8. Group algebras and Hecke algebras

8.1 Group Algebras

For some calculations with automorphism groups of surfaces it is very useful to use the concepts of a group rings, modules, and more generally, Hecke algebras and their modules.

Definition 8.1 Let $\mathcal{R}$ be any ring and let G be a finite group. Then the group algebra $\mathcal{R}[G]$ is the set of all formal linear combinations α

$$\alpha = \sum_{g \in G} a_g g$$

where $a_g \in \mathcal{R}$. Two group algebra elements $\alpha = \sum_{g \in G} a_g g$ and $\beta = \sum_{g \in G} b_g g$ have a convolution product $\gamma = \alpha\beta$ defined by

$$\begin{aligned} \alpha\beta &= \sum_{g \in G} a_g g \sum_{g \in G} b_g g \\ &= \sum_{g \in G} \sum_{h \in G} a_g b_h gh \\ &= \sum_{g \in G} \left(\sum_{h \in G} a_{gh^{-1}} b_h \right) g. \end{aligned}$$

Proposition 8.1 *The group algebra $\mathcal{R}[G]$ is an associative algebra over $\mathcal{R}$ and if $\mathcal{R}$ is a field then $\mathcal{R}[G]$ is a $|G|$-dimensional vector space. The unit element of $\mathcal{R}[G]$ is obtained by taking $a_1 = 1$ and $a_g = 0$ otherwise.*

For the rest of this chapter we assume that $\mathcal{R}$ is a field.
The link between the automorphism group of a surface and its topology the concept of $\mathcal{R}[G]$-module or representation of G.

Definition 8.2 Let V be an $\mathcal{R}$-vector space and let $\rho : G \to GL(V)$ be a homomorphism from G to the group of $\mathcal{R}$-linear transformations of V. The map ρ is called an $\mathcal{R}$-*representation* of G. For $g \in G$ and $v \in V$ we denote the element $\rho(g)v$ by gv, unless we need to explicitly compare two different representations on V.

Now let $\alpha = \sum_{g \in G} a_g g \in \mathcal{R}[G]$, we define αv:

$$\alpha v = \rho(\alpha)v = \sum_{g \in G} a_g \rho(g) v = \sum_{g \in G} a_g g v. \tag{1}$$

It is easily verified that this definition make V into an $\mathcal{R}[G]$-module, namely the following properties are satisfied for $\alpha, \beta \in \mathcal{R}[G]$, $a, b \in \mathcal{R}$ and $u, v \in V$

$$\alpha(au + bv) = a\alpha u + b\alpha v, \tag{8.2}$$
$$(\alpha + \beta)v = \alpha v + \beta v, \tag{8.3}$$
$$(\alpha\beta)v = \alpha(\beta v), \tag{8.4}$$
$$1v = v. \tag{8.5}$$

These equations all rest on the crucial fact that for each $g \in G$, the map $v \to gv$ is $\mathcal{R}$-linear, and for $g, h \in G$,

$$(gh)v = \rho(gh)v = (\rho(g)\rho(h))v = \rho(g)(\rho(h)v)$$

because ρ is a homomorphism of G to invertible linear transformations. By 8.4, extension $\rho : \mathcal{R}[G] \to \mathrm{End}_{\mathcal{R}}(V)$ is an algebra homomorphism. In particular if we take ρ to be the trivial homomorphism $\rho_0 : G \to \mathcal{R}$ given by $\rho_0(g) = 1$, then

$$\rho_0 : \sum_{g \in G} a_g g \to \sum_{g \in G} a_g \tag{6}$$

is a homomorphism of $\mathcal{R}[G]$ which also may be easily checked by direct calculation.

Definition 8.3 An $\mathcal{R}$-vector space V is called an $\mathcal{R}[G]$-module if there is an action $(\alpha, v) \to \alpha v$ satisfying 8.2 - 8.5 The map $\rho : \mathcal{R}[G] \to \mathrm{End}_{\mathcal{R}}(V)$ defined by $\rho(\alpha)v = \alpha v$ is called the representation of $\mathcal{R}[G]$ afforded by V.

Remark 8.1 Typically we shall call a vector space V a G-module when we really mean it is an $\mathcal{R}[G]$-module.

Example 8.1 If G is a group of automorphisms of a surface then the homology groups $H_n(S; \mathcal{R})$ and the cohomology groups $H^n(S; \mathcal{R})$ are G-modules, as noted in Remark 7.12. The main case of interest is when $n = 1$.

Definition 8.4 If V is a G-module, then a vector subspace $W \subseteq V$ is called a G-submodule if $gW \subseteq W$ for every $g \in G$, or alternatively $\alpha W \subseteq W$ for all $\alpha \in \mathcal{R}[G]$. Module is irreducible if it has no submodules other $\{0\}$ or V.

The main theorem we shall quote from the representation theory of groups is.

Theorem 8.2 *Let $\mathcal{R}$ be a field of characteristic 0. Then every finite dimensional $\mathcal{R}[G]$-module V has a direct sum decomposition*

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$$

into irreducible submodules.

For a G-module V one of the submodules of great interest is the submodule of invariants

$$V^G = \{v \in V : gv = v,\ \forall g \in G\}.$$

The following lemma allows us to easily construct the submodule of invariants.

Lemma 8.3 *Let $\varepsilon_G \in \mathcal{R}[G]$ be defined by*

$$\varepsilon_G = \frac{1}{|G|}\sum_{g\in G} g.$$

Then, the induced map $\varepsilon_G : V \to V^G$, $v \to \varepsilon_G v$ is the projection from V to the G-invariants. More generally, if $H \subseteq G$ is a subgroup then

$$\varepsilon_H = \frac{1}{|H|}\sum_{g\in H} h.$$

defines a projection $\varepsilon_H : V \to V^H$, $v \to \varepsilon_h v$ onto the H-invariants.

Proof. First note that if $v \in V^G$ then

$$\varepsilon_G v = \frac{1}{|G|}\sum_{g\in G} gv = \frac{1}{|G|}\sum_{g\in G} v = v.$$

Thus $V^G \subseteq \varepsilon_G V$. Now for $g \in G$

$$\begin{aligned} g\varepsilon_G &= g\left(\frac{1}{|G|}\sum_{h\in G} h\right) = \frac{1}{|G|}\sum_{h\in G} gh = \frac{1}{|G|}\sum_{k\in gG} k = \varepsilon_G, \text{ and} \\ \varepsilon_G g &= \left(\frac{1}{|G|}\sum_{h\in G} h\right) g = \frac{1}{|G|}\sum_{h\in G} hg = \frac{1}{|G|}\sum_{k\in Gg} k = \varepsilon_G. \end{aligned}$$

It follows that $g(\varepsilon_G v) = (g\varepsilon_G)v = \varepsilon_G v$. Thus $V^G \supseteq \varepsilon_G V$ and so ε_G maps V onto V^G. Next note that

$$\varepsilon_G^2 = \left(\frac{1}{|G|}\sum_{h\in G} h\right)\varepsilon_G = \frac{1}{|G|}\sum_{h\in G}(h\varepsilon_G) = \frac{1}{|G|}\sum_{h\in G}\varepsilon_G = \varepsilon_G.$$

Thus the map $v \to \varepsilon_G v$ is a projection. The proof for the subgroup H is identical. ■
As practice in using the idempotents ε_H and using the homomorphism ρ_0 we proof the following lemma for use in the next section on Hecke algebras.

Lemma 8.4 *Let K, H be a pair of subgroups of G. Then for any $g \in G$ the following hold.*

$$\begin{aligned} \rho_0(\varepsilon_H) &= 1,\ \rho_0(\varepsilon_H g \varepsilon_K) = 1, & (8.7) \\ \varepsilon_H g \varepsilon_K &= \frac{1}{|H|\,|K|}\sum_{h\in H}\sum_{k\in K} hgk = \frac{1}{|HgK|}\sum_{x\in HgK} x, & (8.8) \\ \varepsilon_H\varepsilon_K &= \varepsilon_K\varepsilon_H = \varepsilon_H, \text{ if } K \subseteq H. & (8.9) \end{aligned}$$

Proof. For 8.7, $\rho_0(\varepsilon_H) = 1$, by definition and $\rho_0(\varepsilon_H g \varepsilon_K) = \rho_0(\varepsilon_H)\rho_0(g)\rho_0(\varepsilon_K) = 1 \cdot 1 \cdot 1$. For 8.8 the first part is. In the second part note that there are always $\frac{|H||K|}{|HgK|}$ solutions to $hgk = x$ since $H \times K$ acts transitively on HgK by $(h,k) \cdot x = hxk^{-1}$. Finally 8.9 follows from 8.8 by taking $g = 1$. ■

8.2 Hecke algebras

Let H be a subgroup of G. Frequently we will have the situation where G acts on a module V and the set V^H of H-invariants is of interest (we describe the situation for Riemann surfaces shortly). It would be interesting to know the action of G on V^H, if it existed. Pick $g \in G$ the subspace $g(V^H)$ is easily seen to be invariant under gHg^{-1}. Thus if $H = gHg^{-1}$, $v \to gv$ defines a linear transformation on V^H. However if we want to define this for all of G we need $H = gHg^{-1}$ for all $g \in G$, i.e., H is normal in G. Obviously, this is an atypical situation, however, all is not lost. Recalling that ε_H is the projection from V onto the H -invariants then $v \to \varepsilon_H gv$ is an endomorphism of the H invariants of V, which we shall call a Hecke operator which is a slight variant of the traditional Hecke operator (see Remark 8.2). This additional structure can give us some information. These considerations give rise to an subalgebra of the group algebra whose action on V^H is exactly as described.

Definition 8.5 Let $H \subseteq G$ be of groups then the Hecke subalgebra of G determined by H is the subalgebra generated by elements $\varepsilon_H g \varepsilon_H$ for $g \in G$. It is denoted by $\mathcal{R}[H\backslash G/H]$. The element $\varepsilon_H g \varepsilon_H$ will be called a Hecke basis element

We may find a basis, and a multiplication table of $\mathcal{R}[H\backslash G/H]$ by considering the double cosets HgH, $g \in G$, which are the elements of the double coset space $H\backslash G/H$. Now, two double cosets Hg_1H and Hg_2H are either disjoint or equal. In fact they are equal if and only if $g_2 = h_1 g_1 h_2$, $h_1, h_2 \in H$. From 8.8 $\varepsilon_H g \varepsilon_H$ is the average of the double coset HgH,

$$\varepsilon_H g \varepsilon_H = \frac{1}{|HgH|} \sum_{x \in HgH} x.$$

It follows immediately that the elements $\varepsilon_H g \varepsilon_H$, as HgH runs through the double cosets of H, are linearly independent. Next we show that any product $(\varepsilon_H g_1 \varepsilon_H)(\varepsilon_H g_2 \varepsilon_H)$ is a linear combination of $\varepsilon_H g \varepsilon_H$'s. Thus the $\varepsilon_H g \varepsilon_H$ form a basis for $\mathcal{R}[H\backslash G/H]$. To figure out multiplication we work as follows. Let $H^{(g)} = g^{-1}Hg \cap H$. Each double coset HgH is a disjoint union.

$$HgH = \bigcup_i g_i H \tag{10}$$

where

$$g^{-1}Hg = \bigcup_i (g^{-1}g_i) H^{(g)}$$

is the decomposition of $g^{-1}Hg$ into cosets of $H^{(g)}$. For we have

$$Hg = g(g^{-1}Hg) = g\bigcup_{i=1}^{s}(g^{-1}g_i)H^{(g)} = \bigcup_i g_iH^{(g)}, \tag{11}$$

so

$$HgH = \bigcup_i g_iH^{(g)}H = \bigcup_i g_iH.$$

Also, if $gg_iH = gg_jH$ then $g_ig_j^{-1} \in g^{-1}Hg \cap H = H^{(g)}$, so the union is disjoint. Now from 8.11, and the fact that the union is disjoint we have the commutation relation.

$$\varepsilon_H g = \left(\sum_{i=1}^{s}\frac{1}{s}g_i\right)\varepsilon_{H^{(g)}}. \tag{12}$$

We check verify that factor $1/s$ is correct by applying ρ_0 to both sides of the equation 1. If we multiply both sides of 8.12 on the right by ε_H, we get

$$\varepsilon_H g\varepsilon_H = \left(\sum_{i=1}^{s}\frac{1}{s}g_i\right)\varepsilon_{H^{(g)}}\varepsilon_H = \left(\sum_{i=1}^{s}\frac{1}{s}g_i\right)\varepsilon_H,$$

by 8.9. Finally we have

$$\begin{aligned}(\varepsilon_H h\varepsilon_H)(\varepsilon_H g\varepsilon_H) &= (\varepsilon_H h)(\varepsilon_H\varepsilon_H)(g\varepsilon_H) = (\varepsilon_H h)(\varepsilon_H g\varepsilon_H) \\ &= (\varepsilon_H h)\left(\sum_{i=1}^{s}\frac{1}{s}g_i\right)\varepsilon_H \\ &= \frac{1}{s}\sum_{i=1}^{s}\varepsilon_H(hg_i)\varepsilon_H.\end{aligned} \tag{8.13}$$

By determining which $\varepsilon_H(hg_i)\varepsilon_H$ equal to each other each other we may write out the product as unique linear combination of Hecke basis elements. We summarize this discussion as the following.

Proposition 8.5 *The Hecke algebra is an associative algebra with basis $\varepsilon_H h_j\varepsilon_H$, in 1-1 correspondence to the double cosets Hh_jH of $H\backslash G/H$. The identity element is ε_H, corresponding to the trivial double coset H. The multiplication is given by 8.13. In particular, the product may be written as a linear combination of Hecke basis elements*

$$(\varepsilon_H h\varepsilon_H)(\varepsilon_H g\varepsilon_H) = \sum_{i=1}^{k}\frac{s_j}{s}\varepsilon_H h_j\varepsilon_H,$$

where s and $g_1,\ldots,g_s$ are given in 8.10 and $s_j = |\{i : hg_i \in Hh_jH\}|$.

Remark 8.2 In the traditional situation H is not a finite group but $H^{(g)}$ is of finite index in H. Then each double coset may be represented as a finite union of cosets as in 8.10. These elements may be used to define a Hecke operator $V^H \to V^H$, $v \to \sum_i g_iv$.

In the finite case this is $s\varepsilon_H g\varepsilon_H$. The Hecke algebra has as basis the double cosets HgH with multiplication

$$HhH \cdot HgH = \sum_{i=1}^{s} Hhg_iH.$$

Obviously in the infinite case the Hecke algebra cannot be represented in the group algebra. Thus the traditional Hecke operators are multiples of our Hecke operators. The advantage of traditional Hecke operators is that they are still defined if $s^{-1}is$ not defined in $\mathcal{R}$.

Example 8.2 If $H = N$ a normal subgroup then $\mathcal{R}[H\backslash G/H] = \mathcal{R}[G/N]$ represented as a subalgebra of $\mathcal{R}[G]$.

Remark 8.3 Hecke algebras can be interpreted in terms of transitive group actions on a finite set. Suppose that G acts transitively on a finite set X and that $H = G_{x_1} = \{g \in G : gx_1 = x_1\}$. Let $O_1, \ldots O_k$ be the orbits of H acting on X with $O_1 = \{x_1\}$. Then the double cosets HgH of $H\backslash G/H$ are in 1-1 correspondence with the orbits of H via $Hh_jH \leftrightarrow O_j$ if $O_j = Hh_jHx_1$. The elements $g_1, \ldots, g_s$ in 8.10 may be taken to be elements such that $O_j = \{g_1x_0, \ldots, g_sx_0\}$, and so $s = |O_j|$. Now let HgH be another double coset. For each hg_i, if $hg_ix_0 \in O_j$ then the corresponding Hecke basis element $\varepsilon_H h_j \varepsilon_H$ will occur in the sum in 8.13. If $s_j = \{i : hg_ix_0 \in O_j\}$, Then

$$(\varepsilon_H h \varepsilon_H)(\varepsilon_H g \varepsilon_H) = \sum_{i=1}^{k} \frac{s_j}{s} \varepsilon_H h_j \varepsilon_H.$$

Example 8.3 Let $X = \{1, 2, \ldots n\}$, $G = \Sigma_n$, $H = \Sigma_{n-1}$, identified as the stabilizer of 1. Now let $g = (1, 2)$. Then $g^{-1}Hg$ is the stabilizer of 2 and $H^{(g)} = \Sigma_{n-2}$ the set of all permutations fixing both 1 and 2. Now from 8.10

$$|HgH| = s\,|H| = \frac{|g^{-1}Hg|}{|H^{(g)}|}\,|H| = \frac{|H|}{|H^{(g)}|}\,|H|.$$

Now $s = \frac{(n-1)!}{(n-2)!}$, therefore the coset HgH has $\frac{(n-1)!}{(n-2)!}(n-1)! = (n-1)(n-1)!$ elements. Since $|H| = (n-1)!$ then H and HgH are the only two cosets. Alternatively, H has exactly two orbits on X, $O_1 = \{1\}$ and $O_2 = \{2, 3, \ldots n\}$. We need only compute $(\varepsilon_H g \varepsilon_H)^2$ to determine the multiplication table. From Example 1 we may take the g_i's to be $g_2, g_3, \ldots, g_n$ where $g_i = (1, i)$. Since $h = (1, 2)$ then it moves one element of O_2 to O_1 and $n-2$ elements of O_2 to O_2. Therefore

$$(\varepsilon_H g \varepsilon_H)^2 = \frac{1}{n-1}\varepsilon_H + \frac{n-2}{n-1}\varepsilon_H g \varepsilon_H.$$

Comutant interpretation of Hecke algebra Let V be a G-module. The $\mathcal{R}$-algebra $\mathrm{End}_{\mathcal{R}[G]}(V)$ is the set of $\mathcal{R}$-linear tranforms of V commuting with the action of $\mathcal{R}[G]$

$$\mathrm{End}_{\mathcal{R}[G]}(V) = \{L \in \mathrm{End}_{\mathcal{R}}(V) : L(\alpha x) = \alpha L(x), \forall \alpha \in \mathcal{R}[G]\}.$$

We will show that $\mathcal{R}[H\backslash G/H] \backsimeq \mathrm{End}_{\mathcal{R}[G]}(V)$ where V is the permutation module associated to the coset space G/H.

Proposition 8.6 *Let $H \subseteq G$ be an arbitray pair of finite groups,and let $\mathcal{R}$ be a field. Let V be the permutatio module afforded by the permutation module afforded by the coset space G/H. Then $\mathcal{R}[H\backslash G/H] \backsimeq \mathrm{End}_{\mathcal{R}[G]}(V)$.*

Proof. Let V be the principal left ideal $\mathcal{R}[G]\varepsilon_H$. A basis for V is $t_1\varepsilon_H, \dots t_k\varepsilon_H$, where $T = \{t_1, \dots, t_k\}$ is a transversal of H in G, i.e., $G = \bigcup_i t_i H$, a disjoint union of cosets. From this it easily follows that V is a model for the repsentation of the proposition. Each element of $\mathcal{R}[H\backslash G/H]$ has the form $\gamma = \varepsilon_H \delta \varepsilon_H$, for $\delta \in \mathcal{R}[G]$. The map $R_\gamma : \alpha\varepsilon_H \to \alpha\varepsilon_H(\varepsilon_H\gamma\varepsilon_H)$, $\alpha \in \mathcal{R}[G]$, defines a linear map $V \to V$. Since $(\alpha\beta\varepsilon_H)(\varepsilon_H\gamma\varepsilon_H) = \alpha((\beta\varepsilon_H)(\varepsilon_H\gamma\varepsilon_H))$ then $R_\gamma \in \mathrm{End}_{\mathcal{R}[G]}(V)$. We need to show that

$$\mathcal{R}[H\backslash G/H] \to \mathrm{End}_{\mathcal{R}[G]}(V), \text{ where } \gamma \to R_\gamma$$

is an isomorphism. First suppose that $R_\gamma = 0$, then $0 = R_\gamma(\varepsilon_H) = \varepsilon_H(\varepsilon_H\gamma\varepsilon_H) = \varepsilon_H\gamma\varepsilon_H$, and hence the map $\gamma \to R_\gamma$ is injective. Now suppose that $L \in \mathrm{End}_{\mathcal{R}[G]}(V)$, let $\gamma\varepsilon_H = L(\varepsilon_H)$. Then

$$\begin{aligned} L(\alpha\varepsilon_H) &= L((\alpha\varepsilon_H)\varepsilon_H) \\ &= \alpha\varepsilon_H\gamma\varepsilon_H \\ &= \alpha\varepsilon_H(\varepsilon_H\gamma\varepsilon_H) \\ & R_\gamma(\alpha\varepsilon_H). \end{aligned}$$

■

Corollary 8.7 *Let $H \subseteq G$ be an arbitray pair of finite groups,and let $\mathcal{R}$ be a field whose characteristic does not divide $|G|$. Then $\mathcal{R}[H\backslash G/H]$ is a semisimple algebra isomorphic to a direct sum of matrix rings over a divison algebra.*

Proof. According to Maschke's Lemma $\mathcal{R}[G]$ is a semisimple algebra. It follows from ??? theorem that that $\mathcal{R}[H\backslash G/H] \backsimeq \mathrm{End}_{\mathcal{R}[G]}(V)$ has exactly the the form prescribed by the theorem. ■

8.3 Hecke operators determined by a branched cover

Let S be a surface and let $q : S \to T$ be a branched covering. We particularly have in mind the case where $T = \widehat{\mathbb{C}}$, and q is a rational function, though we allow T to be any surface. We recall from Chapter 6 that we have the following situation. Let

$q : S \to T$ be a branched covering of surfaces. Then there is an essentially unique, Galois, branched cover $p : X \to S$, per the following commutative diagram ($r = q \circ p$).

$$\begin{array}{ccc} X & \xrightarrow{p} & S \\ & \searrow^{r} & \downarrow_{q} \\ & & T \end{array}$$

and a conformal action of a group G on X such that the following hold.

- $G = \{g \in \mathrm{Aut}(X) : r \circ g = r\}$, so that $r : X \to T$ is essentially the quotient map $X \to X/G$.
- Let $H = \{g \in G : p \circ g = p\}$ then the map $p : X \to S$ is the quotient map $X \to X/H$.

Now let us show how the projection defines a Hecke algebra action on the cohomology of S. Let $\mathcal{R} = \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$. By Proposition 7.16 $p^* : H^1(S;\mathcal{R}) \to H^1(X;\mathcal{R})$ is injective and maps isomorphically onto $H^1(X;\mathcal{R})^H$. Therefore, if $g \in G$ and $\omega \in H^1(S;\mathcal{R})$ then $(p^*)^{-1}(\varepsilon_H g \varepsilon_H(p^*\omega))$ lies in $H^1(S;\mathcal{R})$. Thus we may realize $\mathcal{R}[H\backslash G/H]$ as an algebra of Hecke operators on $H^1(S;\mathcal{R})$. Linear transformations of $H^1(S;\mathcal{R})$ which are in the image of $\mathcal{R}[H\backslash G/H]$ will be called operators of Hecke type. The algebra generated by all operators of Hecke type, $\mathcal{H}(S)$ will be called the Hecke algebra of S. The Hecke algebra is a refinement of the automorphism group.

Proposition 8.8 *Let $G = \mathrm{Aut}(S)$ then $\mathcal{R}[G] \to \mathcal{H}(S)$ and is an embedding for $\sigma > 2$. For $\sigma = 2$ the image is $\mathcal{R}[G/\langle\iota\rangle]$ where ι is the hyperelliptic involution.*

Proof. Take $q : S \to T$ to be the map $S \to S/G$. The p is the identity map, and $H = \langle 1 \rangle$. Thus that Hecke action is the standard cohomology action of $\mathrm{Aut}(S)$. The remaining facts are well-known see [15]. ■

8.4 REU Problems

Problem R8.1 Determine formulas similar to those for in [**?**] and [**?**] for the trace of the Hecke operator. Interpret the results in terms of the monodromy representation.

Problem R8.2 Classify all projections $q : S \to T$, for low degree d and small genus σ. Initially assume that T is a sphere, and assume that all the branch point lie on a circle. In this case the Galois cover will carry a locally kaleidoscopic tiling.

Problem R8.3 Find interresting examples of surfaces tiled by trianlgles where the Hecke algebra is strictly greater than the group algebra $\mathbb{C}[G]$.

Problem R8.4 In the examples in Problem 27 find a geometric inerpretation of the elements in the Hecke algebra.