Math 546, Exam 4, Fall 2004, Solutions

The exam is worth 50 points.

Write your answers as legibly as you can on the blank sheets of paper provided. Use only **one side** of each sheet. Take enough space for each problem. Turn in your solutions in the order: problem 1, problem 2, ... ; although, by using enough paper, you can do the problems in any order that suits you.

If I know your e-mail address, I will e-mail your grade to you. If I don't already know your e-mail address and you want me to know it, then **send me an e-mail**.

I will leave your exam outside my office TOMORROW by about 6PM, you may pick it up any time between then and the next class.

I will post the solutions on my website at about 4:00 PM today.

1. **(7 points) STATE and PROVE the Chinese Remainder Theorem.**

The Chinese Remainder Theorem. *Suppose m and n are relatively prime non-zero integers. Prove that the groups $\frac{\mathbb{Z}}{mn\mathbb{Z}}$ and $\frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$ are isomorphic.*

Define $\varphi\colon \mathbb{Z} \to \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$ by $\varphi(a) = (a+m\mathbb{Z}, a+n\mathbb{Z})$ for all $a \in \mathbb{Z}$. We show that φ is a group homomorphism. Take a and b in $\mathbb{Z}$. We see that

$$\varphi(a+b) = (a+b+m\mathbb{Z}, a+b+n\mathbb{Z}) = (a+m\mathbb{Z}, a+n\mathbb{Z})+(b+m\mathbb{Z}, b+n\mathbb{Z}) = \varphi(a)+\varphi(b).$$

To show that φ is onto, we use the Lemma from Number Theory which says that the greatest common divisor of any two non-zero integers is equal to a linear combination (with integer coefficients) of the two integers. In particular, there exist integers r and s with

$$(*) \qquad rm + sn = 1.$$

Let $(a + m\mathbb{Z}, b + n\mathbb{Z})$ be an arbitrary element of $\frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$. Observe that $\varphi(asn + brm) = (a + m\mathbb{Z}, b + n\mathbb{Z})$. It is clear that $mn\mathbb{Z}$ is contained in the kernel of φ. We show that $\ker\varphi \subseteq mn\mathbb{Z}$. Take $a \in \ker\varphi$. It is clear that $a \in n\mathbb{Z}$ and $a \in m\mathbb{Z}$. Multiply (*) by a to see that $a \in mn\mathbb{Z}$. The First Isomorphism Theorem says that $\frac{\mathbb{Z}}{\ker\varphi}$ is isomorphic to $\operatorname{im}\varphi$. In other words, $\frac{\mathbb{Z}}{mn\mathbb{Z}}$ is isomorphic to $\frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$.

2. **(8 points) STATE and PROVE the First Isomorphism Theorem.**

The First Isomorphism Theorem. *If $\varphi\colon G \to G'$ is a group homomorphism, then $\bar{\varphi}\colon \frac{G}{\ker\varphi} \to \operatorname{im}\varphi$, which is given by $\bar{\varphi}(g\ker\varphi) = \varphi(g)$, is a group isomorphism.*

We first observe that $\bar{\varphi}$ is a well-defined function. Suppose g_1 and g_2 are in G and $g_1\ker\varphi$ and $g_2\ker\varphi$ are equal cosets. It follows that $g_1 = g_2k$ for some $k \in \ker\varphi$; and therefore, $\varphi(g_1) = \varphi(g_2k) = \varphi(g_2)\varphi(k) = \varphi(g_2)\mathrm{id} = \varphi(g_2)$. We see that $\bar{\varphi}(g_1\ker\varphi) = \bar{\varphi}(g_2\ker\varphi)$, as we desired.

We observe that $\bar{\varphi}$ is a homomorphism. If g_1 and g_2 are in G, then

$$\bar{\varphi}(g_1 \ker \varphi)\bar{\varphi}(g_2 \ker \varphi) = \varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) = \bar{\varphi}(g_1g_2 \ker \varphi).$$

We observe that $\bar{\varphi}$ is onto. Take an arbitrary element g' of the target of $\bar{\varphi}$, which is $\operatorname{im}\varphi$. It follows that $g' = \varphi(g_1)$ for some $g_1 \in G_1$; and therefore, $g' = \bar{\varphi}(g_1 \ker \varphi)$.

We observe that $\bar{\varphi}$ is one-to-one. Take g_1 and g_2 in G_1 with $\bar{\varphi}(g_1 \ker \varphi) = \bar{\varphi}(g_2 \ker \varphi)$. It follows that $\varphi(g_1) = \varphi(g_2)$; so, $\varphi(g_1g_2^{-1}) = \mathrm{id}$. Thus, $g_1g_2^{-1} \in \ker \varphi$ and the cosets $g_1 \ker \varphi$ and $g_2 \ker \varphi$ are equal.

3. **(7 points) Are the groups $\frac{\mathbb{Z}}{6\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}}$ and $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{15\mathbb{Z}}$ isomorphic? PROVE your answer.**

YES. According to the Chinese Remainder Theorem each group is isomorphic to $\frac{\mathbb{Z}}{30\mathbb{Z}}$.

4. **(7 points) Are the groups $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}}$ and $\frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ isomorphic? PROVE your answer.**

NO. The group on the left has 12 elements of order 4, 3 elements of order 2, and 1 element of order 1. The group on the right has 8 elements of order 4, 7 elements of order 2, and 1 element of order 1. Every group isomorphism induces bijection between the elements of order ℓ in the domain and the elements of order ℓ in the target for all non-negative integers ℓ.

5. **(7 points) Are the groups $(\mathbb{R}, +)$ and $(\mathbb{R}^{\text{pos}}, \times)$ isomorphic? PROVE your answer. (I am using $\mathbb{R}^{\text{pos}}$ to represent the set of positive real numbers.)**

YES. Define $\phi\colon \mathbb{R} \to \mathbb{R}^{\text{pos}}$ by $\phi(a) = 10^a$. Observe that

$$\phi(a+b) = 10^{a+b} = 10^a 10^b = \phi(a)\phi(b).$$

The map ϕ is onto because if $r \in \mathbb{R}^{\text{pos}}$, then $\log_{10} r \in \mathbb{R}$ and $\phi(\log_{10} r) = r$. The map ϕ is one-to-one, because if a and b are in $\mathbb{R}$ with $\phi(a) = \phi(b)$, then $10^a = 10^b$ and we may apply $\log_{10}$ to both sides to see that $a = b$.

6. **(7 points) Let $\phi\colon G_1 \to G_2$ and $\theta\colon G_2 \to G_3$ be group homomorphisms. Prove that $\theta \circ \phi$ is a group homomorphism.**

Take g and g' in G_1. Observe that

$$(\theta \circ \phi)(gg') = \theta(\phi(gg')) = \theta(\phi(g)\phi(g')) = \theta(\phi(g))\theta(\phi(g')) = (\theta \circ \phi)(g)(\theta \circ \phi)(g').$$

7. **(7 points) Suppose that S and T are sets and $\phi\colon S \to T$ and $\theta\colon T \to S$ are functions with $\theta \circ \phi$ equal to the identity function on S.**
(a) Does ϕ have to be one-to-one? PROVE or give a COUNTEREXAMPLE.

YES. Take s and s' in S with $\phi(s) = \phi(s')$. Apply θ to each side to get:

$$s = \theta(\phi(s)) = \theta(\phi(s')) = s'.$$

(b) **Does θ have to be onto? PROVE or give a COUNTEREXAMPLE.**

YES. Take $s \in S$. The hypothesis tells us that $\phi(s)$ is an element of T and $\theta(\phi(s)) = s$.