GROUP RINGS

E. L. Lady

Let G be a not-necessarily-abelian group and M a module over a commutative ring R. We say that **G acts on M** if there is a function $G \times M \to M$ (which we write as multiplication) such that $1m = m$ (where 1 here denotes the identity element of G), and for $r \in R,\ g \in G,\ \ g(rm) = r(gm)$, and $g_1(g_2m) = (g_1g_2)m$. (NOTE: The use of the symbol 1 to denote both the identity in R and the identity element of G is an inconsistency which turns out not to create problems.)

We define the **group ring** $R[G]$ as follows: As an R-module, $R[G]$ is the free R-module on the basis $\{g \mid g \in G\}$. Thus every element of $R[G]$ is uniquely represented in the form $\sum_{g\in G} r_g\, g$ with, as usual, almost all r_g trivial. The group operation in G then gives a product defined on all pairs of basis elements. It is easy to see that this extends uniquely to an associative and distributive multiplication on $R[G]$ that makes $R[G]$ into an R-algebra. **Note that the identity element in G is also the identity of R[G].** In fact, we can identify R as a subring of $R[G]$ in such a way that all possible identity elements coincide.

Group rings have been the object of extensive study. The classical text is Donald Passman, Infinite Group Rings (1971). (See also, D. Passman, *What is a group ring?* Amer. Math. Monthly **83** (1976), 173–84 and Passman, The Algebraic Structure of Group Rings (1977).)

One of the main points to notice is that an R-module M together with a group action of G on M is both notationally and conceptually essentially the same thing as an $R[G]$-module.

There is no requirement here that G be finite. However for the case of finite groups, there is a smoothing operation on morphisms which is extremely useful.

Lemma. If G is a finite group and $|G|$ is invertible in R, then for $R[G]$-modules M and N there is an operator that takes R-linear maps $\varphi \in \mathrm{Hom}_R(M,N)$ to $R[G]$-linear maps $\tilde{\varphi} \in \mathrm{Hom}_{R[G]}(M,N)$ such that the following are true:

(1) If φ is $R[G]$-linear then $\tilde{\varphi} = \varphi$.

(2) If $\varphi \in \mathrm{Hom}_R(M,N)$ and $\psi \in \mathrm{Hom}_{R[G]}(N,P)$ then $\widetilde{\psi\varphi} = \psi\tilde{\varphi}$.

PROOF: For $\varphi \in \mathrm{Hom}_R(M,N)$ and $m \in M$, define $\tilde{\varphi}(m) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\varphi(gm)$. To see that $\tilde{\varphi}$ is $R[G]$-linear it suffices to note that for $g_1 \in G$,

$$\begin{aligned}\tilde{\varphi}(g_1 m) &= \frac{1}{|G|}\sum\nolimits_G g^{-1}\varphi(gg_1 m)\\ &= g_1\,\frac{1}{|G|}\sum (gg_1)^{-1}\varphi(gg_1 m)\\ &= g_1\tilde{\varphi}(m),\end{aligned}$$

since multiplication by g_1 permutes the elements of G, so that the family of elements $\{gg_1\}_{g\in G}$ is simply G.

Now if φ is $R[G]$-linear, then

$$\begin{aligned}\tilde{\varphi}(m) &= \frac{1}{|G|}\sum\nolimits_G g^{-1}\varphi(gm)\\ &= \frac{1}{|G|}\sum\nolimits_G g^{-1}g\varphi(m)\\ &= \frac{1}{|G|}\sum\nolimits_G \varphi(m) = \varphi(m).\end{aligned}$$

Also note that if φ is R-linear and ψ is $R[G]$-linear then

$$\begin{aligned}\widetilde{\psi\varphi}(m) &= \frac{1}{|G|}\sum\nolimits_G g^{-1}\psi\varphi(gm)\\ &= \psi\left(\frac{1}{|G|}\sum\nolimits_G g^{-1}\varphi(gm)\right)\\ &= \psi\tilde{\varphi}(m).\end{aligned}$$

☑

Proposition. If $|G|$ is invertible in R and P is an $R[G]$-module which is projective as an R-module, then P is a projective $R[G]$-module.

PROOF: We will show that if M is an $R[G]$-module and $\psi\colon M \to P$ is a $R[G]$-linear epimorphism then ψ splits. Since ψ is R-linear and P is a projective R-module, there exists $\varphi \in \mathrm{Hom}_R(P,M)$ such that $\psi\varphi = 1_P$. Then by the previous Lemma there exists an $R[G]$-linear map $\tilde{\varphi}\colon P \to M$ such that $\psi\tilde{\varphi} = \widetilde{\psi\varphi} = \tilde{1}_P = 1_P$. Therefore ψ is a split epimorphism of $R[G]$-modules. ☑

Maschke's Theorem. If K is a field whose characteristic is zero or relatively prime to $|G|$, then $K[G]$ is a semi-simple ring.

PROOF: It suffices to prove that every $K[G]$-module P is projective. But P is a projective K-module, since K is a field. Thus the result follows from the preceding proposition. ☑

Remark. If G is a finite group and K is a field whose (non-zero) characteristic divides $|G|$, then $K[G]$ is never semi-simple.

PROOF: Let $z = \sum_G g$. Note that for all $g' \in G$, $g'z = z = zg'$ (WHY?). It follows that z is in the center of $K[G]$. It also follows that $z^2 = |G|\, z = 0$ since $|G|$ is a multiple of $\operatorname{char} K$. Thus for all $r \in R$, $(1 + rz)(1 - rz) = 1 - r^2z^2 = 1$, so $1 - rz$ is left invertible. It follows that z is in the Jacobson radical of $K[G]$. Since $z \neq 0$, thus $K[G]$ is not semi-simple. ☑

For $g \in G$, the **conjugacy class** of g is $\{h^{-1}gh \mid h \in G\}$. If G is infinite, then a conjugacy class may be either finite or infinite. If C is a finite conjugacy class, then it is easily seen that $\sum_C g$ is an element of the center of $R[G]$.

HW **Proposition.** The center of $R[G]$ is free as an R-module with a basis consisting of those elements $\sum_C g$, where C ranges over the finite conjugacy classes of G.

For any group algebra $R[G]$ there exists a unique R-algebra morphism $\varepsilon\colon R[G] \to R$ such that $\varepsilon(g) = 1$ for all $g \in G$. This is called the **augmentation map**. $\operatorname{Ker} \varepsilon$ is called the **augmentation ideal** of $R[G]$.

HW **Proposition.** (1) The augmentation ideal is the ideal of $R[G]$ generated by all elements $g - 1$ for $g \in G$.

(2) Let I be the augmentation ideal of $R[G]$. For $g_1, g_2 \in G$, $g_1g_2 - 1 \equiv (g_1 - 1) + (g_2 - 1) \pmod{I^2}$.

(3) Let $[G, G]$ be the **commutator subgroup** of G, i. e. the subgroup generated by all elements $g_1g_2g_1^{-1}g_2^{-1}$ and let I be the augmentation ideal of $\mathbb{Z}[G]$. Then $G/[G, G] \approx I/I^2$.

(4) If G and G' are (not necessarily finite) **abelian** groups and $\mathbb{Z}[G] \approx \mathbb{Z}[G']$ then $G \approx G'$.