MATH 301 - Section B **Fall 2014**

Midterm Exam

RULES

1. All phones and other electronic devices must be silenced for the duration of the exam.
2. No books, notes, or calculators allowed.
3. Out of consideration for your classmates, do not make disturbing noises during the exam. If you need a tissue, please ask for one.
4. Are you still reading the rules? Did you read rule number 1? If you haven't yet taken out your phone to turn it off, read rule number 1 a few more times.

Cheating will not be tolerated. If there are any indications that a student may have given or received unauthorized aid on this exam, the case will be brought to the ISU Office of Academic Integrity.

After finishing the exam, please sign the following statement acknowledging that you understand and accept this policy:

"On my honor as a student I, ________________________, have neither given nor received unauthorized aid on this exam." (print name clearly)

Signature: ______________________________________ Date: _______________

Do not sign the pledge until after you have finished the exam.

1. Give precise definitions of the following:

(a) **semigroup**

Answer:
A *semigroup* is an algebraic structure consisting of a set together with an associative binary operation.

Equivalently:
A *semigroup* is an algebraic structure $\mathbf{A} = \langle A, \cdot \rangle$, where A is a set and $\cdot : A^2 \to A$ is a binary operation on A satisfying the associative law: $\forall a, b, c \in A$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(b) **monoid**

Answer:
A *monoid* is an algebraic structure consisting of a set together with an associative binary operation and an identity element (nullary operation).

Equivalently:
A *monoid* is an algebraic structure $\mathbf{A} = \langle A, \cdot, e \rangle$, where $\langle A, \cdot \rangle$ is a semigroup and e is an element of A satisfying $\forall a \in A$, $a \cdot e = a = e \cdot a$.

(c) **group**

Answer:
A *group* is an algebraic structure $\mathbf{A} = \langle A, \cdot, ^{-1}, e \rangle$ consisting of a set A together with a binary operation $\cdot$, a unary operation $^{-1}$, and a nullary operation e, all satisfying the following *group laws*: for all $a, b, c \in A$,

i. (associativity) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
ii. (identity) $a \cdot e = a = e \cdot a$
iii. (inverse) $a \cdot a^{-1} = e = a^{-1} \cdot a$

Equivalently:
A *group* is a monoid along with a unary operation $^{-1}$ satisfying $a \cdot a^{-1} = a^{-1} \cdot a = e$ for all $a \in A$.

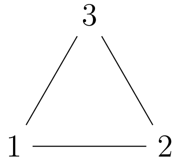
(d) **abelian group**

Answer:
An *Abelian group* is a group with a commutative binary operation, which we usually denote by $+$ instead of $\cdot$. In this case, we write 0 instead of e to denote the *additive identity*, and $-$ instead of $^{-1}$ to denote the *additive inverse*. Thus, an Abelian group is an algebraic structure $\mathbf{A} = \langle A, +, -, 0 \rangle$ satisfying the laws of groups and the following *commutative law*: $\forall a, b \in A$, $a + b = b + a$.

(e) **cyclic group**

Answer:
If G is a group and $g \in G$ and $G = \langle g \rangle$, then we say that G is a **cyclic group** and that g is a **generator** of G.
(Here the notation $\langle g \rangle$ means $\{g^k : k \in \mathbb{Z}\}$.)

2. Let G denote the symmetries of an equilateral triangle.



(a) List the elements of this group using cycle notation.

Answer:

$$\begin{aligned} \mathrm{id} &= (\quad) \\ \mu_1 &= (1,2) \\ \mu_2 &= (2,3) \\ \mu_3 &= (1,3) \\ \rho_1 &= (1,2,3) \\ \rho_2 &= (1,3,2) \end{aligned}$$

(b) What is the order of this group?

Answer: $|G| = 6$.

(c) Is this group cyclic? Is it abelian?
(Give a brief justification for your answers. You may cite 4(b).)

Answer: The group G above is **not abelian**. Indeed, there is at least one pair of noncommuting elements. For example, $\mu_1 \cdot \mu_2 = (1,2)(2,3) = (1,2,3)$, while $\mu_2 \cdot \mu_1 = (2,3)(1,2) = (1,3,2)$. Therefore, $\mu_1 \cdot \mu_2 \neq \mu_2 \cdot \mu_1$.
The group G above is **not cyclic**. Indeed, recall that every cyclic group is abelian (See Problem 4(b).) Therefore, since G is nonabelian, it is not cyclic.

3. Suppose H and K are subgroups of a group G. Prove or disprove the following:

(a) $H \cap K$ is a subgroup of G.

Claim: $H \cap K$ is a subgroup of G.

Proof: Let $I = H \cap K$. We check that I is a subgroup of G. Proposition 3.9 states that this is equivalent to showing that I is closed under the three operations (nullary, unary, binary) of G. In other words, we must show that I contains the identity (the nullary op), I is closed under inverse (the unary op), and I is closed under multiplication (the binary op).

- (nullary closure) Clearly $e \in I$ since both H and K, being themselves subgroups, contain e.
- (unary closure) If $x \in I = H \cap K$, then $x \in H$ and H is a subgroup, so $x^{-1} \in H$. Similarly, $x \in K$ and K a subgroup implies $x^{-1} \in K$. Therefore, $x^{-1} \in H \cap K$.
- (binary closure) Suppose x and y belong to $H \cap K$. Then, since $x, y \in H$ and H is a subgroup, we have $xy \in H$. Similarly, $x, y \in K$ and K a subgroup implies $xy \in K$. Therefore, $xy \in H \cap K$.

(b) $H \cup K$ is a subgroup of G.

This is false, and counterexamples abound. Here are two:

Example 1: In the symmetry group of the triangle from Problem 2 above, let $H = \langle \mu_1 \rangle = \{\mathrm{id}, \mu_1\}$ and $K = \langle \mu_2 \rangle = \{\mathrm{id}, \mu_2\}$. Then the set $H \cup K = \{\mathrm{id}, \mu_1, \mu_2\}$ is not a subgroup since it is not closed under the binary operation: $\mu_1 \cdot \mu_2 = \rho_1 \notin H \cup K$.

Example 2: In the group $\mathbb{Z}_3 \times \mathbb{Z}_3$ that appears in Exercise 33 of Chapter 3, we found that $\langle (0,1) \rangle \cup \langle (1,0) \rangle = \{(0,0), (0,1), (0,2), (1,0), (2,0)\}$, which clearly is not closed under the binary operation of addition modulo 3. For instance, $(0,1) + (1,0) = (1,1)$ which does not belong to the union.

(See also: Homework 4, Exercises 3.44, 3.45.)

4. Let G be a group. Prove the following:

(a) G is abelian if and only if $(gh)^2 = g^2h^2$ holds for all $g, h \in G$.

Proof:
($\Rightarrow$) Suppose G is abelian. Then for all $g, h \in G$ we have

$$(gh)^2 = (gh)(gh) = ghgh = gghh = g^2h^2.$$

($\Leftarrow$) Suppose $(gh)^2 = g^2h^2$ holds for all $g, h \in G$. Fix an arbitrary pair of elements $g, h \in G$. We must show that $gh = hg$. By assumption, $(gh)^2 = g^2h^2$, that is

$$(gh)(gh) = (gg)(hh). \tag{1}$$

Multiplying both sides of (1) on the left by g^{-1} and on the right by h^{-1}, we have

$$g^{-1}(gh)(gh)h^{-1} = g^{-1}(gg)(hh)h^{-1}. \tag{2}$$

By associativity, the left hand side of (2) is $g^{-1}g\, hg\, hh^{-1} = e\, hg\, e = hg$, while the right hand side is $g^{-1}g\, gh\, hh^{-1} = e\, gh\, e = gh$. Therefore, $hg = gh$.

(b) If G is cyclic, then G is abelian.

Proof:
Suppose G is cyclic. Then $G = \langle a \rangle$ for some $a \in G$. Fix an arbitrary pair of elements $g, h \in G$. We must show that $gh = hg$. Since $G = \langle a \rangle$, we have $g = a^j$ for some $j \in \mathbb{N}$ and $h = a^k$ for some $k \in \mathbb{N}$. Therefore,

$$gh = a^j a^k = a^{j+k} = a^{k+j} = hg.$$

(c) Give a specific example of a group G and elements $g, h \in G$ for which $(gh)^2 \neq g^2h^2$. (Justify your answer.)

Answer: Again, the group of symmetries on a triangle that showed up in Problem 2 is an example. Let $g = \mu_1$ and $h = \mu_2$. Then $\mu_1^2 = \text{id} = \mu_2^2$ and $\mu_1\, \mu_2 = \rho_1$, so,

$$(\mu_1\, \mu_2)^2 = \rho_1^2 = \rho_2 \neq \text{id} = \mu_1^2\, \mu_2^2.$$

(d) Give a specific example of a group that is abelian but not cyclic.
(No justification necessary.)

Answer: Many direct products of cyclic groups are abelian but not cyclic. For example, $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$ are both abelian but not cyclic.

(On the other hand, the group $\mathbb{Z}_3 \times \mathbb{Z}_4$ is not only abelian, but also cyclic! Check that the element $(1, 1)$ generates $\mathbb{Z}_3 \times \mathbb{Z}_4$. We will soon see that $\mathbb{Z}_3 \times \mathbb{Z}_4$ is just a "copy" of the cyclic group $\mathbb{Z}_{12}$, whereas $\mathbb{Z}_2 \times \mathbb{Z}_2$ is truly distinct from $\mathbb{Z}_4$.)

5. This problem has several parts. First, state the following (without proof):

(a) *The Well Ordering Principle.* (about subsets of natural numbers)

Answer: Every nonempty subset of the natural numbers is well ordered.

(b) *The Division Algorithm.* (about integers a and b where $b > 0$)

Answer: If a and b are integers and $b > 0$, then there exist integers q, r such that $a = qb + r$ and $0 \leq r < b$.

Prove that every subgroup of a cyclic group is cyclic by following the steps below. First, let $G = \langle a \rangle$ be a cyclic group and fix an arbitrary subgroup $H \leq G$.

(c) Suppose H contains only the identity, e. Say why H must be cyclic in this case. (one line/sentence)

Answer: $H = \{e\} = \langle e \rangle$ is one-generated, that is, cyclic.

(d) Suppose instead that H contains more than just the identity element. Let m be the smallest positive integer such that $a^m \in H$. Why does such a number m exists? (Hint: consider the set $\{m \in \mathbb{N} : a^m \in H\}$; cite a well known principle; say why it applies here.)

Answer: The set $\{m \in \mathbb{N} : a^m \in H\}$ is a subset of the natural numbers. We assumed H contains more than just the identity, so there is some $x \in H$ with $x \neq e$. Since $x \in H \leq G = \langle a \rangle$, there is some m such that $x = a^m$. Therefore, the set $\{m \in \mathbb{N} : a^m \in H\}$ is nonempty, so it satisfies the hypotheses of the Well Ordering Principle, which states that it must be well ordered (i.e., have a least element).

(e) Finally, prove the **Claim** stated on the **next page**. →
(which says that a^m generates H, where m is the number from part (b)).

Claim: If $H \leq G = \langle a \rangle$ and m is the smallest positive integer such that $a^m \in H$, then $H = \langle a^m \rangle$.

Proof: Let $x \in H$. The claim is that a^m generates H, so we need to prove that $x = a^{mq}$ for some $q \in \mathbb{N}$. Since $x \in H \leq G = \langle a \rangle$, we have $x = a^j$ for some j, and it suffices to show that m divides j (since this will give $qm = j$ for some q, whence $x = a^j = a^{qm}$).

By the division algorithm, there exist integers q, r such that $j = qm + r$ where $0 \leq r < m$. Therefore,

$$x = a^j = a^{qm+r} = a^{qm}a^r, \quad \text{so} \quad a^{-qm}x = a^r.$$

Now note that $a^{-qm} \in H$ and $x \in H$ together imply that $a^r \in H$. But $0 \leq r < m$ and m is the smallest positive integer with $a^m \in H$. Therefore, $r = 0$, so $j = qm$, and this proves that $m \mid j$.

6. Answer either (a) or (b). Only one answer will be graded. (If you answer both, then clearly mark which should be graded.)

(a) Show that, for any cyclic group $G = \langle a \rangle$, the subgroup $\langle a^j, a^k \rangle$ generated by a^j and a^k is equal to $\langle a^d \rangle$, where $d = \gcd(j, k)$. (Hint: Recall that there exist integers r and s such that $d = rj + sk$; you may use this fact without proving it.)

(b) Show that for any group G, and any fixed element $g \in G$, the map $\lambda_g : G \to G$ defined by $\lambda_g(a) = ga$ is a permutation of G. Then show that the order of the alternating group on n letters is $|A_n| = n!/2$.

(a) **Claim:** $\langle a^d \rangle = \langle a^j, a^k \rangle$

Proof: We first show $\langle a^d \rangle \subseteq \langle a^j, a^k \rangle$. Since $a^d = a^{rj+sk} = a^{rj}a^{sk} = (a^j)^r(a^k)^s$, we see that $a^d \in \langle a^j, a^k \rangle$, therefore, $\langle a^d \rangle \subseteq \langle a^j, a^k \rangle$.

Next we show $\langle a^j, a^k \rangle \subseteq \langle a^d \rangle$. Since $d = \gcd(j, k)$ we have $d \mid j$ so $j = md$ for some integer m. Therefore, $a^j = a^{dm} \in \langle a^d \rangle$. Similarly, $d \mid k$ so $k = nd$ for some integer n. Therefore, $a^k = a^{dn} \in \langle a^d \rangle$. Since a^j and a^k both belong to $\langle a^d \rangle$, it follows that $\langle a^j, a^k \rangle \subseteq \langle a^d \rangle$.

(b) **Claim:** For any group G, and any fixed element $g \in G$, the map $\lambda_g : G \to G$ defined by $\lambda_g(a) = ga$ is a permutation of G.

Proof: We must show that λ_g is one-to-one and onto. Let $x, y \in G$ and suppose $\lambda_g(x) = \lambda_g(y)$. Then $gx = gy$, so multiplying on the left of both sides by g^{-1} we have $g^{-1}gx = g^{-1}gy$, that is, $x = y$. This proves that λ_g is one-to-one. Let $z \in G$. To show λ_g is onto, we must show that there is some $x \in G$ with $\lambda_g(x) = z$. Indeed, take $x = g^{-1}z$. Then $\lambda_g(x) = \lambda_g(g^{-1}z) = gg^{-1}z = z$.

Claim: The order of the alternating group on n letters is $|A_n| = n!/2$.

Proof: We know there are $|S_n| = n!$ permutations in the full symmetric group on n letters. We want to show that half of these are even permutations. Let B_n denote the set of odd permutations. Fix some transposition $\tau \in S_n$. Any transposition will do, for example, we could choose $\tau = (1, 2)$. Then define $\lambda_\tau : A_n \to B_n$ by $\lambda_\tau(\sigma) = \tau\sigma$.

We will prove that λ_τ is one-to-one and onto, thus proving that $|A_n| = |B_n|$. Since S_n is the disjoint union of the sets A_n and B_n, it will follow that exactly half of the permutations in S_n are even and half are odd, so that $|A_n| = n!/2$.

Indeed, let σ, ρ be two arbitrary even permutation in A_n and suppose $\lambda_\tau(\sigma) = \lambda_\tau(\rho)$. Then $\tau\sigma = \tau\rho$, so left multiplying both sides by $\tau^{-1} = \tau$ we have $\sigma = \rho$. This proves that λ_τ is one-to-one.

Suppose μ is an arbitrary permutation in B_n. We must show there is some permutation $\sigma \in A_n$ such that $\lambda_\tau(\sigma) = \mu$. Indeed, select $\sigma = \tau\mu$. Then $\lambda_\tau(\sigma) = \lambda_\tau(\tau\mu) = \tau\tau\mu = \mu$. (The last equality holds since τ is a transposition, so $\tau^2 = \text{id}$; that is, $\tau = \tau^{-1}$.)

7. (a) Give a precise definition of *equivalence relation*, then give an example.

Answer:

(b) Give a precise definition of *partial order relation*, then give an example.

Answer:

(c) Let $f : X \to Y$ be a function and define the relation $\sim$ on the set X as follows:

$$m \sim n \quad \text{if and only if} \quad f(m) = f(n)$$

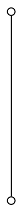
What kind of relation is $\sim$? (Justify your answer by checking the properties.)

Answer:

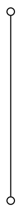
Extra Credit

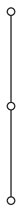
EC 1. (6 points) Below I have drawn the subgroup lattice diagrams for the groups $\mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_7$, $\mathbb{Z}_{12}$, $\mathbb{Z}_{16}$, $\mathbb{Z}_{30}$, and S_3, but I've forgotten which diagram go with which group. I was able to label the first diagram correctly. If you think you can help me label the others, go for it. But don't guess!

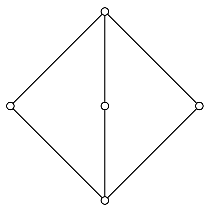
+1 *point for each correct answer,* −1/2 *point for each incorrect answer.*

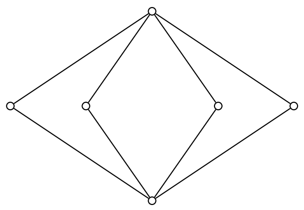


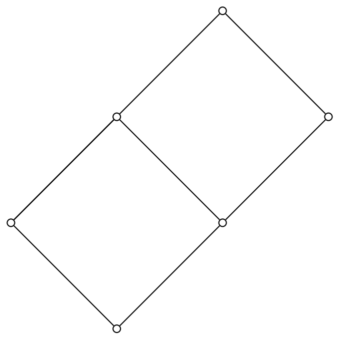
$G = \mathbb{Z}_2$

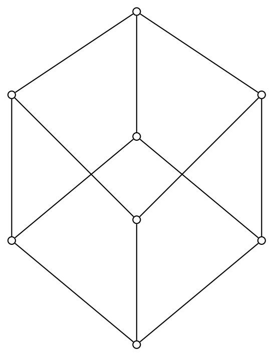












EC 2. (1/2 point) Which group appears in William DeMeo's GitHub gravatar? (William DeMeo the mathematician, not the actor.)