§1	§2	§3	style	total

Math 415 Examination 1 Fall 2006

Modern Algebra I

Please print your **name**: Answer Key

1 True/false

Circle the correct answer; no explanation is required. Each problem in this section counts 5 points.

1. The binary operation $*$ defined on the real numbers $\mathbb{R}$ by the rule $x * y = \sin(x + y)$ for all x and y is commutative but not associative.
   `True False`

   Solution. True. The operation is commutative because $\sin(x + y) = \sin(y + x)$ for all x and y. The operation is not associative because $(x * y) * z = \sin(x + y) * z = \sin(\sin(x + y) + z)$, but $x * (y * z) = \sin(x + (y * z)) = \sin(x + \sin(y + z))$, and these two expressions are not identically equal. For instance, when $x = \frac{\pi}{2}$, $y = \frac{\pi}{2}$, and $z = 0$, the first expression becomes $\sin(\sin(\pi))$, which equals 0; and the second expression becomes $\sin(\frac{\pi}{2} + 1)$, which does not equal 0.

2. The set of complex numbers z such that $z^4 = 16$ is a group under multiplication. `True False`

   Solution. False: $2^4 = 16$ and $(-2)^4 = 16$, but $(2 \times (-2))^4 = 256 \neq 16$. The set is not closed under multiplication, so the set does not form a group under multiplication. What is true is that the set of complex numbers z such that $z^4 = 1$ is a group under multiplication.

3. Every finite group is cyclic. `True False`

   Solution. False: the Klein 4-group is an example of a finite non-cyclic group.

4. Consider the following relation defined on the set of current Texas A&M students:

   > A is related to B if A and B are enrolled in the same mathematics class.

This relation is an equivalence relation. `True` `False`

Solution. False. The relation is not reflexive, because if student A is not enrolled in any mathematics class, then A is not related to A. Also, the relation is not transitive: A and B may be enrolled in Math 415, while B and C may be enrolled in Math 409, but A and C need not be enrolled in a common mathematics class.

5. The two tables below are the group tables of two groups G and H.

G	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

H	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	f	e	d	c	a
c	c	d	f	e	a	b
d	d	c	a	b	f	e
f	f	b	c	a	e	d

The groups G and H are isomorphic groups. `True` `False`

Solution. False. In the group G, there are exactly two elements whose square equals the identity, while in the group H, there are four elements whose square equals the identity. The number of elements whose square equals the identity is a structural property that must be preserved by an isomorphism.

2 Short answer

Fill in the blanks; no explanation is required. Each problem in this section counts 5 points.

6. If $+_{12}$ denotes addition modulo 12, then $11 +_{12} 8 = 7$.

7. The greatest common divisor of 42 and 60 equals 6.

8. How many subgroups does the cyclic group $\mathbb{Z}_6$ have? (Include in your count both the improper subgroup and the trivial subgroup.)

Solution. There are 4 different subgroups of $\mathbb{Z}_6$.

Subgroups of cyclic groups are cyclic, and here is a complete list of cyclic subgroups of $\mathbb{Z}_6$.

$\langle 0 \rangle$ is the trivial subgroup consisting of the single element 0.

$\langle 1 \rangle$ is the improper subgroup, $\mathbb{Z}_6$ itself.

$\langle 2 \rangle$ is a subgroup of order 3 consisting of the elements 0, 2, and 4.

$\langle 3 \rangle$ is a subgroup of order 2 consisting of the elements 0 and 3.

$\langle 4 \rangle$ is the same subgroup as $\langle 2 \rangle$.

$\langle 5 \rangle$ is the same subgroup as $\langle 1 \rangle$, namely the improper subgroup.

9. The subset $\{4, 6\}$ of the cyclic group $\mathbb{Z}_{12}$ generates a subgroup of $\mathbb{Z}_{12}$ of order 6.

   Solution. The subgroup generated by 4 and 6 is the same as the cyclic subgroup generated by 2 (since $\gcd(4, 6) = 2$). Therefore the subgroup has order 6.

10. The partially completed table below represents a binary operation $*$ on the set $\{a, b, c, d\}$. Fill in the table to make the operation $*$ both commutative and associative. (There is a unique solution.)

$*$	a	b	c	d
a				
b		b	a	b
c		a	c	c
d		b	c	d

Solution. Observe that $a = b * c$. Therefore $b * a = b * (b * c)$. If the binary operation is associative, then $b * (b * c) = (b * b) * c$. From the table, $(b * b) * c = b * c = a$. Thus $b * a = a$. If the binary operation is commutative, then also $a * b = a$.

A similar analysis shows that $a * c = (b * c) * c = b * (c * c) = b * c = a$, and by commutativity $c * a = a$ as well.

Moreover, $a * d = (b * c) * d = b * (c * d) = b * c = a$, and $d * a = a$ too.

Finally, $a * a = a * (b * c) = (a * b) * c$. Since it has already been determined that $a * b = a$, the expression $(a * b) * c$ reduces to $a * c$, and this is known already to equal a. Thus $a * a = a$.

In conclusion, all the missing entries of the table must be filled in with the letter a if the operation is to be both associative and commutative.

3 Essay questions

In the following problems, you must give an explanation. (Continue on the back if you need more space.) Each problem counts 15 points. In addition, this section as a whole carries 5 style points based on how well your solutions are written.

11. Let G be an abelian group (written multiplicatively). Let H be the subset of G consisting of all squares of elements of G: in symbols, $H = \{ x^2 \mid x \in G \}$. Prove that H is a subgroup of G.

    Solution. One has to check three properties: (i) the subset H is closed under the group operation of G; (ii) the identity element e of G is an element of H; and (iii) the inverse of every element of H is again an element of H.

    To check the first property, consider two arbitrary elements a and b of H. We need to show that $ab \in H$. By the definition of H, there exist elements x and y of G such that $a = x^2$ and $b = y^2$. Then $ab = x^2y^2 = xxyy$. Because G is an abelian group, $xxyy = xyxy = (xy)^2$. Thus ab is equal to the square of the element xy of G, so $ab \in H$ by the defining property of H.

    The identity element e of G has the property that $ex = x$ for every element x of G. In particular, $ee = e$. Thus e is a square (namely e^2), so $e \in H$ by the defining property of H. Thus property (ii) holds.

    To check property (iii), consider an arbitrary element a of H. We need to show that $a^{-1} \in H$. By the definition of H, there exists an element x in G such that $a = xx$. Now $x^{-1}x^{-1}a = x^{-1}x^{-1}xx = x^{-1}ex = e$, so

$a^{-1} = x^{-1}x^{-1}$. In other words, a^{-1} is a square (namely $(x^{-1})^2$), so $a^{-1} \in H$ by the defining property of H.

Having verified all three properties (i), (ii), and (iii), one concludes that H is a subgroup of G.

12. The real numbers $\mathbb{R}$ form a group under addition; the positive real numbers $\mathbb{R}^+$ form a group under multiplication. Show that the map φ defined by $\varphi(x) = 2^x$ gives an isomorphism between $\langle \mathbb{R}, + \rangle$ and $\langle \mathbb{R}^+, \cdot \rangle$.

    Solution. One has to check three properties: (i) the map φ is one-to-one; (ii) the map φ is onto; and (iii) the map φ is a homomorphism, that is, $\varphi(x + y) = \varphi(x) \cdot \varphi(y)$ for all x and y.

    Property (i) holds because the function 2^x is a strictly increasing function: if $x < y$, then $2^x < 2^y$. Consequently, $2^x = 2^y$ only if $x = y$.

    Property (ii) holds because the function 2^x has an inverse function, namely the base 2 logarithm. Thus if y is an arbitrary element of $\mathbb{R}^+$, there is an element x of $\mathbb{R}$ such that $2^x = y$: namely $x = \log_2 y$.

    To check property (iii), observe that $\varphi(x+y) = 2^{x+y}$, while $\varphi(x)\cdot\varphi(y) = 2^x \cdot 2^y$. The two expressions are indeed equal by the laws of exponents. Thus φ is a homomorphism.

    Having verified all three properties (i), (ii), and (iii), one concludes that φ is an isomorphism.

13. Let S be a non-empty set, and let $\mathcal{P}(S)$ denote the *power set* of S: namely, the collection of all subsets of S. (In particular, the empty set $\varnothing$ is an element of the power set $\mathcal{P}(S)$, and so is the whole set S itself.) Equip the power set $\mathcal{P}(S)$ with the binary operation of *union*. (If A and B are subsets of S, then so is their union $A \cup B$.)

    Is $\langle \mathcal{P}(S), \cup \rangle$ a group? Explain why or why not.

    Solution. Method 1 (applying a theorem). If $\langle \mathcal{P}(S), \cup \rangle$ were a group, then there would be a left cancellation law. Now $S \cup S = S \cup \varnothing$ (since both sides of the equation are equal to S), so cancelling on the left implies that $S = \varnothing$, contrary to the hypothesis. This contradiction shows that $\langle \mathcal{P}(S), \cup \rangle$ cannot be a group after all.

Modern Algebra I

Method 2 (applying the definition). A group should have an associative binary operation, there should be an identity element for the operation, and each element should have an inverse element. The third property is lacking here, so $\langle \mathcal{P}(S), \cup \rangle$ is not a group. Here are more details.

Taking unions is an associative operation: $A \cup (B \cup C) = (A \cup B) \cup C$. (Both expressions represent the set whose elements belong to at least one of the sets A, B, and C.)

Since $\varnothing \cup A = A = A \cup \varnothing$ for every set A, the element $\varnothing$ of the power set is an identity element for the operation of taking the union.

Inverses are missing, however. Indeed, for A and B to be inverse elements in $\langle \mathcal{P}(S), \cup \rangle$ means that $A \cup B = \varnothing$ (since we have previously identified $\varnothing$ as the identity element for $\cup$). Because A and B both are subsets of $A \cup B$, the only way that $A \cup B$ can equal $\varnothing$ is for A and B both to equal $\varnothing$. Thus the *only* element of $\langle \mathcal{P}(S), \cup \rangle$ that has an inverse element is $\varnothing$.

Consequently, $\langle \mathcal{P}(S), \cup \rangle$ is a group only if $\langle \mathcal{P}(S), \cup \rangle$ is the trivial group whose only element is $\varnothing$. By hypothesis, however, S is not the empty set, so $\langle \mathcal{P}(S), \cup \rangle$ has at least one element besides $\varnothing$ (namely, S itself).

In summary, since $\langle \mathcal{P}(S), \cup \rangle$ has at least one element that does not have an inverse element, $\langle \mathcal{P}(S), \cup \rangle$ is not a group.