Math 546, Final Exam , Fall 2004

The exam is worth 100 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.

I will grade the exams on Saturday. When I finish, I will e-mail your grade to you.

I will post the solutions on my website when the exam is finished.

1. (7 points)**STATE and PROVE Cayley's Theorem.**

Cayley's Theorem. *Every group is isomorphic to a group of permutations.*

Proof. Let G be a group. For each element a in G, let λ_a be the function from G to G, which is defined by $\lambda_a(g) = ag$.

(a) We first show that $\lambda_a \colon G \to G$ is one-to-one and onto.

one-to-one: Let x and y be in G with $\lambda_a(x) = \lambda_a(y)$. It follows that $ax = ay$. Multiply both sides of the equation on the left by a^{-1} to see that $x = y$.

onto: Take $x \in G$. We see that $a^{-1}x \in G$ and $\lambda_a(a^{-1}x) = x$.

We now know that each λ_a is an element of $\mathrm{Sym}(G)$.

(b) Consider the function $\Lambda \colon G \to \mathrm{Sym}(G)$, which is given by $\Lambda(a) = \lambda_a$. We claim that Λ is a group homomorphism. Take elements a and b of G. We must show that $\Lambda(ab)$ is equal to $\Lambda_a \circ \Lambda_b$. We know that $\Lambda(ab) = \lambda_{ab}$ and $\Lambda_a \circ \Lambda_b = \lambda_a \circ \lambda_b$. We show that the FUNCTIONS λ_{ab} and $\lambda_a \circ \lambda_b$ are equal by showing that they do the same thing to each element of the domain. Take x in G. We see that $\lambda_{ab}(x) = abx$. We also see that $(\lambda_a \circ \lambda_b)(x) = \lambda_a(\lambda_b(x)) = \lambda_a(bx) = abx$. We conclude that $\lambda_{ab} = \lambda_a \circ \lambda_b$; hence, $\Lambda(ab) = \Lambda_a \circ \Lambda_b$.

(c) We show that Λ is one-to-one. Suppose a and b are in G, with $\Lambda(a) = \Lambda(b)$. This means that the functions λ_a and λ_b from G to G are equal. In particular, $\lambda_a(\mathrm{id}) = \lambda_b(\mathrm{id})$. In other words, $a = a(\mathrm{id}) = b(\mathrm{id}) = b$.

We have proven that Λ is an isomorphism from G onto a subgroup of the permutation group $\mathrm{Sym}(G)$.

2. **(7 points) Apply the proof of Cayley's Theorem to the element** $(1,2,3)$ **of the group**

$$A_4 = \{(1),(1,2,3),(1,3,2),(1,2,4),(1,4,2),(1,3,4),(1,4,3),(2,3,4),(2,4,3),$$

$$(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}.$$

(Number the elements of A_4 **using the order I in which I listed the elements.) What do you get?**

The elements of A_4 correspond to $\{1,2,3,4,5,6,7,8,9,10,11,12\}$ by way of:

$$\begin{gathered}
(1) \leftrightarrow 1\\
(1,2,3) \leftrightarrow 2\\
(1,3,2) \leftrightarrow 3\\
(1,2,4) \leftrightarrow 4\\
(1,4,2) \leftrightarrow 5\\
(1,3,4) \leftrightarrow 6\\
(1,4,3) \leftrightarrow 7\\
(2,3,4) \leftrightarrow 8\\
(2,4,3) \leftrightarrow 9\\
(1,2)(3,4) \leftrightarrow 10\\
(1,3)(2,4) \leftrightarrow 11\\
(1,4)(2,3) \leftrightarrow 12
\end{gathered}$$

The function $\lambda_{(1,2,3)}$ takes

$$\begin{gathered}
(1) \mapsto (1,2,3) \mapsto (1,3,2) \mapsto (1)\\
(1,2,4) \mapsto (1,3)(2,4) \mapsto (2,4,3) \mapsto (1,2,4)\\
(1,4,2) \mapsto (1,4,3) \mapsto (1,4)(2,3) \mapsto (1,4,2)\\
(1,3,4) \mapsto (2,3,4) \mapsto (1,2)(3,4) \mapsto (1,3,4);
\end{gathered}$$

So, $\lambda_{(1,2,3)}$ corresponds to the element

$$(1,2,3)(4,11,9)(5,7,12)(6,8,10)$$

of S_{12}.

3. **(7 points) Let $\varphi\colon G \to G'$ be a group homomorphism. Prove that φ is one-to-one if and only if the kernel of φ is $\{\mathrm{id}\}$.**

⇒ Suppose φ is one-to-one. We know that $\varphi(\mathrm{id}) = \mathrm{id}$ since φ is a group homomorphism. If $x \in \ker\varphi$, then $\varphi(x) = \varphi(\mathrm{id})$. The hypothesis that φ is one-to-one ensures that $x = \mathrm{id}$. Thus, we have shown that $\ker\varphi = \{\mathrm{id}\}$.

⇐ Suppose $\ker\varphi = \{\mathrm{id}\}$. We must show that φ is one-to-one. Take x and y in G with $\varphi(x) = \varphi(y)$. Use the fact that φ is a group homomorphism to see that $\varphi(xy^{-1}) = \mathrm{id}$; hence, $xy^{-1} \in \ker\varphi = \{\mathrm{id}\}$. So, $xy^{-1} = \mathrm{id}$. So, $x = y$, and φ is one-to-one.

4. **(7 points) Give an example of a non-abelian group of order 16. A very short explanation will suffice.**

The group $U_2 \times D_4$ has 2(8)=16 elements. This group is non-abelian because

$$(1,\sigma)(1,\rho) = (1,\sigma\rho) \neq (1,\rho\sigma) = (1,\rho)(1,\sigma).$$

5. **(7 points) Give an example of an abelian, but non-cyclic, group of order 16. Explain.**

The group $\mathbb{Z}_2 \times \mathbb{Z}_8$ also has 16 elements. Every element in this group has order less than or equal to 8.

6. **(7 points) Let H be the subgroup $<(1,2,3)>$ of the group $G = A_4$, and let S be the set of left cosets of H in G. Define multiplication on S by $(g_1H)(g_2H) = (g_1g_2)H$ for all g_1 and g_2 in G. Is S a group? Explain very thoroughly.**

NO!! The "multiplication" does not make any sense. We see that $(1)H = (1,2,3)H$. However,

$$[(1)H][(12)(34)H] \neq [(1,2,3)H][(12)(34)H]$$

because

$$[(1)H][(12)(34)H] = [(12)(34)]H = \{(12)(34), (2,4,3), (1,4,3)\}$$

and

$$[(1,2,3)H][(12)(34)H] = [(1,2,3)(12)(34)]H = \{(1,3,4), (1,2,4), (1,4)(2,3)\}.$$

7. **(9 points) Let N be a normal subgroup of the group G and let H be any subgroup of G. Let HN be the subset $\{hn \mid h \in H \text{ and } n \in N\}$ of G.**
   (a) Prove that HN is a subgroup of G.
   (b) Prove that N is a normal subgroup of HN.
   (c) Let $\varphi\colon H \to \frac{HN}{N}$ be the group homomorphism which is given as the composition of inclusion $H \to HN$, followed by the natural quotient map $HN \to \frac{HN}{N}$. What is the kernel of φ?
   (d) Apply the First Isomorphism Theorem to φ.
   (You just proved the "Second Isomorphism Theorem".)

Lemma. *If $h \in H$ and $n \in N$, then $nh \in HN$.*

Proof. We know that N is a normal subgroup of G; and therefore, $h^{-1}nh \in N$. It follows that $h^{-1}nh = n'$ for some $n' \in N$ and $nh = hn' \in HN$.

(a) **Closure:** Take two typical elements x_1 and x_2 of HN. We see that $x_i = h_in_i$ for some h_i in H and $n_i \in N$. Also,

$$x_1x_2 = h_1n_1h_2n_2 = h_1h_2n_1'n_2 \in HN$$

for some $n_1' \in N$ by the Lemma.

Inverses: Take $x = hn$ from HN. We know that the inverse of x in G is $x^{-1} = n^{-1}h^{-1}$. The Lemma tells us that $x^{-1} \in NH$.

Identity: The identity element of G is in HN because $\mathrm{id} = (\mathrm{id})(\mathrm{id})$.

(b) If n is in N and $x \in HN$, then $x^{-1}nx$ is in N because N is a normal subgroup of all of G.

(c) The kernel of φ is $H \cap N$.

(d) $\frac{H}{H\cap N} \cong \frac{HN}{N}$.

8. **(7 points) Let V_4 be the subset $\{\mathbf{id},(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$ of S_4. It is true that V_4 is a normal subgroup of S_4; however, you do not have to prove this. What familiar group is isomorphic to $\frac{S_4}{V_4}$? Explain.**

Apply the second isomorphism theorem to see that $\frac{S_4}{V_4}$ is isomorphic to S_3. Let $\varphi\colon S_3 \to \frac{S_3V_4}{V_4}$ be the homomorphism which is given by $\varphi(x)$ is equal to the coset xV_4, for each x in S_3. It is clear that φ is onto. The kernel of φ is $S_3 \cap V_4 = \{\text{id}\}$. So, S_3 is isomorphic to $\frac{S_3V_4}{V_4}$. It follows that $\frac{S_3V_4}{V_4}$ consists of six cosets. The subgroup V_4 of the group S_3V_4 has four elements. So, the subgroup S_3V_4 of the group S_4 has 24 elements. Thus, $S_3V_4 = S_4$ and the groups $\frac{S_4}{V_4}$ and S_3 are isomorphic.

9. **(7 points) List the elements of the group $S_3 \times U_4$. What is the order of each element?**

element	order
$((1),1)$	1
$((1),\imath)$	4
$((1),-1)$	2
$((1),-\imath)$	4
$((1,2),1)$	2
$((1,2),\imath)$	4
$((1,2),-1)$	2
$((1,2),-\imath)$	4
$((1,3),1)$	2
$((1,3),\imath)$	4
$((1,3),-1)$	2
$((1,3),-\imath)$	4
$((2,3),1)$	2
$((2,3),\imath)$	4
$((2,3),-1)$	2
$((2,3),-\imath)$	4
$((1,2,3),1)$	3
$((1,2,3),\imath)$	12
$((1,2,3),-1)$	6
$((1,2,3),-\imath)$	12
$((1,3,2),1)$	3
$((1,3,2),\imath)$	12
$((1,3,2),-1)$	6
$((1,3,2),-\imath)$	12

10. **(7 points) Suppose that G is a group with at least two elements and that the only subgroups of G are $\{\text{id}\}$ and G. What is G? Say as much as you can. Prove your statement.**

Proposition. *If G is a group with at least two elements and the only subgroups of G are $\{id\}$ and G, then G is a finite cyclic group of prime order.*

Proof. G **is cyclic:** Let g be an element of G with $g \neq \text{id}$. The hypothesis ensures that $<g> = G$.

G **is finite:** Every infinite cyclic group has many subgroups. The group G only has two subgroups. So G is not infinite.

G **has prime order:** The group G is cyclic; hence, G has exactly one subgroup for each divisor of the order of G. The group G only has two subgroups; so, the order of G only has two positive factors. In other words, the order of G is prime.

11. **(7 points) Let G be a finite group of order n. Let g be an element of G. Prove that g^n is equal to the identity element of G.**

Let m equal the order of g. In other words, m is the least positive integer with $g^m = \text{id}$. It follows that the subgroup $<g>$ of G consists of exactly m elements. Lagrange's Theorem asserts that m divides evenly into n; that is, $md = n$ for some integer d. We see that $g^n = g^{md} = (g^m)^d = (\text{id})^d = \text{id}$.

12. **(7 points) Let a and b be elements of finite order in the group G. State and prove an interesting statement which gives the order of ab in terms of the order of a and the order of b.**

Proposition. *Let a and b be elements of finite order in the group G. Suppose that $ab = ba$ and that the order of a is relatively prime to the order of b. Then the order of ab is equal to the order of a times the order of b.*

Proof. Let ℓ equal the order of a, m equal the order of b, and n equal the order of ab.

$n \leq \ell m$: It is clear that

$$(ab)^{\ell m} = (a^\ell)^m (b^m)^\ell = (\text{id})^m (\text{id})^\ell = \text{id}.$$

So, the order of ab, which is the least positive power of ab which equals id, is less than or equal to ℓm.

$\ell m \leq n$: We know that $(ab)^n = \text{id}$. Let x be the element $a^n = b^{-n}$ of G. We see that $<x>$ is a subgroup of $<a>$. So the order of $<x>$ divides ℓ by Lagrange's Theorem. Also, $<x>$ is a subgroup of $<b>$. So the order of $<x>$ divides m. The integers ℓ and m have no common divisors other than 1 and -1; hence the order of $<x>$ is 1. In other words, $a^n = x = \text{id}$. It follows that ℓ divides into n. Also, $b^{-n} = x = \text{id}$; so, $b^n = \text{id}$ and m divides into n. The integers ℓ and m are relatively prime with $\ell | n$ and $m | n$. It follows that $\ell m | n$; and therefore, $\ell m \leq n$.

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

"NO!" for both parts. Let $S = \{1\}$, $T = \{1, 2\}$, $\phi(1) = 1$, $\theta(1) = 1$, $\theta(2) = 1$. Observe that $\theta \circ \phi$ is the identity function on S, but ϕ is not onto, and θ is not one-to-one.

14. **(7 points) Prove that $\frac{\mathbb{R}}{\mathbb{Z}} \cong U$, where U is the unit circle in $(\mathbb{C} \setminus \{0\}, \times)$ and $\mathbb{R}$ and $\mathbb{Z}$ are groups under addition.**

Define $\varphi\colon \mathbb{R} \to U$ by $\varphi(r) = e^{2\pi \imath r}$ for all $r \in \mathbb{R}$.

φ **is a homomorphism:** Take r and s in $\mathbb{R}$. Observe that

$$\varphi(r+s) = e^{2\pi\imath(r+s)} = e^{2\pi\imath r}e^{2\pi\imath s} = \varphi(r) + \varphi(s).$$

φ **is onto:** Take $u \in U$. Notice that $u = e^{\imath\theta}$ for some real number θ. Notice also, that $\frac{\theta}{2\pi} \in \mathbb{R}$ and $\varphi(\frac{\theta}{2\pi}) = u$.

$\ker\varphi = \mathbb{Z}$**:** It is clear that $\mathbb{Z} \subseteq \ker\varphi$ because if $n \in \mathbb{Z}$, then $\varphi(n) = e^{2\pi\imath n} = \cos 2\pi n + \imath \sin 2\pi n = 1$. On the other hand, if r is in $\mathbb{R}$ and $\varphi(r) = 1$, then $1 = e^{2\pi\imath r} = \cos(2\pi r) + \imath\sin(2\pi r)$. Think about the trigonometry for a few seconds. It follows that $2\pi r$ must be an integer multiple of 2π. In other words, r must be in $\mathbb{Z}$.

Apply the First Isomorphism Theorem: to conclude that $\frac{\mathbb{R}}{\mathbb{Z}} \cong U$.