A decomposition in group rings

Giovani Goraiebe Pollachini

July 18, 2014

Abstract

The aim of this material is to present a decomposition of a group ring RG using idempotents that can be obtained from normal subgroups of G. The definition of a group ring RG is stated, along with some basic properties. Connections between ideals of R and ideals of RG, and of normal subgroups of G and ideals of RG are shown, and it is also pointed out a method to obtain idempotents based on the normal sobgroups of G of finite order. The desired decomposition of RG into a direct sum of rings is, then, obtained. As an example, a decomposition of $\mathbb{Q}\mathbb{Z}_4$ is presented.

1 Definition and basic properties

Definition 1.1. Let G be a group and R a ring (with identity).
The group ring RG is the set

$$RG = \bigoplus_{g \in G} R = R^{(G)} = \left\{ \sum_{g \in G} a_g g : a_g \in R \text{ and } a_g\text{'s are almost always zero} \right\}$$

with

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

$$\sum_{g \in G} a_g g \cdot \sum_{h \in G} b_h h = \sum_{g,h \in G} (a_g b_h) g * h = \sum_{k \in G} c_k k \ , \quad c_k := \sum_{g * h = k} a_g b_h$$

$$1_{RG} = \sum_{g \in G} \delta_{g,e} g = e$$

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

where $*$ and e are the operation and identity of the group G.
In what follows, the sums of the form $\alpha = \sum_{g \in G} a_g g$ have finite terms, and supp α is the set of g's such that $a_g \neq 0$.

It is not difficult to check that the ring properties are satisfied by RG. Additionally, RG is a left R-module, and if $R = K$ is a field, then KG is an algebra over K.

The ring R and the group G can be regarded as subsets of RG via the embeddings

$$\begin{aligned} i_R : R &\to RG & \qquad i_G : G &\to RG \\ r &\mapsto re = \sum_{h\in G} r\delta_{e,h}h & g &\mapsto g = \sum_{h\in G} \delta_{g,h}h \end{aligned}$$

An alternative definition can be stated by means of an universal property.

Definition 1.2. Let G be a group and R a ring (with identity).
A group ring with respect to R and G is a pair (X, ν) such that

$X \supseteq R$ is a ring

$\nu \colon G \to X$ is a mapping and $\nu(g * h) = \nu(g)\nu(h)$ for all $g, h \in G$

the universal property is satisfied: given any ring A and any mapping $f \colon G \to A$ such that $f(g * h) = f(g)f(h)$ for all $g, h \in G$, there exists a unique ring homomorphism $\overline{f} \colon X \to A$ such that $\overline{f} \circ \nu = f$.

It is stated below that the two definitions for a group ring are the same (up to isomorphisms).

Proposition 1.1. *(RG, i_G) is a group ring in the sense of the second definition, and for any other (X, ν) group ring, $X \simeq RG$ as rings (and if $R = K$ is a field, as algebras too).*

An useful consequence of the universal property is stated below.

Corollary 1.2. *Let R be a ring (with unity) and $f \colon G \to H$ be a group homomorphism. Then*

there exists a ring homomorphism $\overline{f} \colon RG \to RH$ such that $\overline{f}(i_G(g)) = i_H(f(g))$ for all $g \in G$.

if R is commutative, then $\overline{f}$ is a homomorphism of R-algebras.

if f is an epimorphism (monomorphism), then $\overline{f}$ is an epimorphism (monomorphism).

2 Ideals in RG

2.1 Augmentation ideals

Using $A = R$ and $f \equiv 1_R$ in the universal property of RG, there exists a ring homomorphism $\epsilon \colon RG \to R$ such that $\epsilon\left(\sum_g a_g g\right) = \sum_g a_g$. In fact, ϵ is an epimorphism, since $r = \sum_g r\delta_{g,e} = \epsilon\left(\sum_g r\delta_{g,e} g\right)$ for all $r \in R$.

Definition 2.1. The epimorphism $\epsilon \colon RG \to R$ given by $\epsilon\left(\sum_g a_g g\right) = \sum_g a_g$ is called the **augmentation mapping** of RG. Its kernel, denoted by $\Delta(G) := \ker(\epsilon)$, is called the **augmentation ideal** of RG.

Proposition 2.1.

$$\Delta(G) = \left\{ \sum_g \left(a_g - \sum_h a_h \delta_{g,e} \right) g \colon a_g \in R \right\}$$
$$= \left\{ \sum_g a_g (i_G(g) - 1_{RG}) \colon a_g \in R \right\}$$

So, the set $\{i_G(g) - 1_{RG} \colon g \in G, g \neq e\}$ *is a basis of* $\Delta(G)$.

As $\Delta(G)$ is not a trivial ideal (if G and R are not trivial), RG is not simple.

Proof. The first equality is shown below. The other set is a reformulation of the first one ($1_{RG} = i_G(g) = \sum_h \delta_{h,e} h$).

($\supseteq$) If $\alpha = \sum_g \left(a_g - \sum_h a_h \delta_{g,e}\right) g$, then

$$\epsilon(\alpha) = \epsilon \left(\sum_g \left(a_g - \sum_h a_h \delta_{g,e} \right) g \right) = \sum_g a_g - \sum_g \sum_h a_h \delta_{g,e}) = \sum_g a_g - \sum_h a_h = 0$$

($\subseteq$) Conversely, if $\alpha = \sum_g a_g g$ is such that $\epsilon(\alpha) = 0$, then

$$\alpha = \sum_g a_g g - \left(\sum_h a_h \right) e = \sum_g \left(a_g - \left(\sum_h a_h \right) \delta_{g,e} \right) g$$

$\square$

Proposition 2.2. $\dfrac{RG}{\Delta(G)} \simeq R$

Proof. It follows from the fact that ϵ is an epimorphism. $\square$

2.2 Relationship between subgroups of G and ideals of RG

There is a way to construct ideals of RG based on normal subgroups of G. And conversely, normal subgroups of G can be build from ideals in RG. These constructs work almost like an invertion, in the sense that:

> if one starts with a normal subgroup $H \trianglelefteq G$ and "operates" two times (one to get an ideal in RG, the other one to get a normal subgroup of G), one recovers H
>
> starting from an ideal $I \trianglelefteq RG$, one goes to a normal subgroup of G and then, to a smaller ideal of RG

The procedure to go from a normal subgroup to an ideal of the group ring is given below. Consider $H \trianglelefteq G$ and let $\omega \colon G \to \frac{G}{H}$ be the canonical projection. Using the universal property of the group ring, with $A = R\left(\frac{G}{H}\right)$ and $f =$

$i_{\frac{G}{H}} \circ \omega \colon G \to R\left(\frac{G}{H}\right)$ (noticing that $f(g * h) = f(g)f(h)$), one obtains a ring homomorphism $\overline{\omega} \colon RG \to R\left(\frac{G}{H}\right)$, and

$$\overline{\omega}\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \omega(g) = \sum_{g\in G} a_g [g]$$

Moreover, $\overline{\omega}$ is an epimorphism, because

$$\sum_{i=1}^{n} a_{[g_i]}[g_i] = \sum_{i=1}^{n} a_{[g_i]}\omega(g_i) = \overline{\omega}\left(\sum_{i=1}^{n} a_{[g_i]} g_i\right)$$

Definition 2.2. Given a normal subgroup H of G , define $\Delta_R(G,H) := \ker(\overline{\omega})$

Proposition 2.3. *$\Delta_R(G,H)$ is the ideal generated by the set $\{i_G(h) - 1_{RG} \colon h \in H, h \neq e\}$. So,*

$$\Delta_R(G,H) = \left\{\sum_h \alpha_h (i_G(h) - 1_{RG}) \colon h \in G, a_g \in R\right\}$$

Proof. Let I be the ideal generated by the set $\{i_G(h) - 1_{RG} \colon h \in H, h \neq e\}$.

($\supseteq$) Let $h \in H$. One has $i_G(h) - 1_{RG} \in \Delta(G,H)$, because

$$\begin{aligned}\overline{\omega}(i_G(h) - 1_{RG}) &= \overline{\omega}\left(\sum_g \delta_{g,h} g - \sum_g \delta_{g,e} g\right)\\ &= \sum_g \delta_{g,h}\omega(g) - \sum_g \delta_{g,e}\omega(g)\\ &= i_{\frac{G}{H}}([h]) - i_{\frac{G}{H}}([e]) = 0\end{aligned}$$

Then $I \subseteq \Delta(G,H)$.

($\subseteq$) Let $\alpha = \sum_g a_g g \in \ker(\overline{\omega}) = \Delta(G,H)$. Let τ be a set of representatives of $\frac{G}{H}$. One can write $\alpha = \sum_{i,j} a_{i,j} q_i * h_j$, with $q_i \in \tau$ and $h_j \in H$.

$$\begin{aligned}0 &= \overline{\omega}\Big(\sum_{i,j} a_{i,j} q_i * h_j\Big)\\ &= \sum_i \sum_j a_{i,j}[q_i * h_j] = \sum_i \left(\sum_j a_{i,j}\right)[q_i]\end{aligned}$$

Then $\sum_j a_{i,j} = 0$. So, one can write

$$\begin{aligned}\alpha &= \sum_{i,j} a_{i,j} q_i * h_j\\ &= \sum_i \sum_j a_{i,j} q_i * h_j - \sum_i \left(\sum_j a_{i,j}\right) q_i\\ &= \sum_j \left(\sum_i a_{i,j} i_G(q_i)\right)(i_G(h_j) - 1_{RG})\end{aligned}$$

Thus, $\alpha \in I$.

□

Considering $H = G$, one has $\overline{\omega} = \epsilon$, the augmentation epimorphism, and $\Delta_R(G,H) = \Delta(G)$, the augmentation ideal of G.
As in that case, one has the following proposition:

Proposition 2.4. *Let $H \trianglelefteq G$. Then $\Delta_R(G,H)$ is an ideal of RG and*

$$\frac{RG}{\Delta_R(G,H)} \simeq R\left(\frac{G}{H}\right)$$

Proof. By the comment before the last definition, $\overline{\omega}$ is an epimorphism, and the result follows.

□

So $\Delta(G, \_)$ takes a normal subgroup of G as input and returns an ideal of RG.

On the other hand, let $I \trianglelefteq RG$.

Definition 2.3. $\nabla(I) := \{g \in G \colon i_G(g) - i_G(e) \in I\}$

It is easy to show that $\nabla(RG) = G$.

Proposition 2.5. *$\nabla(I)$ is a normal subgroup of G.*

Proof.
$\nabla(I)$ is non empty because $e \in \nabla(I)$ $(i_G(e) - i_G(e) = 0 \in I)$.
$g, h \in \nabla(I)$ implies $h^{-1} \in \nabla(I)$ and $g * h^{-1} \in \nabla(I)$:

$$\begin{aligned} i_G(h) - i_G(e) \in I &\implies i_G(h)i_G(h^{-1}) - i_G(e)i_G(h^{-1}) = i_G(e) - i_G(h^{-1}) \in I \\ &\implies i_G(h^{-1}) - i_G(e) \in I \end{aligned}$$

$$\begin{aligned} i_G(g * h^{-1}) - i_G(e) &= i_G(g)i_G(h^{-1}) - i_G(g) + i_G(g) - i_G(e) \\ &= i_G(g)\underbrace{\left(i_G(h^{-1}) - i_G(e)\right)}_{\in I} + \underbrace{i_G(g) - i_G(e)}_{\in I} \in I \end{aligned}$$

So $\nabla(I)$ is a subgroup of G.
Now it is shown that $\nabla(I)$ is a normal subgroup. Given $g \in G$ and $h \in \nabla(I)$, one has

$$\begin{aligned} i_G(g * h * g^{-1}) - i_G(e) &= i_G(g)i_G(h)i_G(g^{-1}) - i_G(g)i_G(e)i_G(g^{-1}) \\ &= i_G(g)\underbrace{\left(i_G(h) - i_G(e)\right)}_{\in I} i_G(g^{-1}) \in I \end{aligned}$$

□

Hence, $\nabla(\_)$ takes an ideal of RG as input and returns normal subgroup of G.

The relationship between the operations considered above is given in the propositions below.

Proposition 2.6. *Let $H \trianglelefteq G$ be a normal subgroup. Then*

$$\nabla(\Delta(G,H)) = H$$

Proof.

($\supseteq$) Let $h \in H$. One has $i_G(h) - i_G(e) \in \Delta(G,H)$, because

$$\begin{aligned}
\overline{\omega}(i_G(h) - i_G(e)) &= \overline{\omega}\left(\sum_g \delta_{g,h} g - \sum_g \delta_{g,e} g\right) \\
&= \sum_g \delta_{g,h}\omega(g) - \sum_g \delta_{g,e}\omega(g) \\
&= i_{\frac{G}{H}}([h]) - i_{\frac{G}{H}}([e]) = 0
\end{aligned}$$

Then $h \in \nabla(\Delta(G,H))$.

($\subseteq$) Let $h \in \nabla(\Delta(G,H))$. Then $i_G(h) - i_G(e) \in \Delta(G,H)$ and

$$\begin{aligned}
0 &= \overline{\omega}(i_G(h) - i_G(e)) \\
&= \overline{\omega}\left(\sum_g \delta_{g,h} g - \sum_g \delta_{g,e} g\right) \\
&= \sum_g \delta_{g,h}\omega(g) - \sum_g \delta_{g,e}\omega(g) \\
&= i_{\frac{G}{H}}([h]) - i_{\frac{G}{H}}([e])
\end{aligned}$$

Hence $i_{\frac{G}{H}}([h]) = i_{\frac{G}{H}}([e])$ and $[h] = [e]$. This means that $h \in H$.

$\square$

Proposition 2.7. *Let $I \trianglelefteq RG$ be an ideal. Then*

$$\Delta(G, \nabla(I)) \subseteq I$$

and the equality does not hold in general.

Proof.

($\subseteq$) Let $\omega\colon G \to \frac{G}{\nabla(I)}$ and $\overline{\omega}\colon RG \to R\left(\frac{G}{\nabla(I)}\right)$.
Then $\Delta(G,\nabla(I)) = \ker(\overline{\omega})$. Denote $H = \nabla(I)$.
Let $\sum_g a_g g \in \ker(\overline{\omega})$.

$$\begin{aligned}
0 &= \overline{\omega}(\sum_g a_g g) \\
&= \sum_{g\in G} a_g \omega(g) \\
&= \sum_{\sigma \in \frac{G}{H}} \sum_{h\in\sigma} a_h \sigma
\end{aligned}$$

Therefore $\sum_{h\in\sigma} a_h = 0$ for all $\sigma \in \frac{G}{H}$.
Now notice that

$$\begin{aligned}
[g] = [h] &\implies h * g^{-1} \in H \\
&\implies i_G(h * g^{-1}) - i_G(e) = i_G(h) i_G(g^{-1}) - i_G(e) \in I \\
&\implies i_G(h) i_G(g^{-1}) i_G(g) - i_G(e) i_G(g) = i_G(h) - i_G(g) \in I
\end{aligned}$$

Then

$$\begin{aligned}
\sum_g a_g g &= \sum_{\sigma\in\frac{G}{H}} \sum_{h\in\sigma} a_h h \\
&= \sum_{[g]\in\frac{G}{H}} \sum_{h\in[g]} a_h i_G(h) - \sum_{[g]\in\frac{G}{H}} \underbrace{\sum_{h\in[g]} a_h}_{=0} i_G(g) \\
&= \sum_{[g]\in\frac{G}{H}} \sum_{h\in[g]} \underbrace{i_R(a_h)}_{\in RG} \underbrace{(i_G(h) - i_G(g))}_{\in I} \in I
\end{aligned}$$

($\not\supseteq$) Consider $I = RG$. Then $\nabla(I) = G$ and $\Delta(G, \nabla(I)) = \Delta(G, G) \neq RG$.

□

2.3 Relationship between ideals in R and ideals in RG

Proposition 2.8. *Let $I \trianglelefteq R$. Then $IG \trianglelefteq RG$ and*

$$\frac{RG}{IG} \simeq \left(\frac{R}{I}\right) G$$

Proof.

- ($IG \trianglelefteq RG$):
  IG is a commutative group under $+$. Let $\alpha = \sum_{g\in R} a_g g \in RG$ and $\beta = \sum_{h\in R} b_h h \in IG$. Then

  $$\alpha\beta = \left(\sum_g a_g g\right)\left(\sum_h b_h h\right) = \sum_{g,h} \underbrace{(a_g b_h)}_{\in I} g * h \in IG$$

  Hence IG is an ideal of RG.

- ($\frac{RG}{IG} \simeq \left(\frac{R}{I}\right) G$):
  Define $\theta\colon \frac{RG}{IG} \to \left(\frac{R}{I}\right) G$ by $\theta\left(\sum_g a_g g + IG\right) = \sum_g (a_g + I) g$. It is well defined because:

  $$\begin{aligned}
  \sum_g a_g g + IG = \sum_g b_g g + IG &\implies \sum_g a_g g - \sum_g b_g g = \sum_g (a_g - b_g) g \in IG \\
  &\implies a_g - b_g \in I,\ \forall g \\
  &\implies a_g + I = b_g + I,\ \forall g \\
  &\implies \sum_g (a_g + I) g = \sum_g (b_g + I) g
  \end{aligned}$$

It is clear that θ is an epimorphism. It is a monomorphism since

$$\sum_g (a_g + I)g = 0 \implies a_g + I = 0,\ \forall g \implies a_g \in I,\ \forall g$$
$$\implies \sum_g a_g g \in IR \implies \sum_g a_g g + IG = 0$$

$\square$

3 Idempotents and a decomposition in RG

There is a standard procedure for constructing idempotents in RG from the finite subgroups of G.

Lemma 3.1. *Let R be a ring (with unity) and let H be a finite subgroup of a group G. Suppose that $|H|$ is invertible in R. Then, setting $\hat{H} := \sum_{h\in H} i_G(h)$,*

$$e_H := \frac{1}{|H|}\hat{H}$$

is an idempotent of the group ring RG. Moreover, if H is a normal subgroup, then e_H is central.

Proof.

- (e_H is an idempotent:)
  One has $i_G(h)\hat{H} = \sum_{h'\in H} i_G(h * h') = \sum_{h''\in H} i_G(h'') = \hat{H}$ for all $h \in H$ (changing the index h' to $h'' = h * h'$ in the sum, and $h' \in H \Leftrightarrow h'' \in H$)

$$\begin{aligned} e_H e_H &= \frac{1}{|H|^2}\hat{H}\hat{H} = \frac{1}{|H|^2}\left(\sum_{h\in H} i_G(h)\right)\hat{H} = \frac{1}{|H|^2}\sum_{h\in H} i_G(h)\hat{H} \\ &= \frac{1}{|H|^2}\sum_{h\in H}\hat{H} = \frac{1}{|H|^2}|H|\hat{H} = \frac{1}{|H|}\hat{H} = e_H \end{aligned}$$

- (e_H is central if $H \trianglelefteq G$:)
  For all $g \in G$, one has $g^{-1}Hg = H$. Hence

$$i_G(g^{-1})\hat{H} i_G(g) = \sum_{h\in H} i_G(g^{-1} * h * g) = \sum_{h'\in H} i_G(h') = \hat{H}$$

$\square$

Lemma 3.2. *Let R be a ring (with unity) and let H be a subgroup of a group G. Then*

$$Ann_r(\Delta(G,H)) \neq 0 \iff H \text{ is finite}$$
$$\left[Ann_l(\Delta(G,H)) \neq 0 \iff H \text{ is finite}\right]$$

In that case,

$$Ann_r(\Delta(G,H)) = \hat{H}\ RG$$
$$\left[Ann_l(\Delta(G,H)) = RG\ \hat{H}\right]$$

Furthermore, if $H \trianglelefteq G$, then

$$Ann_r(\Delta(G,H)) = \hat{H}\ RG = RG\ \hat{H} = Ann_l(\Delta(G,H))$$

Proof. The case in [ ] is analogous, so only the other case is proved.

($\Rightarrow$) Let $\mathrm{Ann}_r(\Delta(G,H)) \neq 0$, and let $\alpha = \sum_g a_g g \in \mathrm{Ann}_r(\Delta(G,H))$ with $\alpha \neq 0$.
For all $h \in H$, $i_G(h) - 1_{RG} \in \Delta(G,H)$, so $(i_G(h) - 1_{RG})\alpha = 0$.
Hence $i_G(h)\alpha = \alpha$, and $\sum_g a_g h * g = \sum_g a_g g$.
Let $g_0 \in$ supp α so $a_{g_0} \neq 0$. Then $h * g_0 \in$ supp α, $\forall h \in H$. But supp α is finite so H is finite.

($\Leftarrow$) Conversely, let H be finite. Then setting $\hat{H} = \sum_{g\in H} i_G(g)$,

$$(i_G(h) - 1_{RG})\hat{H} = i_G(h)\hat{H} - \hat{H} = \sum_{g\in H} i_G(h*g) - \hat{H} = \sum_{g\in H} i_G(g) - \hat{H} = 0$$

for all $h \in H$.
Since $S = \{i_G(h) - 1_{RG} \colon h \in H\}$ generates the left ideal $\Delta(G,H)$ in RG, then $RG\ S = \Delta(G,H)$ is anihilated in the right by $\hat{H}$.

- Now assume $\mathrm{Ann}_r(\Delta(G,H)) \neq 0$. Now it is shown that $\mathrm{Ann}_r(\Delta(G,H)) = \hat{H}\ RG$:

  ($\subseteq$) Let $\alpha = \sum_g a_g g \in \mathrm{Ann}_r(\Delta(G,H))$, $\alpha \neq 0$. As before, in ($\Rightarrow$), one has $\sum_g a_g h^{-1} * g = \sum_g a_g g$, so $\sum_g a_{h*g} g = \sum_g a_g g$, and $a_{h*g} = a_g$. Hence, setting τ a set of representatives of the classes in $\frac{G}{H}$,

$$\begin{aligned}\alpha = \sum_g a_g g &= \sum_{g\in\tau}\sum_{h\in H} a_{h*g}(h*g) = \sum_{g\in\tau}\sum_{h\in H} a_g(h*g)\\ &= \sum_{h\in H}\sum_{g\in\tau} a_g i_G(h) i_G(g) = \sum_{h\in H} i_G(h)\left(\sum_{g\in\tau} a_g i_G(g)\right)\\ &= \hat{H}\left(\sum_{g\in\tau} a_g i_G(g)\right) \in \hat{H}\ RG\end{aligned}$$

  So $\mathrm{Ann}_r(\Delta(G,H)) \subseteq \hat{H}\ RG$

  ($\supseteq$) It is clear from the proof of ($\Leftarrow$).

- If $H \trianglelefteq G$, then $\hat{H}$ is central and

$$\mathrm{Ann}_r(\Delta(G,H)) = \hat{H}\ RG = RG\ \hat{H} = \mathrm{Ann}_l(\Delta(G,H))$$

□

Proposition 3.3. *Let R be a ring (with unity) and let H be a finite normal subgroup of a group G. Suppose that $|H|$ is invertible in R. Set $\hat{H} := \sum_{h\in H} i_G(h)$ and $e_H := \frac{1}{|H|}\hat{H}$ as above. Then one has the following decomposition*

$$RG = RGe_H \dotplus RG(1_{RG} - e_H)$$

where $RGe_H \simeq R\left(\frac{G}{H}\right)$ and $RG(1_{RG} - e_H) = \Delta(G,H) = Ann(RGe_H)$

Proof.

- From a previous lemma, e_H is a central idempotent in RG, and it follows that $RG = RGe_H \dot{+} RG(1_{RG} - e_H)$.

- $RGe_H \simeq R\left(\frac{G}{H}\right)$:
One can show first that $\frac{i_G(G)}{i_G(H)} \simeq i_G(G)e_H$ as groups. Indeed,

  $i_G(G)$ is a group since i_G is a group homomorphism

  $i_G(G)e_H$ is a group, with the operation $i_G(g)e_H \cdot i_G(h)e_H = i_G(gh)e_H$ and the inverse $(i_G(g)e_H)^{-1} = i_G(g^{-1})e_H$

  the map $\phi\colon i_G(G) \to i_G(G)e_h,\ \phi(i_G(g)) = i_G(g)e_H$ is a group epimorphism

  $\ker(\phi) = i_G(H)$, since

$$\begin{aligned}\phi(i_G(g)) = i_G(g)e_H = i_G(e)e_H &\implies i_G(g)\frac{1}{|H|}\sum_{h\in H} i_G(h) = \frac{1}{|H|}\sum_{h\in H} i_G(h)\\ &\implies \sum_{h\in H} i_G(g*h) - \sum_{h'\in H} i_G(h') = 0\\ &\implies \forall h \in H,\ g*h \in H \implies g \in H\end{aligned}$$

  and

$$\begin{aligned}g \in H \implies \phi(i_G(g)) = i_G(g)\frac{1}{|H|}\sum_{h\in H} i_G(h) &= \frac{1}{|H|}\sum_{h\in H} i_G(g*h)\\ &\overset{(*)}{=} \frac{1}{|H|}\sum_{h\in H} i_G(h) = e_H\end{aligned}$$

  where in $(*)$, $i_G(g)\hat{H} = \sum_{h\in H} i_G(g*h) = \sum_{h'\in H} i_G(h') = \hat{H}, \forall g \in H$.

  Therefore $\frac{G}{H} \simeq \frac{i_G(G)}{i_G(H)} \simeq i_G(G)e_H$ and $(RG)e_H \simeq R(i_G(G)e_H) \simeq R\left(\frac{G}{H}\right)$

- $RG(1_{RG} - e_H) = \Delta(G,H)$:
Notice that $\mathrm{Ann}_r(\Delta(G,H)) = \hat{H}\ RG = e_H RG = RGe_H = RG\ \hat{H} = \mathrm{Ann}_l(\Delta(G,H))$ from the previous lemma. And,

$$RG(1_{RG} - e_H) = \{\beta = \alpha - \alpha e_H \colon \alpha \in RG\} = \mathrm{Ann}(RGe_H)$$

  because $\beta = \alpha - \alpha e_H \Leftrightarrow \beta e_H = 0 \Leftrightarrow \beta \in \mathrm{Ann}(RGe_H)$.
It is proved below that $\Delta(G,H) = \mathrm{Ann}(RGe_H)$:

  ($\subseteq$) Let $h \in H$. $1_{RG} - i_G(h) \in \mathrm{Ann}(RGe_H)$ since

$$\begin{aligned}(1_{RG} - i_G(h))\alpha e_H &= (1_{RG} - i_G(h))\frac{1}{|H|}\left(\sum_{h'} i_G(h')\right)\alpha\\ &= \left(\frac{1}{|H|}\sum_{h'} i_G(h') - \frac{1}{|H|}\underbrace{\sum_{h'} i_G(h)i_G(h')}_{=\hat{H}}\right)\alpha\\ &= (e_H - e_H)\alpha = 0\end{aligned}$$

As the elements $(1_{RG} - i_G(h))$ generate $\Delta(G, H)$, one has that $\Delta(G, H) \subseteq \mathrm{Ann}(RGe_H)$.

($\supseteq$) Let $\alpha \in \mathrm{Ann}(RGe_H)$. Then $\alpha e_H = 0$, so

$$\begin{aligned} \alpha &= \alpha - \alpha e_H = \alpha(1_{RG} - e_H) = \alpha \left(\frac{1}{|H|} \sum_h 1_{RG} - \frac{1}{|H|} \sum_h h \right) \\ &= \alpha \frac{1}{|H|} \sum_h \underbrace{(1_{RG} - i_G(h))}_{\in \Delta(G,H)} \in \Delta(G, H) \end{aligned}$$

□

Definition 3.1. Let R be a ring and G a finite group with $|G|$ invertible in R. The idempotent $e_G = \frac{1}{|G|}\hat{G}$ is called the **principal idempotent** of RG.

In case $e_G = \frac{1}{|G|}\hat{G}$ is well defined, that is, when $|G|$ is finite and invertible in R, it is possible to conclude that RG has R as a direct summand of rings.

Corollary 3.4. *Let R be a ring and G a finite group with $|G|$ invertible in R. Then*

$$RG \simeq R \dotplus \Delta(G)$$

Proof. Use the proposition with $G = H$:

$$RG \simeq R\left(\frac{G}{G}\right) \dotplus \Delta(G, G) \simeq R \dotplus \Delta(G)$$

□

Example 3.1. Let

- $G = \mathbb{Z}_4 = \{[0], [1], [2], [3]\}$
- $H = 2\mathbb{Z}_4 = \{[0], [2]\} \trianglelefteq H$
- $R = \mathbb{Q}$

G and H are considered as groups under $* := +$ and $\mathbb{Q}$, a ring (actually a field) under the usual operations. Then $RG = \mathbb{Q}\mathbb{Z}_4$ is a group ring, with adition and multiplication denoted by $+$ and $\cdot$ (or juxtaposition), respectively. The group ring operations in $\mathbb{Q}\mathbb{Z}_4$ will also be denoted as $+$ and $\cdot$ (or juxtaposition).
The usual abuse of notation $i_G(g) = g$ will be adopted. And the group operation in $\mathbb{Z}_4$ is to be denoted by $*$ rather than $+$, in order not to be confused with the sum in RG.
For example, $[0] + [1]$ will denote an element in $\mathbb{Q}\mathbb{Z}_4$, and not the operation of the group, which shall be written as $[0] * [1] = [1]$. And there will be expressions such as $[1]\frac{1}{2}([1] + [2]) = \frac{1}{2}([1] * [1]) + \frac{1}{2}([1] * [2]) = \frac{1}{2}[2] + \frac{1}{2}[3]$, which would look odd in the sum notation for $\mathbb{Z}_4$ (although this still looks odd in this $*$ notation).

Since $|H| = 2 \in \mathbb{Q}$ is invertible, one can compute the idempotent associated to H:

$$\begin{aligned}
e_H &= \frac{1}{2}([0]+[2]) \\
e_He_H &= \left(\frac{1}{2}([0]+[2])\right) \cdot \left(\frac{1}{2}([0]+[2])\right) \\
&= \frac{1}{2}\frac{1}{2}\big(([0]*[0]) + ([0]*[2]) + ([2]*[0]) + ([2]*[2])\big) \\
&= \frac{1}{2}\frac{1}{2}([0]+[2]+[2]+[0]) = \frac{1}{2}([0]+[2]) = e_H
\end{aligned}$$

Thus, by proposition 3.3, one has the decomposition

$$\mathbb{Q}\mathbb{Z}_4 \simeq \mathbb{Q}\mathbb{Z}_4 e_H \dotplus \mathbb{Q}\mathbb{Z}_4([0]-e_H)$$

with $\mathbb{Q}\mathbb{Z}_4 e_H \simeq \mathbb{Q}\left(\frac{\mathbb{Z}_4}{2\mathbb{Z}_4}\right)$ and $\mathbb{Q}\mathbb{Z}_4([0]-e_H) = \Delta(\mathbb{Z}_4, 2\mathbb{Z}_4)$.

- $\mathbb{Q}\left(\frac{\mathbb{Z}_4}{2\mathbb{Z}_4}\right) = \{[[0]],[[1]]\} \simeq \left\{\begin{bmatrix} q_0 & q_1 \\ q_1 & q_0 \end{bmatrix} : q_0, q_1 \in \mathbb{Q}\right\}$
  Define the ring isomorphism
  $$\begin{aligned}
  \theta \colon \mathbb{Q}\left(\frac{\mathbb{Z}_4}{2\mathbb{Z}_4}\right) &\to \left\{\begin{bmatrix} q_0 & q_1 \\ q_1 & q_0 \end{bmatrix} : q_0, q_1 \in \mathbb{Q}\right\} \\
  q_0[[0]]+q_1[[1]] &\mapsto \left[\begin{smallmatrix} q_0 & q_1 \\ q_1 & q_0 \end{smallmatrix}\right]
  \end{aligned}$$
  It is clear that this function is a bijection. To see that it is a homomorphism of rings, one notices that the additivity and the unity preservation are trivial, and the multiplication property follows from
  $$\begin{aligned}
  &\theta\Big(\big(q_0[[0]] + q_1[[1]]\big)\big(q_0'[[0]] + q_1'[[1]]\big)\Big) \\
  &= \theta\Big(q_0q_0'[[0*0]] + q_0q_1'[[0*1]] + q_1q_0'[[1*0]] + q_1q_1'[[1*1]]\Big) \\
  &= \theta\Big((q_0q_0' + q_1q_1')[[0]] + (q_0q_1' + q_1q_0')[[1]]\Big) \\
  &= \begin{bmatrix} q_0q_0' + q_1q_1' & q_0q_1' + q_1q_0' \\ q_0q_1' + q_1q_0' & q_0q_0' + q_1q_1' \end{bmatrix} \\
  &= \begin{bmatrix} q_0 & q_1 \\ q_1 & q_0 \end{bmatrix} \begin{bmatrix} q_0' & q_1' \\ q_1' & q_0' \end{bmatrix} \\
  &= \theta\big(q_0[[0]] + q_1[[1]]\big)\theta\big(q_0'[[0]] + q_1'[[1]]\big)
  \end{aligned}$$

- $\mathbb{Q}\mathbb{Z}_4([0]-e_H) = \Delta(\mathbb{Z}_4, 2\mathbb{Z}_4) \simeq \left\{\begin{bmatrix} q_0 & q_1 \\ -q_1 & q_0 \end{bmatrix} : q_0, q_1 \in \mathbb{Q}\right\}$
  First, the set $\Delta(G,H)$ will be determined explicitly. This set is the ideal of $\mathbb{Q}\mathbb{Z}_4$ generated by $\{[0]-[2]\}$.
  Calculating
  $$\begin{aligned}
  [0]([0]-[2]) &= [0]*[0] - [0]*[2] = [0]-[2] \\
  [1]([0]-[2]) &= [1]*[0] - [1]*[2] = [1]-[3] \\
  [2]([0]-[2]) &= [2]*[0] - [2]*[2] = [2]-[0] \\
  [3]([0]-[2]) &= [3]*[0] - [3]*[2] = [3]-[1]
  \end{aligned}$$

one obtains that

$$\Delta(G,H) = \{q_0([0]-[2]) + q_1([1]-[3])\colon q_0, q_1 \in \mathbb{Q}\}$$

Thus, define the ring isomorphism

$$\begin{aligned} \theta\colon \Delta(G,H) &\longrightarrow \left\{ \begin{bmatrix} q_0 & q_1 \\ q_1 & q_0 \end{bmatrix} : q_0, q_1 \in \mathbb{Q} \right\} \\ {\scriptstyle q_0 \frac{1}{2}([0]-[2]) + q_1 \frac{1}{2}([1]-[3])} &\mapsto \left[\begin{smallmatrix} q_0 & q_1 \\ -q_1 & q_0 \end{smallmatrix}\right] \end{aligned}$$

As in the previous item, bijectivity, additivity and unity preservation are trivial. One has

$$\begin{aligned} \tfrac{1}{2}([0]-[2])\tfrac{1}{2}([0]-[2]) &= \tfrac{1}{2}([0]-[2]) \\ \tfrac{1}{2}([0]-[2])\tfrac{1}{2}([1]-[3]) &= \tfrac{1}{2}([1]-[3]) \\ \tfrac{1}{2}([1]-[3])\tfrac{1}{2}([0]-[2]) &= \tfrac{1}{2}([1]-[3]) \\ \tfrac{1}{2}([1]-[3])\tfrac{1}{2}([1]-[3]) &= -\tfrac{1}{2}([0]-[2]) \end{aligned}$$

Thus,

$$\begin{aligned} &\theta\Big(\big(q_0 \tfrac{1}{2}([0]-[2]) + q_1 \tfrac{1}{2}([1]-[3])\big)\big(q_0' \tfrac{1}{2}([0]-[2]) + q_1' \tfrac{1}{2}([1]-[3])\big) \Big) \\ &\quad = \theta\Big(q_0 q_0' \tfrac{1}{2}([0]-[2]) + q_0 q_1' \tfrac{1}{2}([1]-[3]) + q_1 q_0' \tfrac{1}{2}([1]-[3]) - q_1 q_1' \tfrac{1}{2}([0]-[2]) \Big) \\ &\quad = \theta\Big((q_0 q_0' - q_1 q_1') \tfrac{1}{2}([0]-[2]) + (q_0 q_1' + q_1 q_0') \tfrac{1}{2}([1]-[3]) \Big) \\ &\quad = \begin{bmatrix} q_0 q_0' - q_1 q_1' & q_0 q_1' + q_1 q_0' \\ -q_0 q_1' - q_1 q_0' & q_0 q_0' - q_1 q_1' \end{bmatrix} \\ &\quad = \begin{bmatrix} q_0 & q_1 \\ -q_1 & q_0 \end{bmatrix} \begin{bmatrix} q_0' & q_1' \\ -q_1' & q_0' \end{bmatrix} \\ &\quad = \theta\big(q_0 \tfrac{1}{2}([0]-[2]) + q_1 \tfrac{1}{2}([1]-[3])\big)\theta\big(q_0' \tfrac{1}{2}([0]-[2]) + q_1' \tfrac{1}{2}([1]-[3])\big) \end{aligned}$$

Hence, one obtains

$$\mathbb{Q}\mathbb{Z}_4 \simeq \left\{ \begin{bmatrix} q_0 & q_1 \\ q_1 & q_0 \end{bmatrix} : q_0, q_1 \in \mathbb{Q} \right\} \dotplus \left\{ \begin{bmatrix} q_0 & q_1 \\ -q_1 & q_0 \end{bmatrix} : q_0, q_1 \in \mathbb{Q} \right\}$$

References

[1] César P. Milies, Sudarsan K. Sehgal. *An Introduction to Group Rings*, Kluver, Dordrecht-Boston-London, 2002.

[2] Leo Creedon. *A Course In Group Rings*, 2003.

[3] Frank W. Anderson, Kent R. Fuller. *Rings and Categories of Modules*, Second Edition, Springer-Verlag, 1992.