Midterm

Justify all your answers completely (Or with a proof or with a counter example) unless mentioned differently. No step should be a mystery or bring a question. The grader cannot be expected to work his way through a sprawling mess of identities presented without a coherent narrative through line. If he can't make sense of it in finite time you could loose serious points. Coherent, readable exposition of your work is half the job in mathematics. You will loose serious points if your exposition is messy, incomplete, uses mathematical symbols not adapted...

Problem :

In this problem, we consider $G = \mathbb{Z}/12\mathbb{Z}$.

1. Prove that $12\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$. Give a cyclic generator of $12\mathbb{Z}$ and compute its order. Justify.

2. Let $\pi : \mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ be the quotient map.

   (a) For $k \in \mathbb{Z}$, how is defined $\pi(k)$?

   (b) Prove π is a homomorphism.

   (c) Is π surjective (onto G) ? Justify your answer.

   (d) Give the definition of the kernel of π. Compute it. Is π one-to-one (injective) ? Justify.

3. (a) Prove that G is cyclic, give a cyclic generator, prove it is a cyclic generator and compute its order.

   (b) What is the order of $[2]$ in G ? Describe the subgroup generated by $[2]$ and give its order.

   (c) What is the order of $[5]$ in G ? Describe the subgroup generated by $[5]$ and give its order.

   (d) What are the possible orders for the subgroups of G ? Justify your answer.

   (e) How many subgroups G has ? Give the list of all the subgroups of G and describe them explicitly.

4. (a) Give the definition of the set of units U_{12} of G.

   (b) Give the list of the units of G.

   (c) What is the order of U_{12} ?

   (d) Use the extended euclidean algorithm, to compute the multiplicative inverse of $[5]$ and $[7]$ in U_{12},

   (e) What is the order of $[5]$ in U_{12} ? Describe the subgroup generated by $[5]$ and give its order.

(f) What is the order of $[7]$ in U_{12}? Describe the subgroup generated by $[7]$ and give its order.

(g) Is U_{12} cyclic? Prove it or disprove it.

5. Let $\phi : G \to G$ be a homomorphism.

   (a) Prove that for every $[b] \in G$, there is only one homomorphism ϕ such that $\phi([1]) = [b]$ (Hint : Compute $\phi([k])$ for each $[k] \in G$). Describe the image of ϕ as a subgroup of G.

   (b) Suppose $\phi([1]) = [2]$, is ϕ an automorphism? Justify.

   (c) Let $\phi : G \to G$ be a homomorphism. Suppose $\phi([1]) = [5]$, is ϕ an automorphism? Justify.

   (d) Prove that $[1] \in < [b] >$, where $< [b] >$ is the group generated by some $[b] \in \mathbb{Z}/12\mathbb{Z}$ if and only if $[b]$ is a generator of $\mathbb{Z}/12\mathbb{Z}$.

   (e) Prove that ϕ is an automorphism if and only if $\phi([1]) = [b]$ with $[b]$ a generator of $\mathbb{Z}/12\mathbb{Z}$.

   (f) Deduce that $[b] \in U_{12}$ if and only if the homomorphism define by $\phi([1]) = [b]$ is in $Aut(\mathbb{Z}/12\mathbb{Z})$.

   (g) Now we can define $\psi : U_{12} \to Aut(\mathbb{Z}/12\mathbb{Z})$ sending $[b]$ to the homomorphism define by $\phi([1]) = [b]$.

      i. Prove that it is a homomorphism.

      ii. Prove that it is also an isomorphism