MATH 580 — SECOND MIDTERM EXAM

February 27, 2006

NAME: Solutions

1. Do not open this exam until you are told to begin.
2. This exam has 10 pages including this cover. There are 10 problems.
3. Do not separate the pages of the exam.
4. Your proofs should be neat and legible. You may and should use the back of pages for scrap work.
5. If you are unsure whether you can quote a result from class or the book, please ask.
6. Please turn **off** all cell phones.

PROBLEM	POINTS	SCORE
1	12	
2	12	
3	11	
4	12	
5	6	
6	6	
7	8	
8	12	
9	10	
10	8	
TOTAL	100	

1. (3 points each) **(a)** Define the term "integral domain":

An integral domain is a commutative ring R with no zero divisors, i.e., if $a, b \in R$ and $ab = 0_R$, then $a = 0_R$ or $b = 0_R$.

(b) Define the term "field":

A field is a commutative ring F so that every nonzero element of F is a unit, i.e., if $a \in F$ and $a \neq 0$, then there exists $b \in F$ so that $ab = 1_F$.

(c) Give an example of an integral domain that is not a field. (Justify your answer!)

The integers $\mathbb{Z}$ is an example of an integral domain that is not a field. If $mn = 0$, then we know that $m = 0$ or $n = 0$. However, $2 \in \mathbb{Z}$ is nonzero yet has no inverse in $\mathbb{Z}$.

(d) Give an example of a ring that is not an integral domain. (Justify your answer!)

The ring $\mathbb{Z}/4\mathbb{Z}$ is a ring as we discussed in class, but $\overline{2} \cdot \overline{2} = \overline{0}$, but $\overline{2} \neq \overline{0}$.

2. (3+4+4+4 points) Let $z, w \in \mathbb{C}$.

(a) Define $\overline{z}$.

If $z = a + bi$ with $a, b \in \mathbb{R}$, then $\overline{z} = a - bi$.

(b) Prove that $\overline{z + w} = \overline{z} + \overline{w}$.

Proof: Let $z = a + bi$ and $w = c + di$ with $a, b, c, d \in \mathbb{R}$. Then we have

$$\begin{aligned} \overline{z+w} &= \overline{(a+c) + (b+d)i} \\ &= = (a+c) - (b+d)i \\ &= (a - bi) + (c - di) \\ &= \overline{z} + \overline{w}. \end{aligned}$$

■

(c) Prove that $|z|^2 = z\overline{z}$.

Proof: Let $z = a + bi$ with $a, b \in \mathbb{R}$. Then we have

$$\begin{aligned} |z|^2 &= a^2 + b^2 \\ &= (a + bi)(a - bi) \\ &= z\overline{z}. \end{aligned}$$

■

(d) Prove that $z = \overline{z}$ if and only if $z \in \mathbb{R}$.

Proof: Let $z = a + bi$ with $a, b \in \mathbb{R}$. If $z = \overline{z}$ we have that $a + bi = a - bi$, i.e., $b = -b$. However, this implies $b = 0$ and so $z = a \in \mathbb{R}$. Conversely, suppose $z \in \mathbb{R}$. Then necessarily we have that the imaginary part of z is 0, i.e., $b = 0$. Thus, $z = a = \overline{z}$. ■

3. (3+3+3+2 points) Let R be a ring with the following addition and multiplication tables:

+	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	d	e	f	a
c	c	d	e	f	a	b
d	d	e	f	a	b	c
e	e	f	a	b	c	d
f	f	a	b	c	d	e

·	a	b	c	d	e	f
a	a	a	a	a	a	a
b	a	b	c	d	e	f
c	a	c	e	a	c	e
d	a	d	a	d	a	d
e	a	e	c	a	e	c
f	a	f	e	d	c	b

(a) Is this ring commutative? Give reasons for your answer.

The ring is commutative. If you look at the multiplication table, it is symmetric over the diagonal, which means that $ab = ba$ for all $a, b \in R$.

(b) What are the zero-divisors in R?

First we must determine which element is 0_R. We see that $a + x = x$ for all $x \in R$, so $a = 0_R$. Now we just observe that $c \cdot d = 0_R$ and $d \cdot e = 0_R$, so the zero divisors are c, d, e.

(c) What are the units in R?

First we must determine which element is 1_R. We see that $bx = x$ for all $x \in R$, so $b = 1_R$. Now we just observe that $f \cdot f = 1_R$, so f is a unit.

(d) What familiar ring is this? (No proof is required here.)

Since the only rings we talked about with zero divisors were the rings $\mathbb{Z}/n\mathbb{Z}$ you should immediately think of these rings. There are 6 elements in this ring, so $\mathbb{Z}/6\mathbb{Z}$ would be a good guess. Then just observe that we can identify $a \sim \overline{0}$, $b \sim \overline{1}$, $c \sim \overline{2}$, $d \sim \overline{3}$, $e \sim \overline{4}$, and $f \sim \overline{5}$. We will see how to rigorously show these are the same rings next term.

4. (6 points each)**(a)** Show that $\mathbb{Q}\left(\sqrt{7}\right)$ is a field. You may use the fact that $\mathbb{Q}\left(\sqrt{7}\right) \subset \mathbb{R}$ and $\mathbb{R}$ is a ring.

Proof: Using that $\mathbb{R}$ is a ring, we see we only need to show that $\mathbb{Q}\left(\sqrt{7}\right)$ is a subring of $\mathbb{R}$ so that each element has an inverse in $\mathbb{Q}\left(\sqrt{7}\right)$. Let $a + b\sqrt{7}$ and $c + d\sqrt{7}$ be in $\mathbb{Q}\left(\sqrt{7}\right)$.
closed under addition: $(a+b\sqrt{7})+(c+d\sqrt{7}) = (a+c)+(b+d)\sqrt{7} \in \mathbb{Q}\left(\sqrt{7}\right)$ since $a+c$ and $b+d$ are in $\mathbb{Q}$.
closed under multiplication: $(a+b\sqrt{7})(c+d\sqrt{7}) = (ac+7bd)+(ad+bc)\sqrt{7} \in \mathbb{Q}\left(\sqrt{7}\right)$ since $ac+7bd$ and $ad+bc$ are in $\mathbb{Q}$.
additive identity: $0 = 0 + 0\sqrt{7} \in \mathbb{Q}\left(\sqrt{7}\right)$
multiplicative identity: $1 = 1 + 0\sqrt{7} \in \mathbb{Q}\left(\sqrt{7}\right)$
additive inverse: $-a - b\sqrt{7}$ is in $\mathbb{Q}\left(\sqrt{7}\right)$ since $-a, -b \in \mathbb{Q}$.
multiplicative inverse: $\frac{1}{a+b\sqrt{7}} = \left(\frac{a}{a^2-7b^2}\right) + \left(\frac{-b}{a^2-7b^2}\right)\sqrt{7} \in \mathbb{Q}\left(\sqrt{7}\right)$ since $\frac{a}{a^2-7b^2}$ and $\frac{-b}{a^2-7b^2}$ are in $\mathbb{Q}\left(\sqrt{7}\right)$
Thus we have that $\mathbb{Q}\left(\sqrt{7}\right)$ is a field. ■

(b) Prove that $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{7}\right)$ but $\mathbb{Q} \neq \mathbb{Q}\left(\sqrt{7}\right)$.

Proof: Let $r \in \mathbb{Q}$. Then we have that $r = r + 0\sqrt{7} \in \mathbb{Q}\left(\sqrt{7}\right)$, so $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{7}\right)$. To show that we do not have equality, we show that while $\sqrt{7}$ is in $\mathbb{Q}\left(\sqrt{7}\right)$, $\sqrt{7}$ is not in $\mathbb{Q}$. Suppose there exists $a, b \in \mathbb{Z}$ so that $\left(\frac{a}{b}\right)^2 = 7$. We may assume $\gcd(a,b) = 1$ by cancelling any common factors. Thus we have that $a^2 = 7b^2$. This implies that $7|a^2$ and since 7 is prime $7|a$. So there exists $k \in \mathbb{Z}$ so that $a = 7k$. Substituting this in and cancelling a 7 we have $7k^2 = b^2$. Thus, $7|b^2$ and hence $7|b$. This implies that $7|\gcd(a,b) = 1$, clearly a contradiction. Thus no such a and b exist and we see that $7 \notin \mathbb{Q}$. ■

5. (6 points) Prove that between any two distinct real numbers there are infinitely many rational numbers. You may use the fact that between any two distinct real numbers there is at least one rational number.

Proof: Let x and y be two distinct real numbers with $x < y$. Suppose that there are only finitely many rational numbers between x and y, say $x < r_1 < r_2 < \cdots < r_n < y$. Since r_1 and r_2 are distinct rational numbers, we know in particular that they are distinct real numbers. Thus there is a rational number r between r_2 and r_2. This is a contradiction as r is not in our list and is necessarily between x and y. Thus there must be infinitely many rational numbers between x and y. ■

6. (6 points) Prove that additive inverses in a ring are unique.

Proof: Let R be a ring and let $a \in R$. Suppose there exists $b, c \in R$ so that $a + b = 0_R = b + a$ and $c + a = 0_R = a + c$, i.e., we are assuming a has more then one additive inverse. Then we have

$$\begin{aligned} b &= b + 0_R \\ &= b + (a + c) \quad (\text{since } a + c = 0_R) \\ &= (b + a) + c \quad (\text{by the associativity of addition}) \\ &= 0_R + c \quad (\text{since } b + a = 0_R) \\ &= c. \end{aligned}$$

Thus, $b = c$ and we see that additive inverses are in fact unique. ■

7. (3+5 points) **(a)** List the n^{th} roots of unity.

The n^{th} roots of unity are given by $1, \omega, \omega^2, \ldots, \omega^{n-1}$ where $\omega = e^{\frac{2\pi i}{n}}$.

(b) Prove that the sum of the n^{th} roots of unity is 0.

Proof: We need to show that $\sum_{k=0}^{n-1} \omega^k = 0$. This is a geometric series, so we have

$$\begin{aligned}\sum_{k=0}^{n-1} \omega^k &= \frac{1-\omega^n}{1-\omega} \quad \text{(since } \omega \neq 1\text{)} \\ &= 0 \quad \text{(since } \omega^n = 1 \text{ by the definition of } n^{\text{th}} \text{ root of unity.)}\end{aligned}$$

8. (4 points each) **(a)** Show that $|e^{i\theta}| = 1$ for any $\theta \in \mathbb{R}$.

Proof: Recall that $e^{i\theta} = \cos\theta + i\sin\theta$. Thus, $|e^{i\theta}| = \sqrt{\cos^2\theta + \sin^2\theta} = 1$.

(b) Show that the map $f : \mathbb{C} \to \mathbb{C}$ defined by $f(z) = e^{i\theta} z$ for some fixed $\theta \in \mathbb{R}$ is an isometry.

Proof: Let $z, w \in \mathbb{C}$. Then

$$\begin{aligned}|f(z) - f(w)| &= |e^{i\theta} z - e^{i\theta} w| \\ &= |e^{i\theta}||z - w| \\ &= |z - w| \quad \text{(by part (a)).}\end{aligned}$$

(c) Let $g : \mathbb{C} \to \mathbb{C}$ be an isometry with $g(i) = 1$. Show that g maps the circle of radius 6 centered at i to the circle of radius 6 centered at 1.

Proof: Let z be a point on the circle of radius 6 centered at i. This means that z satisfies the equation $|z - i| = 6$. Now observe that we have

$$\begin{aligned}|g(z) - 1| &= |g(z) - g(i)| \\ &= |z - i| \quad \text{(since } g \text{ is an isometry)} \\ &= 6.\end{aligned}$$

Thus we see that $g(z)$ is on the circle of radius 6 centered at 1, as claimed. ■

9. (5 points each)**(a)** Find the cube roots of 27.

Let ω be a cube root of unity, i.e., $\omega = e^{\frac{2\pi i}{3}}$. Then the cube roots of 27 are

$$\begin{aligned} b &= 3 \\ \omega b &= 3\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) \\ \omega^2 b &= 3\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right). \end{aligned}$$

(b) Using part (a) and the formula from class, show that the roots of $z^3 - 9z - 28 = 0$ are $4, -2+\sqrt{3}i$,and $-2-\sqrt{3}i$.

Recall that the solutions to such an equation are given by $z = \sqrt[3]{A} - \dfrac{p}{3\sqrt[3]{A}}$ for the three different values of $\sqrt[3]{A}$ where $A = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{27}\right)^3}$. In this case we have that $p = -9$ and $q = -28$, so $A = 27$. Therefore, part (a) gives us the three possible values for $\sqrt[3]{A}$. Thus we have that the solutions are

$$\begin{aligned} z_1 &= 3 + 1 = 4 \\ z_2 &= 3\omega + \omega^{-1} = 3\omega + \omega^2 = 2\omega + (\omega + \omega^2) = 2\omega - 1 = -2 - i\sqrt{3}. \\ z_3 &= 3\omega^2 + \omega^{-2} = 3\omega^2 + \omega = 2\omega^2 + (\omega + \omega^2) = 2\omega^2 - 1 = -2 + i\sqrt{3} \end{aligned}$$

where we have used from Problem 7(b) that $1 + \omega + \omega^2 = 0$, i.e., $\omega + \omega^2 = -1$.

10. (8 points) Let R be a ring and $a \in R$ a fixed element. Let $S = \{ra : r \in R\}$, i.e., S is the set of multiples of a. Show that S is a subring of R not necessarily with identity. Determine when $1_R \in S$.

Proof: We must go through and verify each of the conditions to be a subring for S. Let ra and sa be elements of S. Note that by definition all elements of S can be written in this form.
closed under addition: We have $ra + sa = (r+s)a \in S$ since $r + s \in R$.
closed under multiplication: We have $ra \cdot sa = (ras)a \in S$ since $ras \in R$.
additive identity: Note that $0_R \in S$ since $0_R = 0_R a$.
additive inverse: Observe that $-ra = (-r)a \in S$ since $-r \in R$.
Thus we have shown that S is a subring of R that doesn't necessarily have an identity. In fact, $1_R \in S$ if and only if there exists a $b \in R$ so that $b \cdot a = 1_R$. Note this does not mean that R must be a field as we only require such a b for a and not even necessarily that a is a unit as we only require that $b \cdot a = 1_R$, not that $b \cdot a = 1_R = a \cdot b$. ■