Math 546, Spring 2004, Exam 3, Solutions

PRINT Your Name:________________________________

There are 8 problems on 4 pages. The exam is worth 50 points.

I won't grade your exam until Monday. So don't be surprised if I don't e-mail your grade to you until then.

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**.

If you would like, I will leave your exam outside my office after I have graded it. (If you like, I will send you an e-mail when I am finished with it.) You may pick it up any time between then and the next class. **Let me know if you are interested.**

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

1. (5 points) **Define "order". Use complete sentences.**

There are two possible correct answers.

Answer 1. The element a of the group G has *order* n if n is the least positive integer with $a^n = \mathrm{id}$.

Answer 2. The *order* of the finite subgroup H of the group G is the number of elements in H.

2. (5 points) **List ALL of the generators of $(\mathbb{Z}_8, +)$. No explanation is needed.**

The generators of $(\mathbb{Z}_8, +)$ are $[1]_8$, $[3]_8$, $[5]_8$, and $[7]_8$.

3. (5 points) **List ALL of the subgroups of $(U_{12}, \times)$. No explanation is needed.**

Let $u = \cos\frac{2\pi}{12} + \imath\sin\frac{2\pi}{12}$. The group $(U_{12}, \times)$ is cyclic and is generated by u. Every subgroup of $(U_{12}, \times)$ is cyclic. Furthermore, there is exactly one subgroup of $(U_{12}, \times)$ for each divisor of 12. The subgroups of $(U_{12}, \times)$ are $<1> = \{1\}$, $<u^6> = \{1, u^6\}$, $<u^4> = \{1, u^4, u^8\}$, $<u^3> = \{1, u^3, u^6, u^9\}$, $<u^2> = \{1, u^2, u^4, u^6, u^8, u^{10}\}$, and $\{u\} = U_{12}$.

4. (5 points) **Is $(\mathbb{Z}_{15}^{\times}, \times)$ a cyclic group? Explain.**

No. The elements of $(\mathbb{Z}_{15}^{\times}, \times)$ are $[1]_{15}$, $[2]_{15}$, $[4]_{15}$, $[7]_{15}$, $[8]_{15}$, $[11]_{15}$, $[13]_{15}$, and $[14]_{15}$. Thus, $(\mathbb{Z}_{15}^{\times}, \times)$ has 8 elements. Observe that $[1]_{15}$ has order 1 and $[4]_{15}$, $[11]_{15}$, and $[14]_{15}$ have order 2. (Keep in mind that $[14]_{15} = [-1]_{15}$ and $[11]_{15} = [-4]_{15}$; so $[14]_{15}^2 = [1]_{15}$ and $[11]_{15}^2 = [1]_{15}$ are obvious.) Furthermore, $[2]_{15}$, $[7]_{15}$, $[8]_{15}$, $[13]_{15}$, all square to $[4]_{15}$; therefore these elements all have order 4. Very little arithemetic is needed: $[8]_{15} = [-7]_{15}$ and $[13]_{15} = [-2]_{15}$. No element of the group has order 8. The group is not cyclic.

5. (5 points) **Recall that each element of $\mathbb{C}$ is a point on the complex plane. Give a geometric description of the left cosets of U in $(\mathbb{C} \setminus \{0\}, \times)$.**

If r is a positive real number, then the left coset rU consists of the circle with center 0 and radius r. If z is an arbitrary non-zero complex number, then z is equal to ru for some positive real number r and some point u on the unit circle. The left coset zU is equal to the left coset rU. Thus, every left coset of U in $(\mathbb{C}\setminus\{0\}, \times)$ is a circle with center 0. The left cosets of U in $(\mathbb{C}\setminus\{0\}, \times)$ partition $\mathbb{C} \setminus \{0\}$ into disjoint subsets as promised by our proof of Lagrange's theorem.

6. (5 points) **PROVE that every subgroup of $(\mathbb{Z}, +)$ is cyclic.**

Let H be a subgroup of $\mathbb{Z}$. If $H = \{0\}$, then H is cyclic and there is nothing more to show. Henceforth, we assume that H is non-zero. The subgroup H must then contain at least one positive element because H contains some non-zero element n. The inverse of n, which is $-n$, must also be in the subgroup H. One of the numbers n or $-n$ is positive. Let h_0 be the smallest positive element in H. I will prove that $H = <h_0>$. It is obvious that the group H contains $<h_0>$. We must prove that $H \subset <h_0>$. Let h be an arbitrary element of H. Divide h_0 into h to learn $h = sh_0 + r$ for some integers r and s with $0 \le r < h_0$. We see that $r = h - sh_0$ is an element of the group H. Our choice of h_0 guarantees that $r = 0$. Thus $h \in <h_0>$; and the proof is complete.

7. (4 points) **Let m and n be positive integers and let d be the greatest common divisor of m and n. PROVE that there exist integers r and s with $d = rm + sn$.**

Let $H = \{rm + sn \mid r, s \in \mathbb{Z}\}$. It is easy to see that H is closed under addition ($(rm + sn) + (r'm + s'n) = (r + r')m + (s + s')n$) and under the formation of inverses (the inverse of $rm+sn$ is $(-r)m+(-s)n$). Thus H is a subgroup of $\mathbb{Z}$. In the previous problem, we proved that every subgroup of $\mathbb{Z}$ is cyclic. It follows that H is cyclic. Let h_0 be the positive element of H with $H = <h_0>$. Since h_0 is in H, there automatically exist integers r_0 and s_0 with $h_0 = r_0m + s_0n$. We complete the proof by showing that $h_0 = d$.

$d \le h_0$: We know that d is a common divisor of m and n; so d divides $r_0m + s_0n = h_0$; and therefore $d \le h_0$.

$h_0 \le d$: We also know that m and n are elements of H. Every element of H is divisible by h_0; hence, h_0 is a common divisor of m and n. But d is the greatest common divisor of of m and n; so $h_0 \le d$ and the proof is complete.

8. **Let a and b be elements of finite order in the group G.**
   (a) (4 points) List two hypotheses (Hypothesis (1) and Hypothesis (2)) with the property that if Hypothesis (1) and Hypothesis (2) both hold, then the order of ab is equal to the order of a times the order of b.

Hypothesis (1): $ab = ba$

Hypothesis (2): the order of a is relatively prime to the order of b.

(b) (4 points) **Give an example where Hypothesis (1) holds, Hypothesis (2) fails to hold, and the conclusion also fails to hold.**

Consider ρ and ρ^2 in in D_3 . We know that ρ and ρ^2 commute; so Hypothesis (1) holds. On the otherhand, ρ and ρ^2 both have order 3 ; so Hypothesis (2) fails. Furthermore, the product $\rho\rho^2$ has order 1 , not order 9 .

(c) (4 points) **Give an example where Hypothesis (2) holds, Hypothesis (1) fails to hold, and the conclusion also fails to hold.**

Consider the elements σ and ρ in D_3 . We know that σ has order 2 and ρ has order 3 ; thus Hypothesis (2) holds. On the other hand, $\sigma\rho \neq \rho\sigma$ and $\sigma\rho$ has order 2 , not order 6 .

(d) (4 points) **Prove the result which you stated in (a).**

Let $\ell = o(a)$, $m = o(b)$, and $n = o(ab)$. Since ℓ , m and n all are positive integers, it suffices to prove that $n|\ell m$ and $\ell m|n$.

$n|\ell m$: The elements a and b commute; hence,

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

So, $(ab)^{\ell m}$ is the identity. It follows that n , which is the order of ab , must divide ℓm .

$\ell m|n$: Observe that

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

The order of b is m ; thus, $m|n\ell$. The integers m and ℓ are relatively prime; thus, $m|n$.
In a similar manner, we see that

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

The order of a is ℓ ; thus, $\ell|mn$. The integers ℓ and m are relatively prime; so, $\ell|n$.
Finally, we notice that $m|n$ and $\ell|n$, with ℓ and m relatively prime. It follows that $m\ell|n$, and the proof is complete.