# Math 350, Fall 2007
# Midterm 1 Review Solutions

(1) Prove that, for all sets $A$, $B$, $C$, we have $(A\backslash B) \cap C = (A \cap C)\backslash(B \cap C)$.

*Solution:* First suppose that $x \in (A\backslash B) \cap C$. Then $x \in A\backslash B$ and $x \in C$. Hence $x \in A$ and $x \notin B$ and $x \in C$. Hence $x \in A \cap C$ but $x \notin B \cap C$. Hence $x \in (A \cap C)\backslash(B \cap C)$. Conversely, suppose that $x \in (A \cap C)\backslash(B \cap C)$. Then $x \in A \cap C$ but $x \notin B \cap C$. Hence $x \in A$ and $x \in C$. Since $x \notin B \cap C$, then $x \notin B$ or $x \notin C$. Since $x \in C$, we conclude that $x \notin B$. Therefore $x \in A\backslash B$, and so $x \in (A\backslash B) \cap C$.

(2) Construct a Cayley table for the set $\{1, -1, i, -i\}$, where $i$ is the complex number with $i^2 = -1$. The operation is multiplication.

*Solution:*

| | $1$ | $-1$ | $i$ | $-i$ |
|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ |

(3) Consider a vector space $V$ over $\mathbb{R}$, and let $L(V)$ be the collection of all linear transformations $T\colon V \to V$. Recall that $T\colon V \to V$ is a linear transformation if $T(cv + w) = cT(v) + T(w)$ for all $c \in \mathbb{R}$ and $v, w \in V$.
  (a) Prove that the identity function on $V$ belongs to $L(V)$ and is the identity element for $(L(V), \circ)$.
  (b) Prove that composition $\circ$ is an operation on $L(V)$.

*Solution:*
  (a) Let $I\colon V \to V$ be defined by setting $I(v) = v$ for all $v \in V$. Then, for all $c \in \mathbb{R}$ and $v, w \in V$, we have $I(cv + w) = cv + w = cI(v) + I(w)$. Hence $I$ is a linear transformation (so $L(V)$ is nonempty). Also, it is clear that $I \circ S = S \circ I = S$ for all $S \in L(V)$, so $I$ is the identity element of $L(V)$.
  (b) Let $S, T \in L(V)$, and let $c \in \mathbb{R}$ and $v, w \in V$. Then $(S \circ T)(cv + w) = S(cT(v) + T(w)) = cS(T(v)) + S(T(w)) = c(S \circ T)(v) + (S \circ T)(w)$. Hence $S \circ T$ is a linear transformation on $V$. Therefore $\circ$ is an operation on $L(V)$.

(4) For each of the following, determine with proof whether or not it is a group.
  (a) $(G, \cdot)$ where $G = \{2^m 3^n : m, n \in \mathbb{Z}\}$ and $\cdot$ is the usual multiplication on real numbers.
  (b) $(G, +)$ where $G = \{a + b\sqrt{2} \colon a, b \in \mathbb{Z}\}$ and $+$ is the usual addition of real numbers.

*Solution:*
  (a) Certainly if $2^m 3^n$ and $2^p 3^q$ lie in $G$ (with $m, n, p, q \in \mathbb{Z}$), then the product $2^{m+p} 3^{n+q}$ also lies in $G$. The identity element is $2^0 3^0 = 1$. Multiplication is certainly associative on $G$. For all $m, n \in \mathbb{Z}$, the inverse of the element $2^m 3^n$ is $2^{-m} 3^{-n}$. Hence $(G, \cdot)$ is a group.
  (b) If $a + b\sqrt{2}$ and $c + d\sqrt{2}$ (with $a, b, c, d \in \mathbb{Z}$) lie in $G$, then the sum $(a + c) + (b + d)\sqrt{2}$ also lies in $G$. The identity element is $0 = 0 + 0\sqrt{2}$. Addition is certainly associative on $G$. For all $a, b \in \mathbb{Z}$, the inverse of $a + b\sqrt{2}$ is $(-a) + (-b)\sqrt{2}$. Hence $(G, +)$ is a group.

(5) Let $G$ be a group and let $a \in G$ be a fixed element. Define the function $\lambda_a \colon G \to G$ given by $\lambda_a(g) = ag$ for all $g \in G$. Prove that $\lambda_a$ is a bijection.

*Solution:* Suppose that $g, h \in G$ and $\lambda_a(g) = \lambda_a(h)$. Then $ag = ah$, so $g = h$. Hence $\lambda_a$ is injective. Also, if $h \in G$, then let $g = a^{-1}h$. Hence $\lambda_a(g) = h$, so $\lambda_a$ is surjective.

(6) Prove that $A_n$ is nonabelian if $n > 3$. Write out the Cayley table for $A_3$.

*Solution:* Since $(123)(124) \neq (124)(123)$ in $A_n$, it follows that $A_n$ is nonabelian. The Cayley table for $A_3$ is

| $A_3$ | $e$ | $(123)$ | $(132)$ |
|---|---|---|---|
| $e$ | $e$ | $(123)$ | $(132)$ |
| $(123)$ | $(123)$ | $(132)$ | $e$ |
| $(132)$ | $(132)$ | $e$ | $(123)$ |

(7) Determine with proof whether or not the set $\{\alpha \in S_4 : \sigma(2) \neq 3\}$ is a subgroup of $S_4$.

*Solution:* Let $H$ be the subset of $S_4$ in question. Note that $(13), (12) \in H$ but $(13)(12) = (123) \notin H$, so $H$ is not closed under the operation, so $H$ is not a subgroup of $S_4$.

(8) Write $(245)(1354)(125)$ and $(35)(123)(12)$ as (i) a cycle or a product of disjoint cycles in $S_5$; (ii) a product of transpositions in $S_5$. Decide if each is even or odd.

*Solution:* The permutation $(245)(1354)(125) = (14)(253) = (14)(23)(25)$ is odd. The permutation $(35)(123)(12) = (153) = (13)(15)$ is even.

(9) Consider the set $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ endowed with a multiplication such that $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$ and $ik = -j$.
(a) Write out the Cayley table for $Q_8$ (you will have an $8 \times 8$ grid).
(b) Find the identity element and list the inverse of each of the 8 elements.
We will assume that associativity holds. This $(Q_8, \cdot)$ is called the *quaternion group*.
(c) Find the center of $Q_8$.
(d) Show that, if $G$ is a group, then there is an equivalence relation given by $a \sim b$ in $G$ iff $a = gbg^{-1}$ for some $g \in G$. Find the equivalence classes with respect to $\sim$ if $G = Q_8$.

*Solution:*
(a)

| | $1$ | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
|---|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ | $-j$ | $j$ | $-k$ | $k$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ | $k$ | $-k$ | $-j$ | $j$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ | $-k$ | $k$ | $j$ | $-j$ |
| $j$ | $j$ | $-j$ | $-k$ | $k$ | $-1$ | $1$ | $i$ | $-i$ |
| $-j$ | $-j$ | $j$ | $k$ | $-k$ | $1$ | $-1$ | $-i$ | $i$ |
| $k$ | $k$ | $-k$ | $j$ | $-j$ | $-i$ | $i$ | $-1$ | $1$ |
| $-k$ | $-k$ | $k$ | $-j$ | $j$ | $i$ | $-i$ | $1$ | $-1$ |

(b) The identity element is obviously 1. We have the following chart:

| Element | $1$ | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
|---|---|---|---|---|---|---|---|---|
| Inverse | $1$ | $-1$ | $-i$ | $i$ | $-j$ | $j$ | $-k$ | $k$ |

(c) $Z(Q_8) = \{1, -1\}$
(d) Reflexive: $a = eae^{-1}$.
Symmetric: If $a = gbg^{-1}$ for some $g \in G$, then $b = g^{-1}a(g^{-1})^{-1}$.
Transitive: If $a = gbg^{-1}$ and $b = hch^{-1}$ for some $g, h \in G$, then $a = g(hch^{-1})g^{-1} = (gh)c(gh)^{-1}$.
For the second part, since $g \cdot 1 \cdot g^{-1} = 1$ for all $g \in Q_8$, it follows that 1 forms its own equivalence class. Similarly $-1$ forms its own equivalence class. Notice that $jij^{-1} = ji(-j) = (-k)(-j) = kj = -i$. Therefore $i \sim -i$. Trying all various possibilities, we conclude that $\{i, -i\}$ is an equivalence class. Similarly $\{j, -j\}$ and $\{k, -k\}$ are equivalence classes, so the collection of equivalence classes is $\{\{1\}, \{-1\}, \{i, -i\}, \{j, -j\}, \{k, -k\}\}$.

(10) Determine whether the following subsets $H$ are subgroups of the given group $G$.

(a) Let $G = \mathbb{Q}$ and $H = \left\{\frac{n}{2^m} : n \in \mathbb{Z}, m \in \mathbb{Z}_{\geq 0}\right\}$.
(b) Let $G = M(\mathbb{R})$ and $H = \left\{f \in M(\mathbb{R}) \colon f(2) = 0 \text{ and } \int_0^1 xf(x)\,dx = 0\right\}$.
(c) Fix $n \in \mathbb{Z}_{\geq 0}$. Let $G = M(\mathbb{R})$ and

$$H = \{f \in M(\mathbb{R}) \colon f(x) = c_0 + c_1x + \cdots + c_nx^n \text{ for some } c_0, \ldots, c_n \in \mathbb{R} \text{ and for all } x \in \mathbb{R}\}.$$

*Solution:*
(a) We claim that $H$ is a subgroup of $G$. Certainly $0 \in H$ so $H$ is nonempty. Suppose that $\frac{n}{2^m}, \frac{p}{2^q} \in H$, where $n, p \in \mathbb{Z}$ and $m, q \in \mathbb{Z}_{\geq 0}$. Then $\frac{n}{2^m} - \frac{p}{2^q} = \frac{2^q n - 2^m p}{2^{m+q}}$ which belongs to $H$, so $H$ is a subgroup.
(b) We claim that $H$ is a subgroup of $G$. Certainly the zero function $f$ defined by $f(x) = 0$ for all $x \in \mathbb{R}$ belongs to $H$, so $H$ is nonempty. Let $f, g \in H$. Then $(f-g)(2) = f(2) - g(2) = 0$ and $\int_0^1 x(f-g)(x)\,dx = \int_0^1 xf(x)\,dx - \int_0^1 xg(x)\,dx = 0$, so $f - g \in H$. Hence $H$ is a subgroup.
(c) We claim that $H$ is a subgroup of $G$. Certainly the zero function belongs to $H$, so $H$ is nonempty. Let $f, g \in H$. Then there are $c_i$ and $d_j$ such that $f(x) = c_0 + c_1x + \cdots + c_nx^n$ and $g(x) = d_0 + d_1x + \cdots + d_nx^n$ for all $x \in \mathbb{R}$. Then for all $x \in \mathbb{R}$, we have $(f-g)(x) = (c_0 - d_0) + (c_1 - d_1)x + \cdots + (c_n - d_n)x^n$, so $f - g \in H$. Hence $H$ is a subgroup of $G$.

(11) (a) Let $a \in \mathbb{R}^\times$. Prove that the matrix $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ belongs to the center of $\mathrm{GL}_2(\mathbb{R})$.
(b) Prove that, if a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ belongs to the center of $\mathrm{GL}_2(\mathbb{R})$, then $b = c = 0$ and $a = d$. Hint: such a matrix must commute with every element of $\mathrm{GL}_2(\mathbb{R})$, so in particular it commutes with $\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 0 & -1 \end{pmatrix}$. What equations would we then have?

*Solution:*
(a) Let $a \in \mathbb{R}^\times$. For any matrix $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$, it is easy to see that $\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} ap & aq \\ ar & as \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix}$, so $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ belongs to the center.
(b) If $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ belongs to $Z(\mathrm{GL}_2(\mathbb{R}))$, then it must commute with every matrix in $\mathrm{GL}_2(\mathbb{R})$. In particular it must commute with $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, so $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, i.e. $\begin{pmatrix} c & d \\ a & b \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix}$. Therefore $a = d$ and $b = c$. In addition, the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ must commute with $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, so $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, i.e. $\begin{pmatrix} c & d \\ -a & -b \end{pmatrix} = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix}$. So $b = -c$ as well. Hence $b = c = 0$.

(12) For each of the following, prove that the relation given is or is not an equivalence relation. If it is an equivalence relation, describe a complete set of equivalence classes.
(a) Let $x \sim y$ in $\mathbb{R}$ iff $xy \geq 0$.
(b) Let $x \sim y$ in $\mathbb{R}$ iff $|x| = |y|$.

*Solution:*
(a) We claim that the relation is not an equivalence relation because it is not transitive. Indeed, let $x = -1$, $y = 0$ and $z = 1$. Then $x \sim y$ and $y \sim z$ but $x \not\sim z$.
(b) This relation is an equivalence relation. For all $x \in \mathbb{R}$, we have $|x| = |x|$, so $x \sim x$. For all $x, y \in \mathbb{R}$, if $|x| = |y|$, then $|y| = |x|$, so $y \sim x$. For $x, y, z \in \mathbb{R}$, if $|x| = |y|$ and $|y| = |z|$, then $|x| = |z|$, so $x \sim z$. The set of equivalence classes is given by $\{\{x, -x\} \colon x \in \mathbb{R}\}$.

(13) List all the elements of $(\mathbb{Z}_9, \oplus)$ and the inverse of each.

*Solution:*

| Element | [0] | [1] | [2] | [3] | [4] | [5] | [6] | [7] | [8] |
|---|---|---|---|---|---|---|---|---|---|
| Inverse | [0] | [8] | [7] | [6] | [5] | [4] | [3] | [2] | [1] |

(14) Use the Euclidean algorithm to find $(69, 372)$ and $(792, 275)$.

*Solution:* Euclidean algorithm gives

$$\begin{aligned} 372 &= 5 \cdot 69 + 27, \\ 69 &= 2 \cdot 27 + 15, \\ 27 &= 1 \cdot 15 + 12, \\ 15 &= 1 \cdot 12 + 3, \\ 12 &= 3 \cdot 4. \end{aligned}$$

Hence $(69, 372) = 3$. Also we have

$$\begin{aligned} 792 &= 2 \cdot 275 + 242, \\ 275 &= 1 \cdot 242 + 33, \\ 242 &= 7 \cdot 33 + 11, \\ 33 &= 3 \cdot 11. \end{aligned}$$

Hence $(792, 275) = 11$.

(15) Using the Euclidean algorithm, show that 69 and 89 are relatively prime and write 1 as a linear combination of the two numbers.

*Solution:* We have

$$\begin{aligned} 89 &= 1 \cdot 69 + 20, \\ 69 &= 3 \cdot 20 + 9, \\ 20 &= 2 \cdot 9 + 2, \\ 9 &= 4 \cdot 2 + 1, \\ 2 &= 2 \cdot 1. \end{aligned}$$

Thus $(89, 69) = 1$. Reversing the steps we get

$$\begin{aligned} 1 &= 9 - 4 \cdot 2, \\ &= 9 - 4(20 - 2 \cdot 9) = -4 \cdot 20 + 9 \cdot 9 \\ &= -4(89 - 69) + 9(69 - 3 \cdot 20) = -4 \cdot 89 + 13 \cdot 69 - 27 \cdot 20 \\ &= -4 \cdot 89 + 13 \cdot 69 - 27(89 - 69) = \\ &= -31 \cdot 89 + 40 \cdot 69. \end{aligned}$$

(16) Let $n$ be an integer greater than 2. Prove that $\phi(n)$ is an even integer.

*Solution:* Suppose first that $n > 2$ is a power of 2; i.e. we have $n = 2^a$, where $a \in \mathbb{Z}, a \geq 2$. Then $\phi(n) = 2^a(1 - 1/2) = 2^{a-1}$, which is even. Now suppose that $n > 2$ is not a power of 2, so $n$ has an odd prime factor $p$. Then $\phi(n)$ is divisible by $p - 1$ (recall that $\phi(p^a) = p^{a-1}(p - 1)$ for primes $p$ and $a \in \mathbb{Z}_{\geq 1}$), so $\phi(n)$ is even.