**Homework 7, due Nov 15**

You must prove your answer to every question.

**Problem 1** (Exercise 8.5 of Shoup). (10) Let $G_1$ and $G_2$ be Abelian groups, let $H$ be a subgroup of $G_1 \times G_2$. Let

$$H_1 = \{ h \in G_1 : \exists g \in G_2 \ (h, g) \in H \}.$$  

Show that $H_1$ is a subgroup of $G_1$.

**Solution.** We have to show that if $a, b \in H_1$ then so is $a - b$. So, assume $a, b \in H_1$, then there exist $a', b'$ such that $(a, a') \in H$ and $(b, b') \in H$. Then $(a - b, a' - b') \in H$ and therefore $a - b \in H_1$.

**Problem 2** (Exercise 8.6 of Shoup). (10) Give an example of specific Abelian groups $G_1, G_2$ along with a subgroup $H$ of $G_1 \times G_2$ such that $H$ cannot be written as $H_1 \times H_2$, where $H_1$ is a subgroup of $G_1$ and $H_2$ is a subgroup of $G_2$.

**Solution.** Let $G = G_1 = G_2$ be any group of order larger than 1, and let $H = \{ (g, g) : g \in G \}$. It is easy to check that $H$ is a subgroup of $G_1 \times G_2$. Its projection into $G_1$ (the group $H_1$ defined in the previous exercise) is the whole group $G_1$, and its projection onto $G_2$ is the whole group $G_2$. Therefore if it was a product it would be equal to the whole group $G_1 \times G_2$. But $|G_1 \times G_2| = |G|^2$, while $|H| = |G| < |G|^2$.

**Problem 3.** (15) We have seen in class that $m\mathbb{Z} \cong \mathbb{Z}$, and $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$. Show that, on the other hand, $\mathbb{Z}_m \times \mathbb{Z} \not\cong \mathbb{Z}$.

**Solution.** The group $\mathbb{Z}$ has no elements different from 0 that have finite order. On the other hand, in $\mathbb{Z}_m \times \mathbb{Z}$, the element $(1, 0)$ has order $m$. So the two groups cannot be isomorphic.

**Problem 4** (Exercise 8.16 of Shoup). (15) Show that if $G = G_1 \times G_2$ for Abelian groups $G_1, G_2$, and $H_1$ is a subgroup of $G_1$ and $H_2$ is a subgroup of $G_2$ then $G/H_1 \times H_2 \cong G_1/H_1 \times G_2/H_2$.

**Solution.** Let us define the map $\rho : G \to G_1/H_1 \times G_2/H_2$ by $(g_1, g_2) \mapsto (g_1 + H_1, g_2 + H_2)$. It is easy to check that this map is a homomorphism. It is obviously surjective, any element of the form $(g_1 + H_1, g_2 + H_2)$ occurs as the image of $\rho$. We must show that its kernel is $H_1 \times H_2$. The kernel consists of the pairs $(g_1, g_2)$ such that $(g_1 + H_1, g_2 + H_2) = (H_1, H_2)$. Now $g_1 + H_1 = H_1$ if and only if $g_1 \in H_1$, and similarly for $g_2$. Therefore the kernel is the set of pairs $(g_1, g_2)$ with $g_1 \in H_1, g_2 \in H_2$, which is exactly $H_1 \times H_2$.

**Problem 5.** (10) An isomorphism of a group $G$ into itself is called an automorphism. Show that the group $\mathbb{Z}_m$ has exactly $\phi(m)$ different automorphisms.

**Solution.** For $g \in G = \mathbb{Z}_m$ let $\langle g \rangle$ be the smallest nonnegative residue in $\mathbb{Z}$ in the residue class of $g$. Then it is easy to check that for each element $g$ of $\mathbb{Z}_m$ we have $g = \langle g \rangle \cdot [1]$, where $[1]$ the residue class of 1.

It is easy to check that for every element $a \in \mathbb{Z}_m$, the mapping $\rho_a$ defined by $x \mapsto \langle a \rangle \cdot x$ is a homomorphism. It is easy to check that its kernel is 0 (and therefore it is an automorphism) if and only if $a \in \mathbb{Z}_m^\ast$.

It remains to show that every automorphism is of this form. Let $\eta$ be an automorphism of $\mathbb{Z}_m$. Recall that each element of $\mathbb{Z}_m$ can be written in the form $n \cdot [1]$ for some integer $n$. Then, we have

$$\eta(n \cdot [1]) = n \cdot \eta([1]) = n \cdot \langle \eta([1]) \rangle \cdot [1] = \langle \eta([1]) \rangle \cdot (n \cdot [1]).$$

Therefore $\eta = \rho_{\eta([1])}$. 