

Extra Credit Problem Set 3 (Solutions); Due Wednesday, May 6, 2009

1. Let G be a group and R be a ring. Consider the set RG as

$$RG = \left\{ \sum_{g \in G} a_g g \mid a_g \in R, \text{ and } a_g = 0 \text{ for all but finitely many } g \in G \right\}$$

of formal finite R -linear combinations of elements of G .

For $f_1 = \sum_{g \in G} a_g g$ and $f_2 = \sum_{g \in G} b_g g$ define

$$f_1 + f_2 := \sum_{g \in G} (a_g + b_g)g,$$

$$f_1 \cdot f_2 := \sum_{g \in G} c_g g,$$

where for every $g \in G$ we have $c_g = \sum_{h \in G} a_h b_{h^{-1}g}$.

Prove that $(RG, +, \cdot)$ is a ring.

[This ring is called the *group ring of G over R* .]

Solution.

We will check a few of the axioms of a ring and leave the rest to the reader. It is easy to see that $(RG, +)$ is an abelian group and that $1 \in G$ is an identity element with respect to multiplication in RG .

Let us check that multiplication in RG is associative.

Let $f_1, f_2, f_3 \in RG$ be arbitrary. Thus $f_1 = \sum_{g \in G} a_g g$ and $f_2 = \sum_{g \in G} b_g g$, $f_3 = \sum_{g \in G} c_g g$ for some $a_g, b_g, c_g \in R$.

We have $f_1 \cdot f_2 := \sum_{g \in G} d_g g$, where for every $g \in G$ we have $d_g = \sum_{h \in G} a_h b_{h^{-1}g}$.

We also have $f_2 \cdot f_3 := \sum_{g \in G} t_g g$, where for every $g \in G$ we have $t_g = \sum_{h \in G} b_h c_{h^{-1}g}$.

Let $f' = (f_1 \cdot f_2) \cdot f_3$. Then $f' = \sum_{g \in G} u_g g$ where for every $g \in G$ we have

$$\begin{aligned} u_g &= \sum_{h \in G} d_h c_{h^{-1}g} = \sum_{h \in G} \left(\sum_{h_1 \in G} a_{h_1} b_{h_1^{-1}h} \right) c_{h^{-1}g} = \\ &= \sum_{h \in G} \sum_{h_1 \in G} a_{h_1} b_{h_1^{-1}h} c_{h^{-1}g} = \sum_{h_1 \in G} \sum_{h \in G} a_{h_1} b_{h_1^{-1}h} c_{h^{-1}g}. \end{aligned}$$

For a fixed $h_1 \in G$ denote $h_2 = h_1^{-1}h$ where $h \in G$. Since for a fixed $h_1 \in G$ the map $G \rightarrow G$, $h \mapsto h_2 = h_1^{-1}h$ is a bijection, as h runs over G , $h_2 = h_1^{-1}h$ also runs over G taking each element of g as its value exactly once. Note also that $h^{-1}g = h_2^{-1}h_1^{-1}g$ and hence $c_{h^{-1}g} = c_{h_2^{-1}h_1^{-1}g}$.

Therefore

$$u_g = \sum_{h_1 \in G} \sum_{h \in G} a_{h_1} b_{h_1^{-1}h} c_{h^{-1}g} = \sum_{h_1 \in G} \sum_{h_2 \in G} a_{h_1} b_{h_2} c_{h_2^{-1}h_1^{-1}g}.$$

Put $f'' = f_1 \cdot (f_2 \cdot f_3)$. Then $f'' = \sum_{g \in G} v_g g$ where for every $g \in G$ we have

$$\begin{aligned} v_g &= \sum_{h_1 \in G} a_{h_1} t_{h_1^{-1}g} = \sum_{h_1 \in G} a_{h_1} \sum_{h_2 \in G} b_{h_2} c_{h_2^{-1}h_1^{-1}g} = \\ &= \sum_{h_1 \in G} \sum_{h_2 \in G} a_{h_1} b_{h_2} c_{h_2^{-1}h_1^{-1}g} = \sum_{h_1 \in G} \sum_{h_2 \in G} a_{h_1} b_{h_2} c_{h_2^{-1}h_1^{-1}g}. \end{aligned}$$

Thus we see that for every $g \in G$ we have $u_g = v_g$. Hence $f' = f''$, that is $(f_1 f_2) f_3 = f_1 (f_2 f_3)$ in RG , as required. Thus we have verified that multiplication in RG is associative.

Let us now check distributivity. Let $f_1, f_2, f_3 \in RG$ be as above. We need to verify that $(f_1 + f_2) f_3 = f_1 f_3 + f_2 f_3$. We have $f_1 + f_2 = \sum_{g \in G} (a_g + b_g) g$ and therefore $(f_1 + f_2) f_3 = \sum_{g \in G} x_g g$ where

$$x_g = \sum_{h \in G} (a_h + b_h) c_{h^{-1}g} = \sum_{h \in G} a_h c_{h^{-1}g} + b_h c_{h^{-1}g}.$$

We also have $f_1 f_3 = \sum_{g \in G} y_g g$ where $y_g = \sum_{h \in G} a_h c_{h^{-1}g}$ and $f_2 f_3 = \sum_{g \in G} z_g g$ where $z_g = \sum_{h \in G} b_h c_{h^{-1}g}$. Hence $f_1 f_3 + f_2 f_3 = \sum_{g \in G} w_g g$ where

$$w_g = \sum_{h \in G} a_h c_{h^{-1}g} + \sum_{h \in G} b_h c_{h^{-1}g} = \sum_{h \in G} a_h c_{h^{-1}g} + b_h c_{h^{-1}g}.$$

Thus we see that $x_g = w_g$ for every $g \in G$ and hence $(f_1 + f_2) f_3 = f_1 f_3 + f_2 f_3$ in RG .

The proof that $f_1 (f_2 + f_3) = f_1 f_2 + f_1 f_3$ is similar and we omit the details.

2. Let G be a finite group and let $p \geq 3$ be a prime such that $p \mid |G|$. Prove that the group ring $\mathbb{Z}_p G$ is not a domain.

Hint: Think about the value of $(g - 1)^p$ in $\mathbb{Z}_p G$ where $g \in G$ and where $1 = e \in G$ is the identity element of G .

Solution.

Since $p \geq 3$ is a prime such that $p \mid |G|$, the First Sylow Subgroup Theorem implies that there exists a cyclic subgroup $\langle a \rangle$ of order p in G . Thus $|a| = p$.

Consider the element $(g - 1)^p \in \mathbb{Z}_p G$. Here $1 \in G$ is the identity element of G . Note that since $p \geq 3$ is a prime, p is odd and hence $(-1)^p = -1$. Then by the Binomial Theorem we have:

$$(a - 1)^p = g^p + \sum_{j=1}^{p-1} \binom{p}{j} a^{p-j} (-1)^j + (-1)^p = g^p + \sum_{j=1}^{p-1} \binom{p}{j} a^{p-j} (-1)^j - 1.$$

Since p is a prime, we know that $p \mid \binom{p}{j}$ for $j = 1, \dots, p - 1$. Hence in \mathbb{Z}_p we have $\binom{p}{j} = 0$ for $j = 1, \dots, p - 1$. Therefore $(a - 1)^p = a^p - 1$ in $\mathbb{Z}_p G$. However, $|a| = p$ and hence $a^p = 1$ in G and $(a - 1)^p = a^p - 1 = 0$ in $\mathbb{Z}_p G$.

Since $|a| = p > 1$, $a \neq 1$ and hence $a - 1 \neq 0$ in $\mathbb{Z}_p G$.

Thus in $\mathbb{Z}_p G$ we have $a - 1 \neq 0$ but

$$(a - 1)^p = \underbrace{(a - 1)(a - 1) \dots (a - 1)}_{p \text{ times}} = 0.$$

Therefore $\mathbb{Z}_p G$ is not a domain.