Solutions to tutorial questions from October 4, 2012

1. (**a**) Each homomorphism takes 0 to 0, so we should just determine possible values of $\varphi(\overline{1})$. Since the target is $\mathbb{Z}/2\mathbb{Z}$, the possible values are $\overline{0}$ and $\overline{1}$. In fact, both are fine: for $\varphi(\overline{1}) = \varphi(\overline{0}) = 0$ the four required properties reduce to $0+0=0$, $0\cdot 0 = 0$, $-0 = 0$, $0 = 0$, and for $\varphi(\overline{1}) = \overline{1}$ and $\varphi(\overline{0}) = \overline{0}$ the four required properties reduce to $a+b = a+b$, $ab = ab$, $-a = -a$, $0 = 0$.

(**b**) If we start as above, we see that we only need to define $\varphi(\overline{1})$. Since $\overline{1}+\overline{1} = \overline{2} = \overline{0}$ in $\mathbb{Z}/2\mathbb{Z}$, we want $\varphi(\overline{1})+\varphi(\overline{1}) = \overline{0}$ to hold. But in $\mathbb{Z}/3\mathbb{Z}$ we have $\varphi(\overline{1})+\varphi(\overline{1}) = 2\varphi(\overline{1}) = -\varphi(\overline{1})$, and we conclude that $\varphi(\overline{1}) = 0$. Therefore, in this case the only map which is a homomorphism sends all elements to zero.

2. (**a**) As suggested in the hint, we consider the map that takes the class $\overline{n} \in \mathbb{Z}/(ab)\mathbb{Z}$ to the pair $(\overline{n \bmod a}, \overline{n \bmod b}) \in \mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$. This map is manifestly a group homomorphism. Indeed,

$$\begin{aligned}(\overline{(n_1+n_2) \bmod a}, \overline{(n_1+n_2) \bmod b}) = \\ = (\overline{n_1 \bmod a} + \overline{n_2 \bmod a}, \overline{n_1 \bmod b} + \overline{n_2 \bmod a}) = \\ = (\overline{n_1 \bmod a}, \overline{n_1 \bmod b}) + (\overline{n_2 \bmod a}, \overline{n_2 \bmod b}),\end{aligned}$$

and the same for negatives (and of course, the image of zero is zero). To check that this map is an isomorphism, it is sufficient to check that it is a bijection. Our sets consist of the same number of elements (ab), so it is enough to check that this map is injective. If it is not, we have

$$(\overline{n \bmod a}, \overline{n \bmod b}) = (\overline{m \bmod a}, \overline{m \bmod b})$$

for some $\overline{n} \neq \overline{m} \in \mathbb{Z}/(ab)\mathbb{Z}$. But that implies that $(\overline{(n-m) \bmod a}, \overline{(n-m) \bmod b}) = (0,0)$, which in turn means that $n-m$ is divisible by a and by b. Consequently, $n-m$ is divisible by ab (here we use the coprimality assumption!), which is impossible if n and m are different remainders modulo ab.

(**b**) Since the remainder of the product is equal to the product of remainders, the map we discussed is a ring homomorphism, and we already checked that it is a bijection, so the statement follows.

3. By the subring test from class, we need to check that these sets are closed under differences and products. The statement about differences is clear. For products, note that

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay+bz \\ 0 & cz \end{pmatrix}$$

and

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

so the statement follows.

Optional question: in fact the problem was badly worded, and there are no other bijections. Indeed, assume that $\varphi(\overline{1}) = \overline{r}$. Then

$$\varphi(\overline{a}) = \varphi(\underbrace{\overline{1}+\ldots+\overline{1}}_{a \text{ times}}) = \underbrace{\overline{r}+\ldots+\overline{r}}_{a \text{ times}} = \overline{ar},$$

so if we know $\varphi(\overline{1})$, we know all $\varphi(\overline{a})$ just from the Abelian group structure. However, multiplication imposes additional constraints: since we have $\overline{1} \cdot \overline{a} = \overline{a}$ for all $\overline{a}$, this forces $\overline{r} \cdot \varphi(\overline{a}) = \varphi(\overline{1}) \cdot \varphi(\overline{a}) = \varphi(\overline{a})$ for all $\overline{a}$. If we assume that φ is a bijection, we conclude that $\overline{r} \cdot \overline{b} = \overline{b}$ for all $\overline{b}$, so because a unit element is at most unique, we must have $\overline{r} = \overline{1}$ and hence $\varphi(\overline{k}) = \overline{k}$ for all $\overline{k}$.