Test 1 - Abstract Algebra

Dr. Graham-Squire, Spring 2016

Name: Key

12:01
12:18
17

I pledge that I have neither given nor received any unauthorized assistance on this exam.

____
(*signature*)

DIRECTIONS

1. Don't panic.
2. Show all of your work and use correct notation. A correct answer with insufficient work or incorrect notation will lose points.
3. Cell phones and computers are not allowed on this test. Calculators are allowed, though it is unlikely that they will be helfpul.
4. Make sure you sign the pledge above.
5. Number of questions = 6. Total Points = 35.

1. (5 points) Consider the following Cayley table for a group with elements $\{1, 2, 3, \ldots, 12\}$:

	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	3	4	5	6	1	8	9	10	11	12	7
3	3	4	5	6	1	2	9	10	11	12	7	8
4	4	5	6	1	2	3	10	11	12	7	8	9
5	5	6	1	2	3	4	11	12	7	8	9	10
6	6	1	2	3	4	5	12	7	8	9	10	11
7	7	12	11	10	9	8	1	6	5	4	3	2
8	8	7	12	11	10	9	2	1	6	5	4	3
9	9	8	7	12	11	10	3	2	1	6	5	4
10	10	9	8	7	12	11	4	3	2	1	6	5
11	11	10	9	8	7	12	5	4	3	2	1	6
12	12	11	10	9	8	7	6	5	4	3	2	1

Answer the following questions about the group given above:

(a) Find the identity element. How do you know it is the identity?

(b) Find the inverse of 2. How do you know it is the inverse?

(c) Find $\langle 5 \rangle$, that is, the cyclic subgroup generated by 5.

(d) Show through an example that the group is associative. That is, take three elements a, b, and c (none of them the identity, that is too easy) and show that $(ab)c = a(bc)$.

(a) 1 is the identity b/c $1 \cdot * = *$ for any $*$

(b) $2^{-1} = 6$, b/c $2(6) = 1$

(c) $\langle 5 \rangle = \{5, 3, 1\}$

(d) $(2 \cdot 7)10 = 8(10) = 5$

$2(7 \cdot 10) = 2(4) = 5$ ✓

Should be with #2

2. (5 points) Consider again the Cayley table from the previous page, and answer the following questions:

	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	3	4	5	6	1	8	9	10	11	12	7
3	3	4	5	6	1	2	9	10	11	12	7	8
4	4	5	6	1	2	3	10	11	12	7	8	9
5	5	6	1	2	3	4	11	12	7	8	9	10
6	6	1	2	3	4	5	12	7	8	9	10	11
7	7	12	11	10	9	8	1	6	5	4	3	2
8	8	7	12	11	10	9	2	1	6	5	4	3
9	9	8	7	12	11	10	3	2	1	6	5	4
10	10	9	8	7	12	11	4	3	2	1	6	5
11	11	10	9	8	7	12	5	4	3	2	1	6
12	12	11	10	9	8	7	6	5	4	3	2	1

(a) Find two elements that do NOT commute.

(b) Find an w/o identity element that is its own inverse.

(c) Find an Abelian subgroup of order 6. How do you know it is a subgroup?

(d) Find a non-cyclic subgroup of either order 4 or of order 6.

(a) 7 and 6. $7(6)=8$, and $6(7)=12$

(b) 4. $4^2=1$

(c) $\{1,2,3,4,5,6\}$ is Abelian subgroup. Know it is a subgroup b/c all $1 \to 6$ in upper left.

Should b with #1

(d) $\{3,8,10,12,5,1\}$

3. (8 points) (a) Let H be the subgroup of S_6 (S_6 =the group of permutations of 6 elements) where H is defined by

$$H = \{\alpha \in S_6 \,|\, \alpha(5) = 5\}$$

In other words, H is the subset of elements in S_6 that send 5 to itself. Prove that H is a subgroup of S_6.

Since $H \subset S_6$, H is finite, thus can do finite subgroup test. Let $\alpha, \beta \in H$. Then $\alpha(5)=5$ and $\beta(5)=5$.

Then $\alpha\beta(5) = \alpha(\beta(5)) = \alpha(5) = 5$

So $\alpha\beta \in H$

$\blacksquare$

-0.5 if poorly written but proof is solid

(b) Let J be the subgroup of S_6 where J is defined by

$$J = \{\beta \in S_6 \,|\, \beta(3) = 4\}$$

In other words, J is the subset of elements in S_6 that send 3 to 4. Is J a subgroup of S_6? If so, prove it. If not, explain why not.

J is not a subgroup because the identity is not in J. (Also fails closure, inverses)

-0.5 if say not closed b/c $\beta(3)=4$ and don't know what $\alpha(4)$ is.

4. (7 points) (a) Let G be the set of elements of the form $ax + b$, where x is a variable and $a, b \in \mathbb{Z}_{101}$ (Note that 101 is a prime number, which you can use without proof). Assuming we use the binary operation ^of addition modulo 101, prove that G is a group.

- Closure: $(ax+b) + (cx+d) = (a+c)x + (b+d)$. When you do $a+c \pmod{101}$ and $b+d \pmod{101}$, get coefficients in $\mathbb{Z}_{101}$, so has right form.

- Identity: $0 \in G$, $0x + 0$.

- Inverses: Let $ax+b \in G$. Then $(101-a)x + (101-b)$ is an inverse for $ax+b$ b/c $(ax+b) + (101-a)x + (101-b) =$

$$101x + 101 = 0x + 0 \pmod{101} = 0.$$

5

- Associativity. Since addition is component-wise, associativity will follow from associativity of $\mathbb{Z}_{101}$ (or $\mathbb{Z}$).

+4 for all four, with attempt. −0.5 for each faulty reasoning.

(b) Is the group G a cyclic group? If so, what is it generated by? If not, explain why not (do not need a full proof).

1

Not cyclic. $|G| = (101)(101)$, but each element $\alpha \in G$ will have order 101. Suppose $\alpha = ax+b$. Then

$$\alpha^{101} = 101(\alpha) = 101(ax+b) = (101a)x + 101b$$

b/c additive group

+1 for Not,

−0.5 if say yes it is.

$101a \equiv 0 \pmod{101}$ and $101b \equiv 0 \pmod{101}$

$\Rightarrow \alpha^{101} = 0 \Rightarrow |\alpha| = 101 \neq 101^2$ ∎

↳ Can still get 0.5 for some reasoning.

5. (5 points) (a) Find all generators of $\mathbb{Z}_{20}$.

Need all elements relatively prime to (and less than) 20.

$\Rightarrow$ 1, 3, 7, 9, 11, 13, 17, 19 $\boxed{}$

2

(b) Find all generators of $U(18)$ (recall that $U(n)$ is the group of positive integers less than n that are relatively prime to n).

$13 \cdot 7 = 91$

$U(18) = \{1, 5, 7, 11, 13, 17\}$

2

$\langle 5 \rangle = \{5, 7, 17, 13, 11, 1\}$ $\Rightarrow$ 5 is a generator

$\langle 7 \rangle = \{7, 13, 1\}$ $\Rightarrow$ 7, 13 not generators

$17^2 = 289$

$\langle 17 \rangle = \{17, 1\}$ $\Rightarrow$ 17 not a generator

~~$\langle 11 \rangle$~~ 11 is generator because 5, 11 are inverses.

So $\boxed{5, 11}$

(c) Why is $\mathbb{Z}_{20}$ not a group if the binary operation is multiplication modulo 20?

because $0 \in \mathbb{Z}_{20}$ but 0 will not have

1 an inverse b/c $0 \cdot \_\_ = 0$ (not 1).

Also not closed, 2, 4, 5, etc also don't have inverses.

6. (5 points) Choose one of the following proofs to do (you do NOT have to do both):

- Let G be a group. Prove that $Z(G)$, the *center* of a group, is always a subgroup of G. (Recall that the center of a group is the set of all elements in G that commute with every element of G).
- Prove the right cancellation property for a group G. That is, prove that for all $a, b, c \in G$, $ba = ca$ implies that $b = c$.

$$Z(G) = \{g \in G \mid ga = ag \quad \forall\, a \in G\}$$

· Nonempty b/c $e \in Z(G)$.

Two steps: Let $a, b \in Z(G)$. Then $\forall\ h \in G$,

$$(ab)(h) = ahb = hab = h(ab)$$

b/c $b \in Z(G)$ b/c $a \in Z(G)$

$$\Longrightarrow ab \in Z(G)$$

Inverse: Let $a \in Z(G)$. Then $\forall\ h \in G$ $\quad ah = ha$

$$ah = ha \iff a^{-1}aha^{-1} = a^{-1}haa^{-1} \iff ha^{-1} = a^{-1}h \quad \forall h \in H$$

$$\Rightarrow a^{-1} \in Z(G)$$

$$ba = ca \iff (ba)a^{-1} = (ca)a^{-1}$$

(Know a^{-1} exists b/c group

$$\Longrightarrow b = c$$

Extra Credit(1 point) Prove that a group of order 4 cannot have a subgroup of order 3 (Hint: use a Cayley table). Prove by contradiction:

Suppose $G = \{e, a, b, c\}$ with $\{e, a, b\}$ a subgroup. Then

Cayley table for e, a, b must be:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

adding in c gets

	e	a	b	c
e	e	a	b	c
a	a	b	e	
b	b	e	a	
c	c			

No c in this row $\Rightarrow$ open space must be a c, but that gives two c's in one column. $\Rightarrow\Leftarrow$