Algebra Homework 6

Samuel Otten

1

Let \((R, +, \cdot)\) be a ring and \(G\) a semigroup. Throughout this problem let \(h, l, m, n\) vary in \(G\) unless clearly fixed. From 3.1.7, we have the semigroup ring \((R[G], +, \cdot)\) of \(G\) over \(R\) with the well-defined multiplicative operation

\[ * : R[G] \times R[G] \to R[G], (r_g)_{g \in G} \cdot (s_g)_{g \in G} \to (t_g)_{g \in G}, \]

where \(t_g = \sum_{hl=g} r_h \cdot s_l\). Note that we are using \(*\) to emphasize when the multiplication is in \(R[G]\).

(a) We will show that \((R[G], +, \cdot)\) is a ring. First, by 2.8.5(a) \(\bigoplus_{g \in G} R_g\) is a subgroup of the direct product of \((R_g \mid g \in G)\), and so \((R[G], +)\) is a group. Let \((r_g)_{g \in G}, (s_g)_{g \in G} \in R[G]\). Then

\[ (r_g)_{g \in G} + (s_g)_{g \in G} = (r_g + s_g)_{g \in G} \quad \text{addition in \(R[G]\) is component-wise} \]
\[ = (s_g + r_g)_{g \in G} \quad \text{addition in \(R\) is commutative} \]
\[ = (s_g)_{g \in G} + (r_g)_{g \in G}. \]

So we see that \((R[G], +)\) is an abelian group.

Second, we must show that \((R[G], \cdot)\) is a semigroup. We know from 3.1.7 that \(*\) is well-defined. For \((r_g)_{g \in G}, (s_g)_{g \in G}, (t_g)_{g \in G} \in R[G]\), observe

\[ (r_g)_{g \in G} \cdot ((s_g)_{g \in G} \cdot (t_g)_{g \in G}) = (r_g)_{g \in G} \cdot \left( \sum_{hl=g} s_h t_l \right) \quad \text{definition of \(*\)} \]
\[ = \left( \sum_{mn=g} r_m \cdot \left( \sum_{hl=n} s_h t_l \right) \right) \quad \text{definition of \(*\)} \]
\[ = \left( \sum_{mn=g} \left( \sum_{hl=n} r_m(s_h t_l) \right) \right) \quad \text{left-multiplication homomorphism in \(R\)} \]

Let us consider the summands \(r_m(s_h t_l)\), where \(mn = g\) and \(hl = n\). This means \(mhl = g\), so

\[ \left( \sum_{mn=g} \left( \sum_{hl=n} r_m(s_h t_l) \right) \right) = \left( \sum_{mhl=g} r_m(s_h t_l) \right) \quad \text{definition of \(*\)} \]
\[ = \left( \sum_{mhl=g} (r_m s_h) t_l \right) \quad \text{(\(R, \cdot\)) is a semigroup} \]
\[ = \left( \sum_{nl=g} \left( \sum_{mhl=n} r_m s_h \right) t_l \right) \quad \text{right-multiplication homomorphism in \(R\)} \]
\[ = \left( \sum_{mh=n} r_m s_h \right) \ast (t_g)_{g \in G} \quad \text{definition of \(*\)} \]
\[ = \left((r_g)_{g \in G} \ast (s_g)_{g \in G}\right) \ast (t_g)_{g \in G} \quad \text{definition of \(*\)} \]

So we see that \(*\) is associative and \((R[G], \cdot)\) is a semigroup.
Third, we must show that
\[
\ell_{(r_g)_{g \in G}} : R[G] \to R[G], (s_g)_{g \in G} \to (r_g)_{g \in G} \ (*)_{g \in G}
\]
is a homomorphism over addition. For \((r_g)_{g \in G}, (s_g)_{g \in G}, (t_g)_{g \in G} \in R[G]\), we have
\[
\ell_{(r_g)_{g \in G}}((s_g)_{g \in G} + (t_g)_{g \in G}) = \ell_{(r_g)_{g \in G}}((s_g)_{g \in G} + (t_g)_{g \in G})
\]
definition of \(\ell\)
\[
= (r_g)_{g \in G} \ (*)_{g \in G} ((s_g)_{g \in G} + (t_g)_{g \in G})
\]
addition in \(R[G]\) is component-wise
\[
= \left( \sum_{h \in G} r_h(s_l + t_l) \right)_{g \in G}
\]
definition of \(*\)
\[
= \left( \sum_{h \in G} r_h s_l + r_h t_l \right)_{g \in G}
\]
left-multiplication homomorphism in \(R\)
\[
= \left( \sum_{h \in G} r_h s_l \right)_{g \in G} + \left( \sum_{h \in G} r_h t_l \right)_{g \in G}
\]
addition in \(R\) is commutative
\[
= (r_g)_{g \in G} \ (*)_{g \in G} + (r_g)_{g \in G} \ (*)_{g \in G}
\]
definition of \(*\)
\[
= \ell_{(r_g)_{g \in G}}((s_g)_{g \in G}) \ + \ell_{(r_g)_{g \in G}}((t_g)_{g \in G}).
\]
definition of \(\ell\)

So we see that left-multiplication is a homomorphism of \((R[G],+)\).

Fourth, we must show that
\[
\mathcal{R}_{(r_g)_{g \in G}} : R[G] \to R[G], (s_g)_{g \in G} \to (s_g)_{g \in G} \ (*)_{g \in G}
\]
is a homomorphism over addition. As above,
\[
\mathcal{R}_{(r_g)_{g \in G}}((s_g)_{g \in G} + (t_g)_{g \in G}) = ((s_g)_{g \in G} + (t_g)_{g \in G}) \ (*)_{g \in G}
\]
definition of \(\mathcal{R}\)
\[
= (s_g + t_g)_{g \in G} \ (*)_{g \in G}
\]
addition in \(R[G]\) is component-wise
\[
= \left( \sum_{h \in G} (s_h + t_h) r_l \right)_{g \in G}
\]
definition of \(*\)
\[
= \left( \sum_{h \in G} s_h r_l + t_h r_l \right)_{g \in G}
\]
right-multiplication homomorphism in \(R\)
\[
= \left( \sum_{h \in G} s_h r_l \right)_{g \in G} + \left( \sum_{h \in G} t_h r_l \right)_{g \in G}
\]
addition in \(R\) is commutative
\[
= (s_g)_{g \in G} \ (*)_{g \in G} + (t_g)_{g \in G} \ (*)_{g \in G}
\]
definition of \(*\)
\[
= \mathcal{R}_{(r_g)_{g \in G}}((s_g)_{g \in G}) + \mathcal{R}_{(r_g)_{g \in G}}((t_g)_{g \in G}).
\]
definition of \(\mathcal{R}\)

So we see that right-multiplication is a homomorphism of \((R[G],+)\). Therefore, by definition 3.1.1, the semigroup ring \((R[G],+,*)\) is indeed a ring.

(b) From group theory (2.8.5), we define \(\rho_g : R \to R[G]\) by \(\rho_g(r) = (r_k)_{k \in G}\), where
\[
\begin{align*}
    r_k &= \begin{cases} 
        r & \text{if } k = g \\ 
        0_R & \text{if } k \neq g.
    \end{cases}
\end{align*}
\]
We often denote \(\rho_g(r)\) by \(rg\), so
\[
\sum_{g \in G} rg = \sum_{g \in G} \rho_g(rg).
\]
Let \((a_g)_{g \in G} \in R[G]\). Then by 2.8.5(d), there exist uniquely determined \(r_g \in R_g = R, \ g \in G\) (with almost all \(r_g = 0_R\)) such that

\[
(a_g)_{g \in G} = \sum_{g \in G} \rho_g(r_g) = \sum_{g \in G} r_g g.
\]

In particular, 2.8.5(d) gives \(r_g = a_g\) for all \(g \in G\). So \(\sum_{g \in G} r_g g = (r_g)_{g \in G}\). Note that the converse is also true — the sum over \(G\) of \(r_g g\) uniquely determines the element \((r_g)_{g \in G}\). These last facts will be used extensively below, with \((\Rightarrow)\) used to cite the forward implication and \((\Leftarrow)\) the backward.

(c) We will show that \((\sum_{g \in G} r_g g) + (\sum_{g \in G} s_g g) = \sum_{g \in G} (r_g + s_g) g\). It follows from

\[
\left(\sum_{g \in G} r_g g\right) + \left(\sum_{g \in G} s_g g\right) = (r_g + s_g)_{g \in G} + \sum_{g \in G} g
\]

\[
= (r_g + s_g)_{g \in G} \quad \text{addition in } R[G]\text{ is component-wise}
\]

\[
= \sum_{g \in G} (r_g + s_g) g.
\]

(d) We will show that \((\sum_{g \in G} r_g g) \ast (\sum_{h \in G} s_h h) = \sum_{g, h \in G} (r_g s_h) gh\). Observe

\[
\left(\sum_{g \in G} r_g g\right) \ast \left(\sum_{h \in G} s_h h\right) = (r_g)_{g \in G} \ast (s_h)_{h \in G}
\]

\[
= \left(\sum_{gh=l} r_g s_h\right)_{l \in G}, \quad \text{definition of } \ast
\]

But \(l\) varies through all of \(G\), so for any \(x, y \in G\) we have \(xy = l\) for one of the indexes of the sum. Thus, every possible pair of \(r_x s_y\) appears in the sum, which means

\[
\left(\sum_{gh=l} r_g s_h\right)_{l \in G} = \sum_{g, h \in G} (r_g s_h) gh.
\]

(e) If \(R\) and \(G\) have identities \(1_R\) and \(e_G\), respectively, then \(R[G]\) has an identity: namely, \(1_R e_G\).

We know from part (b) that \(1_R e_G = \rho_{e_G}(1_R)\), which is a tuple \((1_g)_{g \in G}\) such that \(1_g = 0_R\) for all \(g \in G\) except \(1_G = 1_R\). Let \((a_g)_{g \in G} \in R[G]\). Then

\[
(a_g)_{g \in G} \ast (1_g)_{g \in G} = \left(\sum_{hl=g} a_h 1_l\right)_{g \in G}, \quad \text{definition of } \ast
\]

Now, let us consider the sum on the right-hand side. For a particular \(g \in G\), when \(h \neq g\) the product of \(a_h\) and \(1_l\) will be \(a_h 0_R = 0_R\). However, when \(h = g\) we will have \(l = e_G\) and \(1_l = 1_R\). Thus \(a_h 1_R = a_h\) in this case. So the \(g^{th}\) component will be \(0_R + \ldots + 0_R + a_h + 0_R + \ldots = a_h\). Since this occurs for each \(g \in G\), we have

\[
\left(\sum_{hl=g} a_h 1_l\right)_{g \in G} = \left(\sum_{h=g} a_h\right)_{g \in G} = (a_g)_{g \in G}.
\]

We see that \(1_R e_G = (1_g)_{g \in G}\) is an identity in \(R[G]\) because also

\[
(1_g)_{g \in G} \ast (a_g)_{g \in G} = \left(\sum_{hl=g} 1_h a_l\right)_{g \in G}
\]

\[
= \left(\sum_{h=g} a_h\right)_{g \in G}
\]

\[
= (a_g)_{g \in G}.
\]
(f) Suppose $R$ and $G$ are both commutative. Then $R[G]$ is also commutative. Let $(a_g)_{g \in G}$ and $(b_g)_{g \in G}$ be elements of $R[G]$. Then

$$
(a_g)_{g \in G} \ast (b_g)_{g \in G} = \sum_{hl=g} a_h b_l \quad \text{definition of } \\
= \sum_{hl=g} b_l a_h \quad R \text{ is commutative} \\
= \sum_{lh=g} b_l a_h \quad G \text{ is commutative} \\
= (b_g)_{g \in G} \ast (a_g)_{g \in G}. \quad \text{definition of } 
$$

It is clear from this that $R[G]$ is commutative.

2

**Proposition.** Let $(R, +, \cdot)$ be a non-zero finite ring. If $R$ has no left zero divisors, then $R$ is a division ring.

**Proof.** We assume $R$ is non-zero and finite. So $(R, \cdot)$ is a non-empty finite semigroup. We also assume $R$ has no left zero divisors. Then by 3.1.11, the Left and Right Cancellation Laws hold in $R$. This means that for any non-zero $a, b, c \in R$,

$$
ab = ac \implies b = c, \\
ba = ca \implies b = c. 
$$

We have satisfied the hypotheses of Problem 5 from Homework 1, and can therefore conclude that $(R, \cdot)$ is a group. But if $(R, \cdot)$ is a group then each element of $R$ has a multiplicative inverse. Thus, $R$ is a division ring, by definition. (Note that $1_R \neq 0_R$ because $R$ is non-zero.) □

3

**Proposition.** $\mathbb{C}[Z_4] \cong \mathbb{C}[Z_2 \oplus Z_2]$.

**Proof.** Assume the order of the indices of $\mathbb{C}[Z_4]$ are $(0, 1, 2, 3)$ and the indices of $\mathbb{C}[Z_2 \oplus Z_2]$ are $((0,0), (0,1), (1,0), (1,1))$. **NOTATION:** for $c \in \mathbb{C}$, we will often write $c$ in place of $(c,0,0,0)$.

Let

$$
x = (0, 1, 0, 0) \in \mathbb{C}[Z_4], \\
y = (0, 1 + i, 1 - i, 0) \in \mathbb{C}[Z_2 \oplus Z_2].
$$

It is readily verifiable that $x^4 = (1,0,0,0) \in \mathbb{C}[Z_4]$ and $y^4 = (1,0,0,0) \in \mathbb{C}[Z_2 \oplus Z_2]$. More specifically, $x$ and $y$ each have order 4 because $x^2 \neq x^4$ and $y^2 \neq y^4$. Define

$$
\phi : (x, c | c \in \mathbb{C}) \longrightarrow (y, c | c \in \mathbb{C}), \quad c_1 + c_2 x + c_3 y^2 + c_4 x^3 \longrightarrow c_1 + c_2 y + c_3 y^2 + c_4 y^3
$$

where $c_i \in \mathbb{C}$ for $1 \leq i \leq 4$. For $c_i, d_i \in \mathbb{C}, 1 \leq i \leq 4$, we have

$$
\phi((c_1 + c_2 x + c_3 x^2 + c_4 x^3) + (d_1 + d_2 x + d_3 x^2 + d_4 x^3)) = \phi((c_1 + d_1) + (c_2 + d_2)x + (c_3 + d_3)x^2 + (c_4 + d_4)x^3) \\
= (c_1 + d_1) + (c_2 + d_2)y + (c_3 + d_3)y^2 + (c_4 + d_4)y^3 \\
= c_1 + c_2 y + c_3 y^2 + c_4 y^3 + d_1 + d_2 y + d_3 y^2 + d_4 y^3 \\
= \phi(c_1 + c_2 x + c_3 x^2 + c_4 x^3) \phi(d_1 + d_2 x + d_3 x^2 + d_4 x^3).
$$

So $\phi$ is a homomorphism under addition.
Note that multiplication in \((x, c \mid c \in \mathbb{C})\) is essentially multiplication in \(\mathbb{C}[x]\) and multiplication in \((y, c \mid c \in \mathbb{C})\) is essentially multiplication in \(\mathbb{C}[y]\) (which is distinct from multiplication in \(\mathbb{C}[\mathbb{Z}_2 \oplus \mathbb{Z}_2]\)). Thus, we also have

\[
\phi((c_1 + c_2 x + c_3 x^2 + c_4 x^3)(d_1 + d_2 x + d_3 x^2 + d_4 x^3)) = \phi((c_1 d_1 + c_2 d_2 + c_3 d_3 + c_4 d_4) + (c_1 d_2 + c_2 d_1 + c_3 d_4 + c_4 d_3)x + (c_1 d_3 + c_2 d_2 + c_3 d_1 + c_4 d_4)x^2 + (c_1 d_4 + c_2 d_3 + c_3 d_2 + c_4 d_1)x^3) \\
= (c_1 d_1 + c_2 d_2 + c_3 d_3 + c_4 d_4) + (c_1 d_2 + c_2 d_1 + c_3 d_4 + c_4 d_3)y + (c_1 d_3 + c_2 d_2 + c_3 d_1 + c_4 d_4)y^2 + (c_1 d_4 + c_2 d_3 + c_3 d_2 + c_4 d_1)y^3 \\
= \phi(c_1 + c_2 x + c_3 x^2 + c_4 x^3)(d_1 + d_2 x + d_3 x^2 + d_4 x^3).
\]

So \(\phi\) is a homomorphism under multiplication.

Let \(c_1 + c_2 y + c_3 y^2 + c_4 y^3\) be an element from \((y, c \mid c \in \mathbb{C})\). Since \(c_1 + c_2 y + c_3 x^2 + c_4 x^3\) is an element in \((x, c \mid c \in \mathbb{C})\) and \(\phi(c_1 + c_2 x + c_3 x^2 + c_4 x^3) = c_1 + c_2 y + c_3 y^2 + c_4 y^3\), we know that \(\phi\) is surjective. Now, suppose \(c_1 + c_2 y + c_3 y^2 + c_4 y^3 = d_1 + d_2 y + d_3 y^2 + d_4 y^3\) in \((y, c \mid c \in \mathbb{C})\). This means \(c_i = d_i\) for \(1 \leq i \leq 4\). But the respective preimages under \(\phi\) are \(c_1 + c_2 x + c_3 x^2 + c_4 x^3\) and \(d_1 + d_2 x + d_3 x^2 + d_4 x^3\), which are obviously equal since \(c_i = d_i, 1 \leq i \leq 4\). Thus, \(\phi\) is injective.

We have now proven that \(\phi\) is an isomorphism between \((x, c \mid c \in \mathbb{C})\) and \((y, c \mid c \in \mathbb{C})\). We will use this to determine an isomorphism between \(\mathbb{C}[\mathbb{Z}_4]\) and \(\mathbb{C}[\mathbb{Z}_2 \oplus \mathbb{Z}_2]\).

Recall that \(x = (0, 1, 0, 0) \in \mathbb{C}[\mathbb{Z}_4]\). By the definition of group ring multiplication, we find

\[
x = (0, 1, 0, 0) \\
x^2 = (0, 0, 1, 0) \\
x^3 = (0, 0, 0, 1) \\
x^4 = (1, 0, 0, 0).
\]

It is necessarily the case that \((x, c \mid c \in \mathbb{C}) \subset \mathbb{C}[\mathbb{Z}_4]\). Let \((c_1, c_2, c_3, c_4) \subset \mathbb{C}[\mathbb{Z}_4]\). By the powers of \(x\) above, and part (b) of Problem 1, we know \((c_1, c_2, c_3, c_4) = c_1 x^4 + c_2 x + c_3 x^2 + c_4 x^3 \in (x, c \mid c \in \mathbb{C})\). Hence, \(\mathbb{C}[\mathbb{Z}_4] \subset (x, c \mid c \in \mathbb{C})\) and indeed \(\mathbb{C}[\mathbb{Z}_4] = (x, c \mid c \in \mathbb{C})\).

In \(\mathbb{C}[\mathbb{Z}_2 \oplus \mathbb{Z}_2]\), we have

\[
y = (0, \frac{1+i}{2}, \frac{1-i}{2}, 0) \\
y^2 = (0, 0, 0, 1) \\
y^3 = (0, \frac{1-i}{2}, \frac{1+i}{2}, 0) \\
y^4 = (1, 0, 0, 0).
\]

Calculations show that

\[
w := iy + \left(\frac{-1-i}{2}\right)(y + y^3) = (0, 1, 0, 0) \\
z := iy + \left(\frac{-1+i}{2}\right)(y + y^3) = (0, 0, 1, 0).
\]

Note that \(w, z \in (y, c \mid c \in \mathbb{C})\) because they are combinations of complex numbers and powers of \(y\). Now, it is obvious that \((y, c \mid c \in \mathbb{C}) \subset \mathbb{C}[\mathbb{Z}_2 \oplus \mathbb{Z}_2]\). Let \((c_1, c_2, c_3, c_4) \subset \mathbb{C}[\mathbb{Z}_2 \oplus \mathbb{Z}_2]\). It follows from the determinations above and Problem 1(b) that \((c_1, c_2, c_3, c_4) = c_1 y^4 + c_2 w + c_3 z + c_4 y^2\). Hence, \((c_1, c_2, c_3, c_4) \subset (y, c \mid c \in \mathbb{C})\) and \(\mathbb{C}[\mathbb{Z}_2 \oplus \mathbb{Z}_2] \subset (y, c \mid c \in \mathbb{C})\). Therefore, \(\mathbb{C}[\mathbb{Z}_2 \oplus \mathbb{Z}_2] = (y, c \mid c \in \mathbb{C})\).

Define

\[
\overline{\phi} : \mathbb{C}[\mathbb{Z}_4] \rightarrow \mathbb{C}[\mathbb{Z}_2 \oplus \mathbb{Z}_2], (c_1, c_2, c_3, c_4) \mapsto \phi(c_1 + c_2 x + c_3 x^2 + c_4 x^3).
\]

This is well-defined because a tuple from \(\mathbb{C}[\mathbb{Z}_4]\) uniquely determines an element of \((x, c \mid c \in \mathbb{C})\) and the image of an element under \(\phi\) is unique. Moreover, \(\overline{\phi}\) is an isomorphism because \(\phi\) is an isomorphism and \(\mathbb{C}[\mathbb{Z}_4] = (x, c \mid c \in \mathbb{C}), \mathbb{C}[\mathbb{Z}_2 \oplus \mathbb{Z}_2] = (y, c \mid c \in \mathbb{C})\). \(\Box\)
Let $K$ be a field and $G$ a finite group. We will determine

$$\text{Z}(K[G]) = \{(s_g)_{g \in G} \mid (s_g)_{g \in G} (r_g)_{g \in G} = (r_g)_{g \in G} (s_g)_{g \in G} \text{ for all } (r_g)_{g \in G} \in K[G]\}.$$ 

By the definition of a field, $K$ is commutative and all non-zero elements are invertible. If $G$ is abelian, then $K[G]$ is commutative by Problem 1(f) and $\text{Z}(K[G]) = K[G]$. So suppose $G$ is not abelian. Recall from Problem 6(f) of Homework 2 that $\text{Z}(G) = \{h \in G \mid hg = gh \text{ for all } g \in G\}$, and note that $\text{Z}(G) \neq G$ because $G$ is not abelian. CLAIM: $\text{Z}(K[G]) = A$ where $A$ is the set of all $(a_g)_{g \in G}$ such that $a_h = a_k$ whenever $h$ and $k$ are conjugate in $G$. (Note that when $g \in Z(G)$ the conjugacy class of $g$ is $\{g\}$.) Thus, there is really no stipulation on $a_g$ for $g \in Z(G)$. Our strategy will be to show that $A \subseteq \text{Z}(K[G])$, and then to show that the complement of $A$ is a subset of the complement of $\text{Z}(K[G])$. This will prove the claim.

Let $(a_g)_{g \in G} \in A$. This means $a_h = a_k$ whenever $h$ and $k$ are conjugate. Let $(r_g)_{g \in K[G]}$ and pick $g \in G$. We must show that $((a_g)_{g \in G} (r_g)_{g \in G})_g$ is equal to $((r_g)_{g \in G} (a_g)_{g \in G})_g$. By the definition of group ring multiplication,

$$((a_g)_{g \in G} (r_g)_{g \in G})_g = \sum_{(h,l) \in G \times G} a_h \cdot r_l, \quad (1)$$

$$((r_g)_{g \in G} (a_g)_{g \in G})_g = \sum_{(h,l) \in G \times G} r_h \cdot a_l. \quad (2)$$

Consider some summand $a_h r_l$ from (1). We have $h$ and $l^{-1} h l$ conjugate in $G$ because $h = l(l^{-1} h l)$. Thus, $a_h = a_{l^{-1} h l}$ by the definition of $A$. Now, $h$ and $l$ are paired indices from (1), so $hl = g$. Furthermore, $l(l^{-1} h l) = (l^{-1}) h l = h$. This means $l$ and $l^{-1} h l$ are paired indices and $r_l a_{l^{-1} h l}$ must appear in (2). But $r_l = r_l$ and $a_h = a_{l^{-1} h l}$, and since $K$ is commutative, we have $a_h r_l = r_l a_{l^{-1} h l}$. This means every summand from (1) also appears in (2) and thus (1)=(2). Since $g$ was an arbitrary coordinate, it follows that every coordinate is equal and in fact

$$(a_g)_{g \in G} (r_g)_{g \in G} = (r_g)_{g \in G} (a_g)_{g \in G}.$$ 

Therefore, $(a_g)_{g \in G} \in \text{Z}(K[G])$ and $A \subseteq \text{Z}(K[G])$.

Let $(a_g)_{g \in G}$ be such that $a_h \neq a_k$ for some $h$ and $k$ conjugate in $G$; that is, $(a_g)_{g \in G} \notin A$. We must show that $(a_g)_{g \in G}$ does not commute with some element of $K[G]$; that is, $(a_g)_{g \in G} \notin \text{Z}(K[G])$. We are assuming $h$ and $k$ are distinct, which means the conjugacy class of $h$ contains at least two elements, and so $h \notin Z(G)$. Thus, there exists $l_h \in G$ such that $hl_h \neq l_h h$. Put $g_h = hl_h$.

Consider $(r_g)_{g \in G} \in K[G]$ where

$$r_g = \begin{cases} a_k & g = h \\ a_g & g \neq h. \end{cases}$$

In other words, $(r_g)_{g \in G}$ is identical to $(a_g)_{g \in G}$ except that $r_h = r_k = a_k$. Now we look at

$$((a_g)_{g \in G} (r_g)_{g \in G})_{g_h} = \sum_{(h,l) \in G \times G} a_h \cdot r_l, \quad (3)$$

$$((r_g)_{g \in G} (a_g)_{g \in G})_{g_h} = \sum_{(h,l) \in G \times G} r_h \cdot a_l. \quad (4)$$

Let $a_h r_l$ be a summand from (3) with $h_i \neq h$, $l_i \neq l$. Then $r_h a_l$ necessarily appears as a summand in (4). But $a_h = r_h$, and $a_i = r_i$ by the construction of $(r_g)_{g \in G}$. Hence, $a_h r_l = r_h a_l$. So we see that most of the summands from (3) and (4) are equal. However, consider $a_h r_{l_h}$ from (3) and $r_{l_h} a_{l_h}$ from (4). We claim that $a_h r_{l_h} \neq r_{l_h} a_{l_h}$.
By construction, \( r_l = a_l \), so we may reframe the question in terms of \( a_h a_l \) and \( r_h a_l \). Suppose the claim is false and \( a_h a_l = r_h a_l \). Since \( K \) is a field, \( a_l^{-1} \) exists and we have
\[
a_h a_l a_l^{-1} = r_h a_l a_l^{-1}.
\]
But this implies \( a_h = r_h \) which is a contradiction because \( r_h = a_k \) and \( a_h \neq a_k \) by assumption. Therefore, the claim is true and \( a_h r_l \neq r_h a_l \). Since all the other summands are equal, this single unequal pair of summands means
\[
((a_g)_{g \in G} (r_g)_{g \in G})_g \neq ((r_g)_{g \in G} (a_g)_{g \in G})_g,
\]
and consequently
\[
(a_g)_{g \in G} (r_g)_{g \in G} \neq (r_g)_{g \in G} (a_g)_{g \in G}.
\]
Since \( (a_g)_{g \in G} \) does not commute with all elements of \( K[G] \), it follows that \( (a_g)_{g \in G} \not\in Z(K[G]) \).

Having proven both inclusions, we know \( Z(K[G]) = A \), where \( A \) is the set of all \( (a_g)_{g \in G} \) such that \( a_h = a_k \) whenever \( h \) and \( k \) are conjugate in \( G \).

5

**Proposition.** Let \( R \) be a commutative ring and let \( I \) be the set of nilpotent elements in \( R \). Then
(a) \( I \) is an ideal in \( R \), and
(b) \( R/I \) has no non-zero nilpotent elements.

**Proof.** (a) Recall from the definition of nilpotent that \( a \in I \) if \( a^n = 0_R \) for some \( n \in \mathbb{Z}^+ \). Let \( r \in R \). We must show that \( rI \subseteq I \). So we choose \( ri \in rI \) and consider \( (ri)^n \) where \( n \) is such that \( ri^n = 0_R \). Then, since \( R \) is commutative,
\[
(ri)^n = (ri)(ri) \ldots (ri) = \underbrace{rr \ldots r}_{n \text{-times}} \underbrace{ii \ldots i}_{n \text{-times}} = r^n i^n.
\]
Furthermore, \( (ri)^n = r^n 0_R = 0_R \) because \( i^n = 0_R \) by the choice of \( n \). Thus, by the definition of a nilpotent element and the definition of \( I \), \( ri \in I \). This means \( rI \subseteq I \) and \( I \) is an ideal in \( R \).

(b) We know from group theory (2.5.5(c)) that \( I \) is the identity element of \( R/I \) with respect to addition, so \( I \) is called the “zero element” of \( R/I \). Let \( A \in R/I \) with \( A \neq I \). We must show that \( A^n \neq I \) for any \( n \in \mathbb{Z}^+ \).

Note that congruence modulo \( I \) is an equivalence relation, so \( R/I \) is a partition of \( R \) and \( A \) and \( I \) are necessarily disjoint. Since all nilpotent elements are in \( I \), there are no nilpotent elements of \( R \) in \( A \). Now, choose \( n \in \mathbb{Z}^+ \). Then by 3.2.7(c),
\[
A^n = \langle a_1 a_2 \ldots a_n \mid a_i \in A, 1 \leq i \leq n \rangle.
\]
Choose \( a \in A \). Then clearly \( a^n \in A^n \). Suppose \( a^n \in I \), that is, \( a^n \) is nilpotent. Then \( (a^n)^m = 0_R \) for some \( m \in \mathbb{Z}^+ \). But this implies \( a^{nm} = 0_R \) and we noted that \( a \) is not nilpotent—a contradiction. Therefore, \( a^n \) is not nilpotent and \( a^n \not\in I \). Thus, an element of \( A^n \) is not in \( I \) and so \( A^n \neq I \). This means \( A \) is not a nilpotent element of \( R/I \). \( \Box \)
Let $R$ be a ring with identity and denote $1_R$ by 1 and $0_R$ by 0. Let $S = M_{nn}(R)$ and let $I$ be a particular ideal in $S$. For $A \in S$, let $A_{ij}$ be the entry of row $i$, column $j$ in $A$. Let $J = \{ A_{11} \mid A \in I \}$. (See attachment for explicit matrices throughout.)

(a) We will show that $J$ is an ideal in $R$; that is, $rJ \subseteq J$ for any $r \in R$. Choose $r \in R$ and $j \in J$. It will suffice to show that $rj \in J$.

By the definition of $J$, there is $A \in I$ with $A_{11} = j$. Let $M$ be the matrix in $S$ with

$$M_{ij} = \begin{cases} r & i = j = 1 \\ 0 & i \neq 1 \text{ or } j \neq 1. \end{cases}$$

Consider $MA$. We see that $(MA)_{11} = rj + 0 + 0 + \ldots + 0 = rj$. Since $I$ is an ideal and $A \in I$, we have $MA \in I$. Hence, $rj$ is the entry in row 1, column 1 of an element of $I$. It follows that $rj \in J$. So $J$ is an ideal in $R$.

(b) Let $E^{rs} \in S$ be the matrix with 1 in row $r$, column $s$ and 0 everywhere else. Let $A \in S$ and $1 \leq p, q, r, s \leq n$. We will show that $E^{pr}AE^{sq} = A_{rs}E^{pq}$.

First, consider $AE^{sq}$. If $j \neq q$ then column $j$ of $E^{sq}$ is entirely 0, so column $j$ of $AE^{sq}$ is composed of $A_{ij}0 + A_{j2}0 + \ldots + A_{jn}0 = 0$ for each row $1 \leq i \leq n$. In other words, column $j$ of $AE^{sq}$ is entirely 0 if $j \neq q$. Now, for column $q$ in $AE^{sq}$ we have

$$A_{11}0 + A_{21}0 + \ldots + A_{1n}1 + \ldots + A_{in}0 = A_{is}$$

for each row $1 \leq i \leq n$. In other words, column $s$ of $A$ is column $q$ of $AE^{sq}$ and $AE^{sq}$ is 0 everywhere else.

Define $B = AE^{sq}$. We must multiply $E^{pr}B$. If $i \neq p$ then row $i$ of $E^{pr}$ is entirely 0, so row $i$ of $E^{pr}B$ is composed of $0B_{1j} + 0B_{2j} + \ldots + 0B_{nj} = 0$ for each column $1 \leq j \leq n$. In other words, row $i$ of $E^{pr}B$ is entirely 0 if $i \neq p$. Now, for row $p$ in $E^{pr}B$ we have

$$0B_{1j} + 0B_{2j} + \ldots + 1B_{rj} + \ldots + 0B_{nj} = 1B_{rj}$$

for each column $1 \leq j \leq n$. But $B_{rj} = 0$ when $j \neq q$, so row $p$ is entirely 0 except in column $q$. When $j = q$, $B_{rq} = A_{rs}$ because of our determination of $B$ above. Thus we have row $p$, column $q$ of $E^{pr}B$ equal to $A_{rs}$. This proves that

$$E^{pr}A^{sq} = E^{pr}B = A_{rs}E^{pq}.$$  

(c) Let $A \in I$ and $1 \leq i, j \leq n$. We will show that $A_{ij}$ is an element of $J$.

Since $A \in I$, $A_{11} \in J$ by the definition of $J$. Since $I$ is an ideal, $AE^{11} \in I$ and also $E^{11}(AE^{11}) \in I$. This means the entry in row 1, column 1 of $E^{11}AE^{11}$ is in $J$. But we showed in part (b) that this product of matrices takes $A_{ij}$ and places it in row 1, column 1 in the product matrix (using 1 and 1 in place of $p$ and $q$). Therefore, $A_{ij}$ is in row 1, column 1 of $E^{11}AE^{11}$. It follows that $A_{ij} \in J$.

(d) We will show that $I$ equals the set of $n \times n$ matrices with coefficients in $J$.

Let $A \in I$. We showed in part (c) that every entry of $A$ is an element of $J$. Thus, $A \in M_{nn}(J)$ and we have $I \subseteq M_{nn}(J)$. Let $B \in M_{nn}(J)$. So every entry in $B$ is from $J$, which means by the definition of $J$ that for all $1 \leq i, j \leq n$ there exists an $A^{ij} \in I$ such that $A_{ij}^{11} = B_{ij}$. Note that $MA^{ij} \in I$ and $A^{ij}M \in I$ for all $M \in S$ because $I$ is an ideal. And since $I$ is a subring, it is closed under addition. This will allow us to construct the matrix $B$ while remaining in $I$, which will prove that $B \in I$ and $M_{nn}(J) \subseteq I$.

Consider

$$B^* = \sum_{1 \leq i, j \leq n} E^{11}A^{ij}E^{1j}.$$  

Each summand is in $I$ because $A^{ij} \in I$ and $I$ is an ideal, so $B^* \in I$. Let us look at row $i$, column $j$ of $B^*$. By part (b), the product $E^{1i}A^{ij}E^{1j}$ takes $A_{11}^{ij}$ and places it in row $i$, column $j$ of $B^*$ (the sum does not alter this fact because the corresponding entries in the other summands are 0). But $A_{11}^{11}$ was defined to be $B_{ij}$. Hence, $B_{ij}^* = B_{ij}$ for all $1 \leq i, j \leq n$ and $B^* = B$. This means $B \in I$ and $M_{nn}(J) \subseteq I$. Therefore, $I = M_{nn}(J)$.  

8
**Proposition.** Let $D$ be a division ring and $n \in \mathbb{Z}^+$. Then $M_{nn}(D)$ is a simple ring.

**Proof.** Let $I$ be an ideal in $S = M_{nn}(D)$ with $I \neq \{0_S\}$, where $0_S$ is the $n \times n$ matrix with all entries $0_D$. We must show that $I$ is necessarily the entire ring $S$.

The fact that $I \neq \{0_S\}$ means there is $A \in I$ with $A_{ij} = a$ for some $1 \leq i, j \leq n$ and $0_D \neq a \in D$. By part (b) of Problem 6, we know that $B = E_{1i}^1A_{ij}^1$ takes $A_{ij} = a$ and puts it in $B_{11}$. All other entries of $B$ are $0_D$. But $A \in I$ and $I$ is an ideal, so $B \in I$. If we define $J = \{A_{11} \mid A \in I\}$, then we see $a = A_{11} = B_{11} \in J$.

Since $D$ is a division ring and $a$ is non-zero, $a^{-1} \in D$. Consider the matrix $C \in S$ with $C_{11} = a^{-1}$ and all other entries $0_D$. Now, $B \in I$ so $CB \in I$. The entry in row 1, column 1 of $CB$ is $(a^{-1}a) + 0_D + 0_D + \ldots + 0_D = 1_D$. This means $1_D \in J$. (It is also obvious that $0_D \in J$ because $0_S A \in I$ and the 11-entry is $0_D$.) We saw in part (d) of Problem 2 that $I = M_{nn}(J)$. Since $1_D, 0_D \in J$, the $n \times n$ identity matrix is necessarily an element of $I$ because all of its entries are from $J$. Let $M$ be any matrix in $S$. Then the product of $M$ and the identity matrix is in $I$ by the definition of an ideal, so $M \in I$. Thus, $S = I$.

It follows that the only ideals of $S$ are the trivial ones, so $S = M_{nn}(D)$ is simple. □