Math 546, Exam 3, Fall 2011

Write everything on the blank paper provided.

You should KEEP this piece of paper.

If possible: turn the problems in order (use as much paper as necessary), use only one side of each piece of paper, and leave 1 square inch in the upper left hand corner for the staple. If you forget some of these requests, don't worry about it – I will still grade your exam. The exam is worth 50 points. There are **8** problems.

Write **coherently** in **complete sentences**. **No Calculators or Cell phones.**

1. (7 points) **Define** *normal subgroup*. **Use complete sentences. Write everything that is necessary for your definition to make sense, but nothing extra.**

The subgroup H of the group G is a normal subgroup if ghg^{-1} is in H for all $g \in G$ and $h \in H$.

2. (7 points) **Define** *group homomorphism*. **Use complete sentences. Write everything that is necessary for your definition to make sense, but nothing extra.**

The function φ from the group $(G, *)$ to the group $(G', *')$ is a group homomorphism if $f(g_1 * g_2) = \varphi(g_1) *' \varphi(g_2)$ for all g_1 and g_2 in G.

3. (6 points) **Let ℓ, m, and n be fixed positive integers and let H be the subgroup**

$$H = \{am + bn \mid a, b \in \mathbb{Z}\}$$

of $\mathbb{Z}$. (I believe that H is a subgroup. I do not need to see a proof.) Suppose that H is also equal to $\{c\ell \mid c \in \mathbb{Z}\}$. Prove that ℓ is the greatest common divisor of n and m.

We see that $m \in H = \{c\ell \mid c \in \mathbb{Z}\}$ so $\ell | m$ and $n \in H = \{c\ell \mid c \in \mathbb{Z}\}$ so $\ell | n$. Thus, ℓ is a common divisor of m and n. We now show that ℓ is the greatest common divisor of m and n. Suppose z is a common divisor of m and n. We must show that $z \le \ell$. If z happens to be negative, then z is certainly less than the positive ℓ; so we need only think about the problem when z is positive. We know that $\ell \in H = \{am + bn \mid a, b \in \mathbb{Z}\}$; so $\ell = am + bn$ for some a and b; but z divides m and z divides n; so z also divides $am + bn = \ell$. Thus, $\ell = \#z$ for some positive integer $\#$ and $z \le \ell$.

4. (6 points) **Let $S = \mathbb{R} \setminus \{-2\}$. Define an operation $*$ on S by $a * b = ab + 2a + 2b + 2$. I believe that $(S, *)$ is a group. I want you to exhibit a group isomorphism from $(\mathbb{R} \setminus \{0\}, \times)$ to $(S, *)$. Prove that your candidate is a group isomorphism.**

Define $\varphi\colon \mathbb{R} \setminus \{0\} \to S$, by $f(r) = r - 2$. It is clear that $g\colon S \to \mathbb{R} \setminus \{0\}$, given by $g(s) = s + 2$, is the inverse of φ. It follows that φ is one-to-one and onto. We must show that φ is a homomorphism. Take r and r' from $\mathbb{R} \setminus \{0\}$. We see that

$$\varphi(r) * \varphi(r') = (r-2) * (r'-2) = (r-2)(r'-2) + 2(r-2) + 2(r'-2) + 2$$

$$= rr' - 2r' - 2r + 4 + 2r - 4 + 2r' - 4 + 2 = rr' - 2 = \varphi(rr')$$

5. (6 points) **Let X and Y be sets. Suppose that $f\colon X \to Y$ and $g\colon Y \to X$ are functions. Suppose further that $(g \circ f)(x) = x$ for all x in X.**
   (a) Does f have to be one-to-one? If yes, prove it. If no, give an example.
   (b) Does f have to be onto? If yes, prove it. If no, give an example.

(a) Yes, f has to be one-to-one. Suppose x and x' are in X with $f(x) = f(x')$. Apply g to see that

$$x = g(f(x)) = g(f(x')) = x'.$$

(b) No, f does not have to be onto. Take $X = 1$ and $Y = \{1, 2\}$. Define $f\colon X \to Y$ by $f(1) = 1$. Define $g\colon Y \to X$ by $g(1) = g(2) = 1$. We have $(g \circ f)(1) = 1$ and 1 is the only element of X. It is obvious that f is not onto because there is no element x of X with $f(x) = 2$.

6. (6 points) **Let $G = <g>$ be a cyclic group of order 48. Draw the lattice of subgroups of G.**

7. (6 points) **Prove that every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.**

Let $(G, *)$ be an infinite cyclic group with generator g. Define $\varphi\colon \mathbb{Z} \to G$ by $\varphi(n) = g^n$, where g^n means

$$\begin{cases} \underbrace{g * g * \cdots * g}_{n \text{ times}} & \text{for } 0 < n \\ \text{id} & \text{for } n = 0 \\ \underbrace{g^{\text{inv}} * g^{\text{inv}} * \cdots * g^{\text{inv}}}_{|n| \text{ times}} & \text{for } n < 0 \end{cases}$$

It is clear that f is onto because the words "g generates G" means that every element of G is equal to g^n for some integer n. The group G is infinite so g^n is equal to id only for $n = 0$; so the kernel of φ is $\{0\}$ and therefore φ is injective. The function φ is a homomorphism because

$$\varphi(n+m) = g^{n+m} = g^n * g^m = \varphi(n) * \varphi(m)$$

for all n and m in $\mathbb{Z}$.

8. (6 points) **Consider the function $\varphi\colon (\mathbb{R}^2, +) \to (\mathbb{R}, +)$ which is given by $\varphi\left(\begin{bmatrix} a \\ b \end{bmatrix}\right) = a + b$. Is f a group homomorphism? If yes, prove it and identify the kernel and image of φ. If no, give a counterexample.**

Yes. Take $\begin{bmatrix} a \\ b \end{bmatrix}$ and $\begin{bmatrix} a' \\ b' \end{bmatrix}$ from $\mathbb{R}^2$. We see that

$$\varphi\left(\begin{bmatrix} a \\ b \end{bmatrix} + \begin{bmatrix} a' \\ b' \end{bmatrix}\right) = \begin{bmatrix} a + a' \\ b + b' \end{bmatrix} = a + a' + b + b' = (a + b) + (a' + b')$$

$$= \varphi\left(\begin{bmatrix} a \\ b \end{bmatrix}\right) + \varphi\left(\begin{bmatrix} a' \\ b' \end{bmatrix}\right).$$

The image of $\mathbb{F}$ is all of $\mathbb{R}$ because if $r \in \mathbb{R}$, then $\varphi\left(\begin{bmatrix} r \\ 0 \end{bmatrix}\right) = r$. The kernel of φ is the subgroup $\left\{\begin{bmatrix} r \\ -r \end{bmatrix} \middle| r \in \mathbb{R}\right\}$ of $\mathbb{R}^2$ because if $\begin{bmatrix} a \\ b \end{bmatrix}$ is an arbitrary element of $\mathbb{R}^2$, then $\begin{bmatrix} a \\ b \end{bmatrix}$ is in the kernel of $\mathbb{F}$ if and only if $\varphi\begin{bmatrix} a \\ b \end{bmatrix} = 0$; that is, $a - b = 0$; that is, $a = b$.