Homework 9, due Nov 29

You must prove your answer to every question.

Problem 1. (15) Show that in an integral domain with characteristic $p$ we have $(a + b)^p = a^p + b^p$.

Solution. By the binomial theorem, we have

$$(a + b)^p = \binom{p}{0} a^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{p-1} ab^{p-1} + \binom{p}{p} b^p.$$  

On the right-hand side, all terms but the first and the last one have a coefficient of the form $\binom{p}{k}$ where $0 < k < p$. An earlier exercise showed that every coefficient of this form is divisible by $p$, therefore it is 0 in an integral domain of characteristic $p$.

Problem 2 (15). For a finite Abelian group $G$ with the multiplicative notation, and a ring $R$ let $F_1$ be the set of functions $\alpha : G \to R$. We introduce an addition and a multiplication operation on $F_1$ as follows.

$$(\alpha + \beta)(g) = \alpha(g) + \beta(b),$$

$$(\alpha * \beta)(g) = \sum_{h \in G} \alpha(h)\beta(h^{-1}g).$$

Verify that these two operations define the structure of a ring over $F$. [Hint: it may help viewing a function $\alpha(g)$ here as a “formal sum” $\sum_{g \in G} \alpha(g) \cdot g$.]

Solution. We have to check that the ring properties are satisfied. Instead of checking that the addition operation defines a group we point out that this follows from the fact that with respect to addition the set $F_1$ is the direct sum of the additive group of the ring $R$ with itself, as many times as there are elements in the group $G$, indexed by the elementes of $g$: for example if $G = \{ g_1, \ldots, g_n \}$ then this group can be written as $R + \cdots + R$ (n times). The zero is the function assigning 0 to everything.

For multiplication, it helps writing the definition in the following form:

$$(\alpha * \beta)(g) = \sum_{h_1h_2 = g} \alpha(h_1)\beta(h_2). \tag{1}$$

Then easy computation shows that both $(\alpha * \beta * \gamma)(g)$ and $(\alpha * \beta * \gamma)(g)$ are equal to

$$\sum_{h_1h_2h_3 = g} \alpha(h_1)\beta(h_2)\gamma(h_3).$$

Commutativity of multiplication comes from the form (1) whose right-hand side is, due to the commutativity of the group $G$ and the multiplication in $R$, symmetric in $\alpha$ and $\beta$.

For the distributivity property:

$$((\alpha + \beta) * \gamma)(g) = \sum_{h_1h_2 = g} (\alpha + \beta)(h_1)\gamma(h_2) = \sum_{h_1h_2 = g} (\alpha(h_1) + \beta(h_1))\gamma(h_2) = \sum_{h_1h_2 = g} \alpha(h_1)\gamma(h_2) + \beta(h_1)\gamma(h_2) = \sum_{h_1h_2 = g} \alpha(h_1)\gamma(h_2) + \sum_{h_1h_2 = g} \beta(h_1)\gamma(h_2) = (\alpha * \gamma)(g) + (\beta * \gamma)(g).$$

The unity is the function $\varepsilon$ assigning 1 to $1_G$ and 0 to everything else. Indeed,

$$(\varepsilon * \alpha)(g) = \sum_{h} \varepsilon(h)\alpha(gh^{-1}) = \varepsilon(1_G)\alpha(g1_G^{-1}) = \alpha(g).$$