}$. Since $r' = r - r_\tau\tau(1+h+\cdots+h^{p-1})$, we have

$$\begin{aligned} r'\cdot(1-h) &= (r - r_\tau\tau(1+h+\cdots+h^{p-1}))(1-h) \\ &= r\cdot(1-h) + r_\tau\tau(1+h+\cdots+h^{p-1})\cdot(1-h) \\ &= 0 + r_\tau\tau(1+h+\cdots+h^{p-1}) - r_\tau\tau(1+h+\cdots+h^{p-1})h \\ &= r_\tau\tau(1+h+\cdots+h^{p-1}) - r_\tau\tau(1+h+\cdots+h^{p-1}) \\ &= 0 \end{aligned}$$

since $(1+h+\cdots+h^{p-1})h = (1+h+\cdots+h^{p-1})$, as h is of order p. By the inductive hypothesis, $r' \in K[G;\sigma]\cdot(1+h+\cdots+h^{p-1})$ and $r_\tau\tau(1+h+\cdots+h^{p-1}) \in K[G;\sigma]\cdot(1+h+\cdots+h^{p-1})$, hence so is r.

□