Math 546, Exam 4, Summer, 2002

PRINT Your Name:________________________________

There are 10 problems on 5 pages. Each problem is worth 5 points.

Neither your exam, nor your score, will not be available until class on Monday.

1. Define "group isomorphism". Use complete sentences.

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

2. Let d be the greatest common divisor of the integers a and b. Prove that there exist integers r and s with $d = ra + sb$.

Let $H = \{ra + sb \mid r, s \in \mathbb{Z}\}$. It is clear that H is a subgroup of $\mathbb{Z}$. We know that every subgroup of $\mathbb{Z}$ is cyclic. Let h be the positive generator of H. We complete the proof by showing that $h = d$.

On the one hand, we know that a and b are each in H. Thus, a and b are each divisible by h. In other words, h is a common divisor of a and b. The number d is the GREATEST common divisor of a and b. It follows that $h \le d$.

On the other hand, h is in H. So $h = ra + sb$ for some integers r and s. The integer d divides a; d also divides b. It follows that d divides $ra + sb = h$. The integers d and h are both positive; so h is equal to d, or $2d$, or $3d$, etc. At any rate, we have shown that $d \le h$. Combine the two inequalities to conclude that $d = h$; thereby completing the proof.

3. Let G be the subgroup of $(\mathbb{Z}, +)$ which consists of all multiples of 3. Consider the function $\varphi\colon \mathbb{Z} \to G$ which is given by $\varphi(n) = 3n$ for all integers n. Prove that φ is an isomorphism.

We check that φ is a homorphism. Take n and m in $\mathbb{Z}$. We see that

$$\varphi(n + m) = 3(n + m) = 3n + 3m.$$

On the other hand, we also see that

$$\varphi(n) + \varphi(m) = 3n + 3m.$$

We conclude that $\varphi(n + m) = \varphi(n) + \varphi(m)$.

We check that φ is onto. Take a typical element g of G. The element g is "a multiple of 3"; so, $g = 3n$ for some integer n; and therefore, $g = \varphi(n)$.

We check that φ is one-to-one. Take integers n and m with $\varphi(n) = \varphi(m)$. In other words, $3n = 3m$ in $\mathbb{Z}$. One may divide by 3 (over $\mathbb{Q}$, at least) in order to conclude that $n = m$.

4. Prove that the groups $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_8^\times, \times)$ are not isomorphic. The proof does not have to be long, but it does have to be clear.

The group $(\mathbb{Z}_4, +)$ is cyclic with generator $[1]_4$. Every element in the group $\mathbb{Z}_8^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$, squares to ther identity element. Thus $\mathbb{Z}_8^\times$ is not a cyclic group. We know that if two groups are isomorphic and one of them is cyclic, then they both must be cyclic. It follows that $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_8^\times, \times)$ are not isomorphic.

5. Recall that each element of S_4 is a function from $\{1,2,3,4\}$ to $\{1,2,3,4\}$. Let
$$T = \{\sigma \in S_4 \mid \sigma(1) = 1\}.$$
Is T a subgroup of S_4? Prove your answer.

The set T IS a group. The identity element of S_4 is in T. The set T is closed because if σ and τ are both in T, then $\sigma \circ \tau$ is in T, since
$$(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(1) = 1.$$
The set T is also closed under the formation of inverse. If σ is in T, then the inverse of σ is a non-negative power of σ (since S_4 is finite). We already saw that T is closed.

6. Recall that each element of S_4 is a function from $\{1,2,3,4\}$ to $\{1,2,3,4\}$. Let
$$W = \{\sigma \in S_4 \mid \sigma(1) \text{ is equal to either } 1 \text{ or } 2\}.$$
Is W a subgroup of S_4? Prove your answer.

The set W is NOT a group because W is not closed. Indeed, $(2,3)$ and $(1,2,3)$ are in W, but $(2,3)(1,2,3) = (1,3)$ is not in W.

7. How many elements of S_4 have order 2?

There are $\boxed{9}$ elements of order 2 in S_4. There are 6 transpositions (i,j) and there are three elements which are the product of disjoint transpositions $(i,j)(k,\ell)$, with i,j,k,ℓ all distinct.

8. Let $\mathbb{R}^{\text{pos}}$ represent the group of positive real numbers under multiplication. Exhibit an isomorphism from the group $\mathbb{R}^{\text{pos}} \times U$ to the group $(\mathbb{C} \setminus \{0\}, \times)$. Prove that your isomorphism really is an isomorphism.

Define $\varphi\colon \mathbb{R}^{\text{pos}} \times U \to \mathbb{C} \setminus \{0\}$ by $\varphi(r,u) = ru$, for $r \in \mathbb{R}^{\text{pos}}$ and $u \in U$. We see that φ is a homomorphism. Take (r,u) and (s,v) from $\mathbb{R}^{\text{pos}} \times U$. Observe that
$$\varphi\Big((r,u)(s,v)\Big) = \varphi(rs, uv) = rsuv, \textbf{and}$$
$\varphi(r,u)\varphi(s,v) = rusv$. These two expressions are equal because complex multiplication is commutative.

We see that φ is onto. Let $z = a + b\imath$ be a non-zero complex number. We see that the modulus $|z| = \sqrt{a^2+b^2}$ is a positive real number with $z/|z|$ a number in U. Thus, $(|z|, z/|z|)$ is an element of $\mathbb{R}^{\text{pos}} \times U$, with $\varphi(|z|, z/|z|) = |z|(z/|z|) = z$.

We see that φ is one-to-one. Take (r,u) and (s,v) from $\mathbb{R}^{\text{pos}} \times U$ with $\varphi(r,u) = (s,v)$. It follows that $ru = sv$. Take the modulus of both sides to see that $r = |ru| = |sv| = s$. Divide both sides by $r = s$ to see that $u = ru/r = sv/r = sv/s = v$. We have shown that $r = s$ and $u = v$. We conclude $(r,u) = (s,v)$.

9. Is the group $D_4 \times U_3$ isomorphic to the group S_4? Exhibit an isomorphism or prove that the groups are not isomorphic.

These groups are NOT isomorphic. The group $D_4 \times U_3$ contains an element of order 6, namely, (σ, u), where u is a cube root of 1, which does not equal 1. On the other hand, S_4 does not contain any elements of order 6. We know that if $\varphi\colon G \to G'$ is a group isomorphism, then $\varphi(g)$ and g have the same order for each g in G.

10. Express the permutation $(6,9)(4,7,9)(4,8)$ as a product of disjoint cycles.

The permutation is equal to $\boxed{(4,8,7,6,9)}$.