Ideais em anéis de grupo

Allysson Gomes Dutra

19 de julho de 2014

Resumo: A proposta deste trabalho é apresentar algumas construções de ideais em um anel de grupos RG se utilizando de subgrupos normais de G, ou de ideais de R. Dentre os ideais construidos, o ideal de aumento $\Delta(G)$ será o mais importante por suas boas propriedades que serão essenciais para a demonstração do teorema de Maschke, que dá condições necessárias e suficientes para que um anel de grupo seja semisimples.

1. Introdução.

Dado um grupo G e um anél R, define-se o anel de grupos RG cujos elementos são combinações lineares da forma

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

onde $a_g \in R$ e somente uma quantidade finita destes coeficiêntes são não-nulos. A soma em RG é definida por

$$\alpha + \beta = \sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g.$$

O produto em RG é definido por

$$\alpha\beta = \left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} a_g b_g gh.$$

Com as operações acima RG é um anel.
Consideremos o grupo G_1 formado pelos elementos $e, -e, i, -i$ e multiplicação formada na seguinte tabela

.	e	-e	i	-i
e	e	-e	i	-i
-e	-e	e	-i	i
i	i	-i	-e	e
-i	-i	i	e	-e

Os elementos de $\mathbb{R}G_1$ são da forma $ae + b(-e) + ci + d(-i)$ com $a, b, c, d \in \mathbb{R}$. Considerando o ideal gerado $I_1 = [1e + 1(-e), 1i + 1(-i)]$ vejamos que $\mathbb{R}G_1/I_1$ é isomorfo ao anel dos complexos . A aplicação

$$\theta : \mathbb{C} \longrightarrow \mathbb{R}G_1/I_1$$

definida por $\theta(a + bi) = (ae + bi) + I_1$ é um homomorfismo de anéis. Se $\theta(a + bi) = 0$, então $ae + bi + I_1 = 0$, assim

$$0 = (ae + bi + I_1)(ae - bi + I_1) = a^2 e + (-b^2(-e)) + I_1,$$

como $1e + I_1 = -1(-e) + I_1$, segue que $-b^2(-e) + I_1 = b^2 e + I_1$, portanto $(a^2 + b^2)e + I_1 = 0$. Logo $a = b = 0$, pois caso contrário temos $a^2 + b^2 \neq 0$, assim

$$1e + I_1 = [1/(a^2 + b^2)e + I_1][(a^2 + b^2)e + I_1] = 0,$$

que implica $I_1 = \mathbb{R}G_1$, contradição.

Seja $ae+b(-e)+ci+d(-i)+I_1 \in \mathbb{R}G_1/I_1$, como $1e+I_1=-1(-e)+I_1$ e $1i+I_1=-1(-i)+I_1$, então

$$-be+I_1=b(-e)+I_1 \; edi+I_1=d(-i)+I_1,$$

assim

$$ae+b(-e)+ci+d(-i)+I_1=(a-b)e+(c-d)i+I_1=\theta((a-b)+(c-d)i).$$

Logo, θ é um isomorfismo.

De forma análoga ao exemplo acima, se considerarmos o grupo G_2 cujos elementos são $e,-e,i,-i,j,-j,k,-k$ e multiplicação formada na seguinte tabela

.	e	-e	i	-i	j	-j	k	-k
e	e	-e	i	-i	j	-j	k	-k
-e	-e	e	-i	i	-j	j	-k	k
i	i	-i	-e	e	k	-k	-j	j
-i	-i	i	e	-e	-k	k	j	-j
j	j	-j	-k	k	-e	e	i	-i
-j	-j	j	k	-k	e	-e	-i	i
k	k	-k	j	-j	-i	i	-e	e
-k	-k	k	-j	j	i	-i	e	-e

então o anel quociente $\mathbb{R}G_2/I_2$ é isomorfo ao anel dos quatérnions $\mathbb{H}$, onde
$I_2=[1e+1(-e),1i+1(-i),1j+1(-j),1k+1(-k)]$.

Podemos ainda definir multiplicação de elementos do anel R por elementos de RG da seguinte maneira, dado $\lambda \in R$ e $\alpha=\sum_{g\in G} a_g g \in RG$ então

$$\lambda\alpha=\lambda\left(\sum_{g\in G} a_g g\right)=\sum_{g\in G}(\lambda a_g)g.$$

Com a multiplicação por elementos de R o anel de grupo RG possui estrutura de R-módulo à esquerda. No caso de R comutativo RG possui estrutura de álgebra sobre R, e neste caso é referido como álgebra de grupo de G sobre R. Ainda no caso em que R é comutativo, é fácil ver que a aplicação $*: RG \longrightarrow RG$ definida por

$$(\sum_{g\in G} a_g g)^*=\sum_{g\in G} a_g g^{-1}$$

é uma involução, ou seja, vale que $(\alpha+\beta)^*=\alpha^*+\beta^*$, $(\alpha\beta)^*=\beta^*\alpha^*$ e $(\alpha^*)^*=\alpha$.

Definição 1.1 Considere a função $\varepsilon: RG \longrightarrow R$ definida por

$$\varepsilon(\sum_{g\in G} a_g g)=\sum_{g\in G} a_g.$$

Esta função é chamada de **aplicação aumento**. Seja $r\in R$, então $\varepsilon(r1)=r$, assim a plicação ε é sobrejetora. Seja $rg\in RG$ e $rh\in RG$ $(g\neq h)$, então $rg\neq rh$ e $\varepsilon(rg)=\varepsilon(rh)=r$, portanto ε não é injetiva. Vejamos que ε é um homomorfismo de RG em R (epimorfismo). Sejam $\alpha=\sum_{g\in G} a_g g\in RG$ e $\beta=\sum_{g\in G} b_g g\in RG$. Então

$$\bullet\varepsilon(\alpha+\beta)=\varepsilon\left(\sum_{g\in G}(a_g+b_g)g\right)=\sum_{g\in G}(a_g+b_g)=\sum_{g\in G}a_g+\sum_{g\in G}b_g=\varepsilon(\alpha)+\varepsilon(\beta).$$

Agora, seja $\alpha=\sum_{g\in G} a_g g\in RG$ e $\sum_{h\in G} b_h h\in RG$, então

$$\bullet\varepsilon(\alpha\beta)=\varepsilon\left(\sum_{g,h\in G} a_g b_h gh\right)=\sum_{g,h\in G} a_g b_h=\left(\sum_{g\in G} a_g\right)\left(\sum_{h\in G} b_h\right)=\varepsilon\left(\sum_{g\in G} a_g g\right)\varepsilon\left(\sum_{h\in G} b_h h\right)=\varepsilon(\alpha)\varepsilon(\beta).$$

Assim temos que $Ker(\varepsilon)$ é um ideal não trivial de RG, e pelo teorema de isomorfismo para anéis conclui-se que

$$RG/Ker(\varepsilon) \cong R.$$

O ideal $Ker(\varepsilon)$ é chamado de **ideal de aumento** de RG e é denotado por $\Delta(G)$.

Proposição 1.2 O conjunto $\{g-1; g \in G, g \neq 1\}$ é uma base para $\Delta(G)$ sobre R, ou seja, $\Delta(G) = \{\sum_{g\in G} a_g(g-1); g \in G, g \neq 1\}$ e $\{g-1; g \in G, g \neq 1\}$ é linearmente independente sobre R.

Demonstração. Seja $\alpha = \sum_{g\in G} a_g g \in \Delta(G)$. Então $\sum_{g\in G} a_g = 0$, assim

$$\alpha = \sum_{g\in G} a_g g - 0 = \sum_{g\in G} a_g g - \sum_{g\in G} a_g 1 = \sum_{g\in G} a_g(g-1),$$

então $\Delta(G)$ é gerado por $\{g-1; g \in G, g \neq 1\}$. Se $\sum_{g\in G} a_g(g-1) = 0$, então

$$\sum_{g\in G} a_g g - \sum_{g\in G} a_g 1 = \sum_{g\in G} a_g g - (\sum_{g\in G} a_g)1 = 0 \Rightarrow a_g = 0$$

para todo $g \in G$ com $g \neq 1$, assim $\{g-1; g \in G, g \neq 1\}$ é linearmente independente, e portanto uma base de $\Delta(G)$ sobre R. $\square$

Note que RG possui dimensão $|G|$ sobre R e $\Delta(G)$ possui dimensão $|G|-1$ sobre R. Se R é um corpo RG e $\Delta(G)$ são espaços vetoriais, caso contrário são R-módulos.

Definição 1.3 Para um subgrupo normal H de um grupo G, denotaremos por $\Delta_R(G,H)$ o ideal de RG gerado pelo conjunto $\{h-1; h \in H\}$. Isto é,

$$\Delta_R(G,H) = \{\sum_{h\in H} \alpha_h(h-1); \alpha_h \in RG\}.$$

Com objetivo de encontrar uma base para $\Delta_R(G,H)$ sobre R, vamos considerar um conjunto $Q = \{q_i\}_{i\in I}$ de elementos de G (representantes) onde as classes laterais q_iH com $i \in I$ formam uma partição disjunta de G. Assim todo elemento $g \in G$ pode ser escrito unicamente da forma $g = q_ih_i$ com $q_i \in Q$ e $h_i \in H$.

Proposição 1.4 O conjunto $B_H = \{q(h-1); q \in Q, h \in H, h \neq 1\}$ é uma base de $\Delta_R(G,H)$ sobre R.

Demonstração. Primeiro vamos demonstrar que B_H é linearmente independente sobre R. Tomemos uma combinação linear $\sum_{i,j} r_{i,j}q_i(h_j-1) = 0$, com $r_{i,j} \in R$. Assim, podemos reescrever como

$$\sum_{i,j} r_{ij}q_ih_j = \sum_i(\sum_j r_{ij})q_i.$$

Como $h_j \neq 1$ para todos valores de j, então $q_ih_j \neq q_k$ para todos i,j,k, assim $r_{ij} = 0$ para todos os valores i,j. Para mostrar que B_H também gera $\Delta_R(G,H)$, é suficiente mostrar que todo elemento da forma $g(h-1)$, com $g \in G$, $h \in H$, pode ser reescrito como combinação linear de elementos em B_H. Como $g = q_ih_j$ para algum $q_i \in Q$ e algum $h_j \in H$. Então

$$g(h-1) = q_ih_j(h-1) = q_i(h_jh-1) - q_i(h_j-1).$$

Logo B_H é uma base de $\Delta_R(G,H)$. $\square$

Observe que $\Delta_R(G,G) = \Delta(G)$.

Sendo H um subgrupo normal de G, podemos considerar o homomorfismo canonico $\rho : G \longrightarrow G/H$ que pode ser estendido como um epimorfismo $\rho^* : RG \longrightarrow R(G/H)$ tal que

$$\rho^*\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \rho(g).$$

Proposição 1.5 Seja H um subgrupo normal de um grupo G. Então, $Ker(\rho^*) = \Delta_R(G,H)$ e

$$\frac{RG}{\Delta_R(G,H)} \cong R(G/H).$$

Demonstração. Todo elemento α de RG pode ser escrito como como uma soma finita $\alpha = \sum_{i,j} r_{ij} q_i h_j$, $r_{ij} \in R$, $q_i \in Q$ e $h_j \in H$. Então

$$\rho^*(\alpha) = \sum_i (\sum_j r_{ij})\rho(q_i).$$

Consequentemente, se $\alpha \in Ker(\rho^*)$ então $\sum_j r_{ij} = 0$ para cada valor de i. Assim,

$$\alpha = \sum_{i,j} r_{ij} q_i h_j = \sum_{i,j} r_{ij} q_i h_j - \sum_i (\sum_j r_{ij}) q_i = \sum_{i,j} r_{ij} q_i (h_j - 1) \in \Delta_R(G,H).$$

Portanto, $Ker(\rho^*) \subset \Delta(G,H)$. A outra inclusão é trivial. Assim, $Ker(\rho^*) = \Delta(G,H)$ e pelo teorema do isomorfismo têm-se

$$\frac{RG}{\Delta_R(G,H)} \cong R(G/H).$$

□

Pelo visto acima, dado um subgrupo normal H de um grupo G, podemos a partir deste contruir o ideal $\Delta_R(G,H)$ de RG. Agora vamos na direção oposta, a partir de um ideal de RG construiremos um subgrupo normal de G. Seja I um ideal do anel de grupo RG, considere o conjunto

$$\triangledown(I) = \{g \in G; g - 1 \in I\}.$$

Vejamos que $\triangledown(I)$ é um subgrupo de G. Se $g, h \in \triangledown(I)$ então

$$gh - 1 = g(h-1) + g - 1 \in I,$$

disto segue que $gh \in \triangledown(I)$. E se $g \in \triangledown(I)$, temos que

$$g^{-1} - 1 = -g^{-1}(g-1) \in I,$$

portanto $g^{-1} \in \triangledown(I)$, assim $\triangledown(I)$ é um subgrupo de G. Seja $g \in G$ e $h \in \triangledown(I)$, temos que $gh = (ghg^{-1})g$ e ainda

$$h - 1 \in I \Rightarrow g(h-1)g^{-1} \in I \Rightarrow ghg^{-1} - 1 \in I \Rightarrow ghg^{-1} \in \triangledown(I),$$

portanto $g\triangledown(I) \subseteq \triangledown(I)g$. A inclusão oposta é analoga, assim $g\triangledown(I) = \triangledown(I)g$, logo $\triangledown(I)$ é normal. Cabe agora uma pergunta, quem é o subgrupo $\triangledown(\Delta_R(G,H))$?, o próximo resultado trata disso.

Proposição 1.6 Se H é um subgrupo normal de G, então $\triangledown(\Delta_R(G,H)) = H$.

Demonstração. Seja $g \in \triangledown(\Delta_R(G,H))$ diferente de 1. Então $g - 1 \in \Delta(G,H)$ e pode ser representado como a seguir

$$g - 1 = \sum_{i,j} r_{ij} q_i (h_j - 1).$$

Uma vez que 1 aparece no lado esquerdo da igualdade acima, também deve aparecer no lado direito; assim, existe i_0 tal que $q_{i_0} = 1$. Temos que algum elemento da forma $r_{i_0,j}(h_j - 1)$ deve ser igual a $g - 1$, então para algum j_0 tem-se $r_{i_0,j_0}(h_{j_0} - 1) = g - 1$, portanto $g = h_{j_0} \in H$. Logo $\triangledown(\Delta_R(G,H)) \subseteq H$. Como a inclusão oposta é imediata, segue que $\triangledown(\Delta_R(G,H)) = H$.

□

Podemos pensar na outra situação possível, em que se toma um ideal I de RG e se pergunta se o ideal $\Delta_R(G,\nabla(I))$ é igual a I. A resposta é não; é fácil ver que $\Delta_R(G,\nabla(I)) \subseteq I$, mas a inclusão contrária não vale em geral, pois se tomarmos $I = RG$, então $\nabla(I) = G$, entretanto $\Delta(G) \neq RG$.

A partir de subgrupos normais de um grupo G pudemos construir ideais de RG, vejamos agora como obter ideais de RG a partir de ideais de R.
Proposição 1.7 Seja I um ideal de R e seja G um grupo. Então

$$IG = \{\sum_{g\in G} a_g g; a_g \in I\}$$

é um ideal de RG, e também

$$RG/IG \cong (R/I)\,G.$$

Demonstração. Seja $\alpha = \sum_{g\in G} a_g g \in IG$ e $\beta = \sum_{h\in G} b_h h \in RG$ (então $a_g \in I$ e $b_h \in R$ para todos $g, h \in G$).

$$\alpha\beta = \left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} a_g b_h gh \in IG$$

então IG é um ideal de RG.

Defina

$$\theta : \frac{RG}{IG} \longrightarrow \left(\frac{R}{I}\right) G$$

por

$$\theta\left(\sum_{g\in G} b_g g + IG\right) = \sum_{g\in G} (b_g + I) g.$$

Agora vamos mostrar que θ é um isomorfismo.

$$\begin{aligned}
\bullet\theta\left(\sum_{g\in G} a_g g + IG + \sum_{g\in G} b_g g + IG\right) &= \sum_{g\in G}(a_g + b_g + I)g \\
&= \sum_{g\in G}(a_g + I) + \sum_{g\in G}(b_g + I) \\
&= \theta\left(\sum_{g\in G} a_g g + IG\right) + \theta\left(\sum_{g\in G} b_g g + IG\right).
\end{aligned}$$

$$\begin{aligned}
\bullet\theta\left(\left(\sum_{g\in G} a_g g + IG\right)\left(\sum_{h\in G} b_h h + IG\right)\right) &= \sum_{g,h\in G}(a_g b_h + I)gh = \sum_{g\in G}(a_g + I)g \sum_{h\in G}(b_h + I)h \\
&= \theta\left(\sum_{g\in G} a_g g + IG\right)\theta\left(\sum_{h\in G} b_h h + IG\right)
\end{aligned}$$

Portanto θ é um homomorfismo.
Vejamos que θ é bijeção. Se $\theta(\sum_{g\in G} a_g g + IG) = 0$, então $\sum_{g\in G}(a_g + I)g = 0$, assim $a_g + I = 0$ para todo $g \in G$,

e portanto $a_g \in I$ para cada $g \in G$, logo $\sum_{g\in G} a_g g + IG = 0$.

Seja $\sum_{g\in G}(r_g + I)g \in (R/I)G$, temos que $\theta(\sum_{g\in G} r_g g + IG) = \sum_{g\in G}(r_g + I)g \in (R/I)G$.

Logo θ é um isomorfismo. $\square$

2. Semisimplicidade.

Nosso objetivo a seguir é determinar as condições necessárias e suficientes sobre um grupo G e um anel R para que o anel de grupo RG seja semisimples. Começaremos definindo semisimplicidade para módulos e para anéis e depois trabalhamos alguns resultados necessários para cumprir nosso objetivo.

Definição 1.8 Um R-módulo M é chamado semisimples se todo submódulo de M é um somando direto. E um anel R é chamado semisimples se ele for um R-módulo a esquerda semisimples.

Proposição 1.9 R é um anel semisimples se e somente se todo R-módulo é semisimples.

Demonstração. Resultado 2.5.7 da referência [1]. □

Gostariamos de saber se submódulo de um R-módulo semisimples também é semisimples, é disto que trata a próxima proposição.

Proposição 2.0 Seja $N \neq \{0\}$ um submódulo de um R-módulo semisimples M. Então N é semisimples.

Demonstração. Seja S um submódulo arbitrário de N. Então S é também um submódulo de M, assim existe outro submódulo S' tal que $M = S \oplus S'$. Vejamos que $N = S \oplus (S' \cap N)$. De fato, claramente $S \cap (S' \cap N) \subseteq S \cap S = \{0\}$. Dado um elemento $n \in N$, nós podemos escrever $n = x + y$ com $x \in S$ e $y \in S'$. Mas $y = n - x \in N$, então $y \in N \cap S'$, como dejado. □

Com a ajuda do resultado acima vamos mostrar que módulos quocientes de R-módulos semisimples também são semisimples.

Corolário 2.1 Seja N um submódulo de um R-módulo semisimples M. Então M/N é isomorfo a um submódulo de M e portanto também é semisimples.

Demonstração. Sendo M semisimples, existe um submódulo N' de M tal que $M = N \oplus N'$, como $N \oplus N'/N \cong N'$, segue pela proposição acima que M/N é semisimples. □

Agora voltaremos a lidar com anéis de grupos, onde definiremos algumas noções de RG para formular e demonstrar os próximos resultados. Seja X um subconjunto de um anel de grupo RG. O anulador à esquerda de X é o conjunto

$$Ann_l(X) = \{\alpha \in RG; \alpha x = 0, \forall x \in X\}.$$

De forma análoga nós definimos o anulador à direita de X por

$$Ann_r(X) = \{\alpha \in RG; x\alpha = 0, \forall x \in X\}.$$

Dado um elemento $\alpha = \sum_{g \in G} a_g g$ nós definimos o suporte de α como sendo o subconjunto de elementos de G que aparecem efetivamente na expressão de α, isto é:

$$supp(\alpha) = \{g \in G; a_g \neq 0\}.$$

Lema 2.2 Seja H um subgrupo normal de um grupo G e R um anel. Então $Ann_r(\Delta(G, H)) \neq 0$ se e somente se H é finito.

Demonstração. Consideremos que $Ann_r(\Delta(G, H)) \neq 0$ e escolha $\alpha = \sum_{g \in G} a_g g \neq 0$ em $Ann_r(\Delta(G, H))$. Para cada elemento $h \in H$ nós temos que $(h - 1)\alpha = 0$, consequentemente $h\alpha = \alpha$. Isto é,

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

Tome $g_0 \in supp(\alpha)$. Então, $\alpha_{g_0} \neq 0$ e a igualdade acima mostra que $hg_0 \in supp(\alpha)$ para todo $h \in H$. Uma vez que $supp(\alpha)$ é finito, isto claramente implica que H deve ser finito. □

Lema 2.3 Seja I um ideal de um anel R. Suponha que existe um ideal à esquerda J tal que $R = I \oplus J$ (como um R-módulo à esquerda). Então, $J \subseteq Ann_r(I)$.

Demonstração. Tome elementos arbitrários $x \in J$, $y \in I$. Uma vez que J é um ideal à esquerda e I um ideal, nós temos que $yx \in J \cap I = \{0\}$. Consequentemente, $yx = 0$ e então $x \in Ann_r(I)$.

□

Lema 2.4 Para $\alpha \in RG$, e $g \in G$ de ordem p, $\alpha(1-g) = 0$ se e somente se $\alpha \in RG(1 + g + ... + g^{p-1})$.

Demonstração. Lema 6.2 da referência [3].

□

Lema 2.5 Se RG é semisimples, então G é finito e $|G|$ é invertível em R.

Demonstração. Assumindo que $\Delta(G)$ é um somando direto de RG, o lema acima diz que $Ann_r(\Delta(G)) \neq 0$ e portanto pelo **lema 2.2** G é finito
Seja p um primo que divide $|G|$, pelo teorema de Cauchy na teoria de grupos existe um elemento $g \in G$ de ordem p. Sendo RG semisimples, segue do resultado 4.24 da referência [3] que RG é Von Neumann regular, então existe um elemento $h \in RG$ tal que $(1-g)h(1-g) = 1-g$, então $[1-(1-g)h](1-g) = 0$. Pelo lema acima, nós podemos escrever $1-(1-g)h = \beta(1+g+...+g^{p-1})$ para algum $\beta \in RG$. Utilizando a aplicação aumento ε obtemos $1 = \varepsilon(\beta)p$, então p é invertível em R. Decompondo $|G|$ em números primos, pelo que acabamos de mostrar segue que $|G|$ é produto de invertíveis, portanto $|G|$ também é invertível.

□

Com base nos resultados auxiliares desenvolvidos acima poderemos determinar as condições necessárias e suficiente sobre um anel R e um grupo G para que o anel de grupo RG seja semisimples, resultado este devido a Heinrich Maschke (1853-1908).

Teorema 2.6 (**Maschke**) Seja G um grupo. Então, o anel de grupo RG é semisimples se e somente se as seguintes condições são satisfeitas:

1. R é um anel semisimples.
2. G é finito.
3. $|G|$ é invertível em R.

Demonstração. Assuma que RG é semisimples. Nós sabemos que $R \cong RG/\Delta(G)$, assim pelo **corolário 2.1** segue que R é semisimples. A semisimplicidade de RG implica pelo **lema 2.5** que G é finito e $|G|$ é invertível em R.
Reciprocamente, assuma que as condições 1.,2. e 3. valem e que M é um RG-submódulo de RG. Uma vez que R é semisimples, segue pelo **proposição 1.9** que RG é semisimples como um R-módulo. Consequentemente , existe um R-submódulo N de RG tal que $RG = M \oplus N$. Seja $\pi : RG \longrightarrow M$ a projeção canonica associada a esta soma direta, defina $\pi^* : RG \longrightarrow M$ pela seguinte expressão

$$\pi^*(x) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gx).$$

Vejamos que π^* é um RG-homomorfismo tal que $(\pi^*)^2 = \pi^*$ e $Im(\pi^*) = M$. Uma vez que π^* é um R-homomorfismo, para mostrar que também é um RG-homomorfismo é suficiente mostrar que $\pi^*(ax) = a\pi^*(x)$, para todos $x, a \in G$. Nós temos

$$\pi^*(ax) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gax) = \frac{a}{|G|} \sum_{g \in G} (ga)^{-1}\pi((ga)x).$$

Quando g percorre todos os elementos de G, o produto ga também percorre todos os elementos de G, assim

$$\pi^*(ax) = \frac{a}{|G|} \sum_{t \in G} t^{-1}\pi(tx) = a\pi^*(x).$$

Uma vez que π é uma projeção em M, nós sabemos que $\pi(m) = m$, paratodos $m \in M$. Também, sabendo que M é um RG-módulo, temos $gm \in M$ para todos $g \in G$. Segue que

$$\pi^*(m) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gm) = \frac{1}{|G|} \sum_{g \in G} g^{-1}gm = m.$$

Dado um elemento arbitrário $x \in RG$, nós temos que $\pi(gx) \in M$, consequentemente $\pi^*(x) \in M$ e disto segue que $Im(\pi^*) \subset M$. Portanto $\pi^*(\pi^*(x)) = \pi^*(x)$ para todos os $x \in RG$ e assim, $(\pi^*)^2 = \pi^*$. Finalmente, o fato de $\pi^*(m) = m$, para todo $m \in M$ também mostra que $M \subset Im(\pi^*)$, logo $M = Im(\pi^*)$.
Agora mostraremos que M é um somando direto no RG-módulo RG. Dado $x \in RG$, temos que $x = \pi^*(x) + (x - \pi^*(x))$. Como $\pi^*(x - \pi^*(x)) = 0$, então $x - \pi^*(x) \in Ker(\pi^*)$, assim $RG = M + Ker(\pi^*)$.
Se $x \in M \cap Ker(\pi^*)$, então $0 = \pi^*(x) = x$, segue que $M \cap Ker(\pi^*) = \{0\}$, portanto $RG = M \oplus Ker(\pi^*)$. Do fato de $Ker(\pi^*)$ também ser um RG-submódulo de RG, decorre o desejado. Logo, RG é um anel semisimples. $\square$

Referências

[1] C. Polcino Milies e S. K. Sehgal, An Introduction to Group Rings, 2002, 63-138.
[2] Leo Creedon, A Course In Group Rings, 2003, 25-26.
[3] Tsi-Yuen Lam, A First Course in Noncommutative Rings, 2001.