

MATH 30A FALL 04

QUIZZES AND PRACTICE QUIZZES

There were 2 quizzes and 6 practice quizzes given in class. This course covered group theory up through Sylow Theorems and some rings and fields.

PRACTICE QUIZ

There were two problems.

1. Suppose that $(A, *)$, $(B, *)$ are binary structures and $\phi : A \rightarrow B$ is a mapping which is onto and preserves the multiplication. Suppose that A is commutative. Then is B necessarily commutative?

The answer is Yes. Suppose that $a, b \in B$. Since ϕ is onto, there are elements $x, y \in A$ which map to a, b respectively. Then

$$a * b = \phi(x) * \phi(y) = \phi(x * y) = \phi(y * x) = \phi(y) * \phi(x) = b * a.$$

Therefore, B is commutative.

2. Suppose that $*$ is an associative binary operation on a set A . Then show that $\bar{*}$ is associative where $x\bar{*}y = y * x$

Take any $a, b, c \in A$. Then

$$(a\bar{*}b)\bar{*}c = c * (b * a) = (c * b) * a = a\bar{*}(b\bar{*}c)$$

So, $\bar{*}$ is also associative.

ANSWERS TO PRACTICE QUIZ 4

Quiz Wednesday on sections 0-4. Closed book. Bring ONE page (letter sized) of notes.

0. Does there exist a binary structure on the empty set? Is there a group with no elements?

Yes, there is a unique mapping

$$* : \emptyset \times \emptyset \rightarrow \emptyset$$

making the empty set into a binary structure. However, a group must have at least one element e .

1. Give an example of two binary structures on the set $\{0, 1\}$, one which is a group and one which is not.

You did this in your homework. There are 16 binary structures on $\{0, 1\}$ and exactly two of them are group structures. The strange group structure is $a * b = 1$ if $a = b$ and $a * b = 0$ if $a \neq b$. There are lots of non-group structures, such as the left hand rule: $a * b = a$.

2. Give an example of a group which is not commutative.

$GL(2, \mathbb{Z})$ is not commutative.

3. What is the definition of a binary operation? What is the binary operation?

A binary operation on a set S is a mapping

$$* : S \times S \rightarrow S$$

The mapping is the operation. Strictly speaking, a mapping is a set of ordered pairs. In this case it is:

$$\{(a, b), c \in (S \times S) \times S \mid c = a * b\}$$

Cartesian product is not associative. However, most mathematicians choose to ignore this technicality and pretend that it is.

4. Write down all the theorems we learned.

Some important theorems are

- a. $(U_n, \cdot) \cong (\mathbb{Z}_n, +)$
- b. $(U, \cdot) \cong (\mathbb{R}_{2\pi}, +)$
- c. The unit and inverse are unique if they exist.
- d. Commutativity is a structural property of groups.

5. If G is a group and $a, b \in G$ then prove that $(ab)^{-1} = b^{-1}a^{-1}$.

Let $x = (ab)^{-1}$ and $y = b^{-1}a^{-1}$. Then we will show that $x = y$.

By definition of inverse we have:

$$abx = e$$

We also have:

$$aby = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$$

Since $abx = aby$ we conclude by left cancellation that $x = y$ as claimed.

6. Let $G = \mathbb{Z}$ with the binary operation \oplus defined by

$$a \oplus b := a + b + 1$$

Then prove that (G, \oplus) is a group.

First note that $a + b + 1$ is always an integer. So $G = \mathbb{Z}$ is closed under this operation. Next we need to verify the three axioms. So, let a, b, c be integers.

(1) (Associativity)

$$(a \oplus b) \oplus c = (a + b + 1) + c + 1 = a + b + c + 2$$

$$a \oplus (b \oplus c) = a + (b + c + 1) + 1 = a + b + c + 2$$

So, \oplus is associative.

(2) (unit) I claim that $e = -1$ is the unit. Indeed, for all $x \in \mathbb{Z}$ we have:

$$x \oplus (-1) = x + (-1) + 1 = x.$$

(3) (inverse) The inverse of x is $-x - 2$. Here is the proof:

$$x \oplus (-x - 2) = x + (-x - 2) + 1 = -1 = e$$

Therefore, (\mathbb{Z}, \oplus) is a group. I was careful to verified that we have a *right* unit and a *right* inverse. This is because some definitions of a group only assume the existence of a right unit and right inverses. In this case, the operation \oplus is obviously commutative because the expression $a + b + 1$ remains unchanged when a, b are switched. So it doesn't really matter.

PRACTICE QUIZ

1. Give an example of a group G and a subgroup H so that the left cosets of H are not equal to the right cosets. Write down the cosets.
2. Give an example of a finite group G of order n and a number d dividing n so that G does not have an element of order d .
- 3 Show that if G has an element of order 15 then it also has elements of order 3 and 5.
- 4 Find a group G which has elements of order 3 and 5 but no elements of order 15.
- 5 If S_5 acts on a set X with 7 elements, is there necessarily a singleton orbit?
- 6 Give an example of a homomorphism $\phi : \mathbb{Z} \rightarrow G$ whose kernel is $3\mathbb{Z}$.
- 7 Show that the composition of two homomorphisms is a homomorphism.

PRACTICE QUIZ

1. Give an example of a group G and a subgroup H so that the left cosets of H are not equal to the right cosets. Write down the cosets.

The example we did in class was $G = S_3$ with $H = \langle (12) \rangle = \{e, (12)\}$. The left cosets of H are

$$H, \quad (123)H = \{(123), (13)\}, \quad (132)H = \{(132), (23)\}$$

The right cosets are:

$$H, \quad H(123) = \{(123), (23)\}, \quad H(132) = \{(132), (13)\}$$

2. Give an example of a finite group G of order n and a number d dividing n so that G does not have an element of order d .

The group $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ has order $n = 8$ and $d = 8$ divides 8 but G does not have an element of order 8. To see this note that

$$4(a, b) = (4a, 4b) = (0, 0)$$

for all $(a, b) \in \mathbb{Z}_4 \times \mathbb{Z}_2$ making the order of each element at most 4.

3 Show that if G has an element of order 15 then it also has elements of order 3 and 5.

If $a \in G$ has order 15 then a^3 has order 5 and a^5 has order 3.

There is also another argument assuming that G is finite. If G has order 15 then 15 divides n , the order of the group. But then n must be divisible by 3 and 5. Since these numbers are prime, Cauchy's Theorem implies that G has elements of order 3 and 5. This is not such a great proof since it uses "overkill," the use of very complicated theorems to prove an easy theorem. Also it assumes that G is finite, which is not given.

4 Find a group G which has elements of order 3 and 5 but no elements of order 15.

The group S_5 has elements $g = (123)$ and $h = (12345)$ of order 3,5 resp. However, it does not have elements of order greater than 6 since the only cycle types are:

$$e, (ab), (abc), (abcd), (abcde), (ab)(cd), (ab)(cde)$$

which have order 1,2,3,4,5,2,6 resp.

5 If S_5 acts on a set X with 7 elements, is there necessarily a singleton orbit?

No, X could be the set $X = \{1, 2, 3, 4, 5, \text{odd}, \text{even}\}$ with two orbits of size 5 and 2. S_5 could act on the five numbers by permutation in the usual way and it could act on the last two elements according to sign, i.e., $g(\text{even}) = \text{even}$ and $g(\text{odd}) = \text{odd}$ if g is even, $g(\text{even}) = \text{odd}$ and $g(\text{odd}) = \text{even}$ if g is odd.

6 Give an example of a homomorphism $\phi : \mathbb{Z} \rightarrow G$ whose kernel is $3\mathbb{Z}$.

Let $\phi : \mathbb{Z} \rightarrow S_3$ be given by $\phi(n) = (123)^n$. This is a homomorphism since

$$\phi(n + m) = (123)^{n+m} = (123)^n(123)^m = \phi(n)\phi(m)$$

The kernel of ϕ is

$$\ker \phi = \{n \mid (123)^n = e\} = 3\mathbb{Z}$$

as required.

7 Show that the composition of two homomorphisms is a homomorphism.

Suppose that $\phi : G \rightarrow H$ and $\psi : H \rightarrow K$ are group homomorphisms. Note that the words *group homomorphism* imply that G, H, K are groups. Then for all $a, b \in G$ we have

$$\psi\phi(ab) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b))$$

Therefore, $\psi \circ \phi$ is a homomorphism of groups.

PRACTICE QUIZ 6

1. H a subgroup of G . Two elements a, b in G . If $aH \neq bH$ then show $H(a^{-1}) \neq H(b^{-1})$.

Two cosets aH, bH are equal iff $b^{-1}a \in H$. This was proved in class and I am sure it is in the book somewhere. But, if not:

$$aH = bH \iff b^{-1}aH = H \iff b^{-1}a \in H$$

Similarly, $Hc = Hd$ iff $cd^{-1} \in H$. ($Hc = Hd \iff Hcd^{-1} = H \iff cd^{-1} \in H$.) So, aH, bH are not equal iff $b^{-1}a \notin H$. If we let $c = b^{-1}, d = a^{-1}$ then $cd^{-1} = b^{-1}a \notin H$ which implies that $Hc \neq Hd$ or: $Hb^{-1} \neq Ha^{-1}$.

2. If K a subgroup of H and H a subgroup of G . then show each left coset of K is contained in some left coset of H .

Any left coset aK of K is contained in the left coset aH .

3. Find an example of a nonabelian group G of order pq where p, q are prime and $pq \neq 6$.

The dihedral group of order 10 is nonabelian. This is the subgroup of S_5 generated by $t = (12345)$ and $s = (25)(34)$. To see that this formula is correct, use the geometric description of the dihedral group. It is the group of symmetries of the regular n -gon. In this case it is the pentagon with vertices 1, 2, 3, 4, 5. The reflection across the axis which goes through the vertex 1 and through the opposite edge 3 – 4 switches 3, 4 and also switches 2, 5. So, it is $s = (25)(34)$.

4. Find 2 examples of a group of order p^3 which is not cyclic.

They are: $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$.

There are also two nonabelian groups of order p^3 making a total of exactly five groups of order p^3 for each prime p . This will be a topic for next semester.

5. Find an example of a finite group acting on an infinite set.

The simplest example is the trivial group which acts on any set in a unique way. For a nontrivial example, take $G = \mathbb{Z}_2$ acting on $X = \mathbb{Z}$ by

$$g \cdot x = (-1)^g x.$$

6. Find an example of an infinite group acting on a finite set.

Any group has a trivial action on any set by

$$g \cdot x = x \quad \forall g \in G, x \in X$$

A nontrivial example is $G = \mathbb{Z}$, $X = \mathbb{Z}_n$ with action

$$g \cdot x = gx \text{ modulo } n$$

7. If $\phi : G \rightarrow H$ is a homomorphism and X is an H -set show X is a G -set in a "natural way" (the orbits are the same).

The natural action is given by

$$g \cdot x = \phi(g)x$$

Here is the proof that this is an action:

$$(1) e \cdot x = \phi(e)x = ex = x.$$

$$(2) (gh) \cdot x = \phi(gh)x = \phi(g)\phi(h)x = \phi(g)(hx) = g(hx).$$

7.5 What is the relation between the two stabilizers that you get for the same element of X ?

The relation is that $G_x = \phi^{-1}H_x$. In words, the stabilizer of x in G is the inverse image under the mapping ϕ of the stabilizer of x in H . To see this note first that if $g \in \phi^{-1}(H_x)$ then

$$g \cdot x = \phi(g)x = x$$

since $\phi(g)$ is in the stabilizer of x . Conversely, if g stabilizes x then,

$$g \cdot x = x = \phi(g)x$$

So, $h = \phi(g) \in H$ stabilizes x and $g \in \phi^{-1}(h) \subseteq \phi^{-1}(H_x)$.

ANSWERS TO QUIZ I

20 minutes. Closed book. ONE page (letter sized) of notes allowed.

1. Give an example of a monoid M which is not a group and explain why. [Why is M a monoid? Why is it not a group?]

Here are a couple of answers.

Take $M = \mathbb{Z}_+$ under multiplication. The product of two positive integers is positive So \mathbb{Z}_+ is closed. (\mathbb{Z}_+, \cdot) is associative since multiplication is of integers is associative. $1 \in \mathbb{Z}_+$ is the multiplicative unit. So (\mathbb{Z}_+, \cdot) is a monoid. It is not a group since it does not have inverses of all of its elements. For example 2 does not have an inverse since $1/2 \notin \mathbb{Z}_+$.

Another example is $(\mathbb{N}, +)$. \mathbb{N} is closed under addition. Addition is associative and $0 \in \mathbb{N}$ is the unit. So, $(\mathbb{N}, +)$ is a monoid. It is not a group since not all elements have inverses. For example, the inverse of 1 is -1 which is not in \mathbb{N} .

2. Give an example of a binary structure which is not a semigroup and explain why. [Why is it a binary structure? Why is it not a semigroup?]

There are various natural operations one could take. One could also define an ad hoc structure on a set with two elements.

- (1) Take $(\mathbb{Z}, -)$. Since the difference of two integers is an integer, \mathbb{Z} is closed under $-$ and $(\mathbb{Z}, -)$ is a binary structure. It is not associative since, e.g.,

$$(1 - 2) - 3 = -4 \neq 1 - (2 - 3) = 0.$$

- (2) Take $(\mathbb{Z}_+, *)$ where $a * b = a^b$. Since $a, b > 0$, a^b is a positive integer so the set \mathbb{Z}_+ is closed under this operation (exponentiation) and we have a binary structure.

$$(2 * 1) * 2 = 2^2 = 4 \neq 2 * (1 * 2) = 2^1 = 2.$$

- (3) Take positive real number under division.
- (4) Take some stupid function like $a * b = 2a + b - ab$.

3. State your favorite theorem. Make sure the statement is precise. [No proof.]

1. A binary structure can have at most one two-sided unit.
2. Any two groups of order 2 are isomorphic.
3. Every group with 4 elements is abelian.

4a. If $(S, *)$ is a set with a binary operation, what is the definition of a *structural property* of $(S, *)$?

A structural property of $(S, *)$ is a property which is shared by all isomorphic structures.

4b. Give an example of two isomorphic groups A and B and a property of A which is not a property of B .

By definition, any structural property of A must also be a property of B . So this question is asking for a *nonstructural* property of A .

1. The group of positive real number under multiplication is isomorphic to the additive group of all real numbers. The elements of the first group are all positive.

2. $(\mathbb{Z}_4, +) \cong (U_4, \cdot)$. The first group is a set of integers. The second is not.

QUIZ 2 ANSWERS

Open book and notes.

1. True or False. Give explanation.

- (1) A group of order 12 has an element of order 2. **True by Cauchy.**
- (2) A group of order 27 has an element of order 9. **False. The group $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ has no element of order 9**
- (3) If G has elements of order 2,3,4,5 then G has at least 120 elements. **False. The group $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$ has order 60 and it has elements of order 2,3,4,5**

2 Let $a, b \in GL(2, \mathbb{Z})$ be the matrices:

$$a = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Find the orders of a, b and ab .

a has order 3, b has order 4 and

$$ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

has infinite order.

3 Give an explicit isomorphism

$$\phi : \mathbb{Z}_6 \xrightarrow{\cong} \mathbb{Z}_2 \times \mathbb{Z}_3$$

Let $\phi(x) = (x, x)$. This is obviously a homomorphism since

$$\phi(x + y) = (x + y, x + y) = (x, x) + (y, y) = \phi(x)\phi(y)$$

Also, calculation shows that it is a bijection:

$$\phi(0) = (0, 0)$$

$$\phi(1) = (1, 1)$$

$$\phi(2) = (0, 2)$$

$$\phi(3) = (1, 0)$$

$$\phi(4) = (0, 1)$$

$$\phi(5) = (1, 2)$$

There are exactly two correct answers to this question. The other correct answer is $\psi(x) = (-x, -x)$

$$\psi(0) = (0, 0)$$

$$\psi(1) = (1, 2)$$

$$\psi(2) = (0, 1)$$

$$\psi(3) = (1, 0)$$

$$\psi(4) = (0, 2)$$

$$\psi(5) = (1, 1)$$

(The number of possible isomorphisms is the Euler ϕ function which in this case is $\phi(6) = 2$.) **4** Find a group G and a homomorphism

$$\phi : S_3 \rightarrow G$$

whose kernel is A_3 . (S_3 is the symmetric group, A_3 is the alternating group on 3 letters)

Let $\phi(\sigma)$ be the sign of σ . This is ± 1 in the multiplicative group $G = \{1, -1\}$. In class we defined the homomorphism

$$\phi : S_n \rightarrow \mathbb{Z}_2$$

which is zero on even permutations and 1 on odd permutations. The kernel is A_n by definition.

5 A cyclic group G of order 5 acts on a set X with exactly 5 elements. If there are $g \in G$ and $x \in X$ so that $gx \neq x$ then show that the action is transitive (i.e., has only one orbit).

The size of the orbit of x divides the order of the group. So it is either 1 or 5. If $gx \neq x$ then x is not a singleton orbit. So the orbit size is not 1. It must be 5. So the orbit is the entire set X and the action is transitive.

6 Suppose that H is a subgroup of G and $g \in G$, $g \notin H$ so that the order of g is 3. Then prove that the index of H in G is at least 3.

The group $\langle g \rangle$ acts on the set of left cosets of H in G by left multiplication. If $gH \neq H$ then H is not a fixed point. So the orbit size must be 3. This orbit consists of three distinct left cosets of H in G . So the index is at least 3.

Here is another proof. The left cosets H, gH, g^2H must be distinct. The reason is:

- (1) $H \neq gH$ since $g \notin H$.
- (2) $gH \neq g^2H$ since if these were equal we could multiply by g^{-1} and get $H = gH$ which is a contradiction.

- (3) $g^2H \neq H$ since if these were equal we could multiply both by g and get $H = gH$ which is again a contradiction.

7 Look at the Cayley graph on the board. What is the group G and what are the generators a (solid arrows) and b (dotted lines).?

The group has four elements and its is generated by a since you can get from one point to another by going along the arrows a . So,

$$G = \langle a \rangle = \{e, a, a^2, a^3\} \cong \mathbb{Z}_4$$

The element b must be a^2 since it does the same as going on two arrows labeled a .