MATH 581 — FIRST MIDTERM EXAM

April 21, 2006

NAME: Solutions

1. Do not open this exam until you are told to begin.
2. This exam has 9 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		
2		
3		
4		
5		
6		
7		
8		
9		
10		
TOTAL	100	

1. Throughout this problem R and S are commutative rings and F is a field.

(a) Define what it means for $I \subset R$ to be an ideal.

The set $I \subset R$ is an ideal if it is nonempty, for every $a, b \in I$ one has $a + b \in I$, and for every $r \in R$ and $a \in I$ one has $ar \in I$.

(b) Define what it means for $f(x) \in F[x]$ to be irreducible.

The polynomial $f(x)$ is irreducible if whenever one has $f(x) = g(x)h(x)$ for $g(x), h(x) \in F[x]$, then $g(x)$ or $h(x)$ must be a constant polynomial.

(c) Give an example of a reducible polynomial $f(x) \in \mathbb{Q}[x]$ that has no roots in $\mathbb{Q}$.

Let $g(x) = (x^2 + 1)^2$. This polynomial has no roots in $\mathbb{Q}$ (or even $\mathbb{R}$ for that matter) but is clearly reducible.

(e) Let $a \in R$. Define $\langle a \rangle$.

$$\langle a \rangle = \{ar : r \in R\}.$$

2. Let $\phi : R \to S$ be a ring homomorphism between two commutative rings.

(a) Define $\ker \phi$.

$$\ker \phi = \{r \in R : \phi(r) = 0_S\}.$$

(b) Prove that $\ker \phi$ is an ideal of R.

Proof: First observe that $0_R \in \ker \phi$ since ϕ is a homomorphism. Let $a, b \in \ker \phi$. Then $\phi(a + b) = \phi(a) + \phi(b) = 0_S + 0_S = 0_S$. Thus, $a + b \in \ker \phi$. Let $r \in R$. Then we have $\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0_S = 0_S$. Thus, $ra \in \ker \phi$. Hence we have that $\ker \phi$ is an ideal. ■.

3. (a) Prove that if $I \subset R$ is an ideal and I contains a unit, then $I = R$.

Proof: Let u be the unit in I and $v \in R$ so that $vu = 1_R$. Let $r \in R$. By the definition of ideal, since $u \in I$, then $rv \cdot u = r \cdot 1_R = r$ is in I. Thus $I = R$. ■

(b) Let F be a field. Prove that the only ideals in F are $\langle 0_F \rangle$ and F.

Proof: Let $I \subset F$ be a field. First, it is clear that $\langle 0_R \rangle$ is an ideal in F. If $I \neq \langle 0_F \rangle$, then there exists a non-zero element in I. Since F is a field, this non-zero element must be a unit and hence $I = F$ by part (a). ■

4. Let I and J be ideals in R. Prove that $I \cap J$ is an ideal in R.

Proof: Since I and J are ideals in R, each one contains 0_R and hence $0_R \in I \cap J$ which shows it is non-empty. Let $a, b \in I \cap J$. Thus $a, b \in I$ and $a, b \in J$. Since I and J are ideals, $a + b \in I$ and $a + b \in J$. Thus $a + b \in I \cap J$. Let $r \in R$. Then $ar \in I$ and $ar \in J$ since I and J are ideals. Thus, $ar \in I \cap J$. Hence we see $I \cap J$ is an ideal. ■

5. Prove that the map $\phi : \mathbb{Q}[\sqrt{7}] \to \mathbb{Q}[\sqrt{7}]$ given by $\phi(a + b\sqrt{7}) = a - b\sqrt{7}$ is an isomorphism.

Proof: Observe that $\phi(1) = 1$. Let $a + b\sqrt{7}, c + d\sqrt{7} \in \mathbb{Q}[\sqrt{7}]$. It is then easy to see ϕ is a homomorphism:

$$\begin{aligned}
\phi((a + b\sqrt{7}) + (c + d\sqrt{7})) &= \phi((a + c) + (b + d)\sqrt{7}) \\
&= (a + c) - (b + d)\sqrt{7} \\
&= (a - b\sqrt{7}) + (c - d\sqrt{7}) \\
&= \phi(a + b\sqrt{7}) + \phi(c + d\sqrt{7})
\end{aligned}$$

and

$$\begin{aligned}
\phi((a + b\sqrt{7}) \cdot (c + d\sqrt{7})) &= \phi((ac + 7bd) + (ad + bc)\sqrt{7}) \\
&= (ac + 7bd) - (ad + bc)\sqrt{7} \\
&= (a - b\sqrt{7}) \cdot (c - d\sqrt{7}) \\
&= \phi(a + b\sqrt{7})\phi(c + d\sqrt{7}).
\end{aligned}$$

To see ϕ is surjective, observe that $\phi(a - b\sqrt{7}) = a + b\sqrt{7}$. It is clear ϕ is injective by observing that $\phi(a + b\sqrt{7}) = 0$ if and only if $a = b = 0$. Thus, we have that ϕ is an isomorphism. ■

6. Prove that the composition of two isomorphisms is again an isomorphism. (You may NOT quote any results about composition of functions from Math 580!)

Proof: Let $f : R \to S$ and $g :\to T$ be two isomorphisms. Then we wish to show $h = g \circ f : R \to T$ is an isomorphism. First observe that $h(1_R) = g(f(1_R)) = g(1_S) = 1_T$. Let $a, b \in R$. We have

$$\begin{aligned} h(a+b) &= g(f(a+b)) \\ &= g(f(a)+f(b)) \\ &= g(f(a)) + g(f(b)) \\ &= h(a) + h(b) \end{aligned}$$

where we have used that f and g are homomorphisms. As for the multiplicative structure, we have

$$\begin{aligned} h(ab) &= g(f(ab)) \\ &= g(f(a)f(b)) \\ &= g(f(a))g(f(b)) \\ &= h(a)h(b) \end{aligned}$$

where we again have used that f and g are homomorphisms. Thus we have that h is a homomorphism. Now we need to see that h is injective and surjective. We show injectivity by showing the kernel is $\langle 0_R \rangle$. Let $r \in \ker h$. Then $g(f(r)) = 0_T$. Since g is injective we must have $f(r) = 0_S$. Since f is injective we must have $r = 0_R$, as claimed. Now to show h is surjective, let $t \in T$. Since g is surjective there exists a $s \in S$ so that $g(s) = t$. Since f is surjective there exists a $r \in R$ so that $f(r) = s$. Thus we have $h(r) = t$ and hence h is surjective. We have shown that h is an isomorphism as claimed. ■

7. Prove that $\mathbb{R}[x]/\langle x^2+1 \rangle \cong \mathbb{C}$.

Proof: We use the first isomorphism theorem to prove this result. Define $\phi : \mathbb{R}[x] \to \mathbb{C}$ by $\phi(f(x)) = f(i)$. It is clear that this map is surjective, for instance, $\phi(a+bx) = a+bi$. Note that $\phi(1) = 1$. To see that ϕ respects the additive and multiplicative structures, observe that we have

$$\begin{aligned} \phi(f(x)+g(x)) &= f(i) + g(i) \\ &= \phi(f(x)) + \phi(g(x)) \end{aligned}$$

and

$$\begin{aligned} \phi(f(x)g(x)) &= f(i)g(i) \\ &= \phi(f(x))\phi(g(x)). \end{aligned}$$

Thus we see ϕ is an onto homomorphism from $\mathbb{R}[x]$ to $\mathbb{C}$. It is clear that $\langle x^2+1 \rangle \subset \ker \phi$. The fact that $\mathbb{R}[x]$ is a PID and x^2+1 is irreducible over $\mathbb{R}[x]$ then gives that $\ker \phi = \langle x^2+1 \rangle$. Thus, the first isomorphism theorem allows us to conclude that $\mathbb{R}[x]/\langle x^2+1 \rangle \cong \mathbb{C}$. ■

8. Prove that $\sqrt[5]{\frac{17}{25}}$ is not a rational number. (It may be helpful to consider the polynomial $f(x) = 25x^5 - 17$.)

Proof: Consider the polynomial $f(x) = 25x^5 - 17$. Note that this polynomial is irreducible over $\mathbb{Q}$ by Eisenstein applied with $p = 17$. If $\sqrt[5]{\frac{17}{25}}$ were in $\mathbb{Q}$, then $f(x)$ would necessarily be reducible as it would have a root in $\mathbb{Q}$. Thus it must be that $\sqrt[5]{\frac{17}{25}} \notin \mathbb{Q}$. ■

9. Let $\phi : R \to S$ be an homomorphism between commutative rings.

(a) Define the image of ϕ, i.e., $\phi(R)$.

$$\phi(R) = \{\phi(r) : r \in R\}.$$

(b) Prove that $\phi(R)$ is a subring of S.

Proof: First observe that since ϕ is a homomorphism, 0_S and 1_S are both in $\phi(R)$. Let $\phi(a)$ and $\phi(b)$ be in $\phi(R)$. Using that ϕ is a homomorphism, $\phi(a) + \phi(b) = \phi(a + b) \in \phi(R)$. Thus $\phi(R)$ is closed under addition. Again using ϕ is a homomorphism we have $\phi(a)\phi(b) = \phi(ab) \in \phi(R)$ and so $\phi(R)$ is closed under multiplication. It only remains to show that $-\phi(a) \in \phi(R)$. However, we know that $-\phi(a) = \phi(-a)$ since ϕ is a homomorphism, so this is clear as well. Thus $\phi(R)$ is a subring of S. ■

(d) Prove that if R is a field, then $\phi(R)$ is a field. (Problem 2(b) may be helpful here!)

Proof: Note that we have $\phi : R \to \phi(R)$ by the definition of $\phi(R)$ and moreover this is now a surjective homomorphism. The first isomorphism theorem now tells us that $R/\ker\phi \cong \phi(R)$, so it only remains to determine the possibilities for $\ker\phi$. Since ϕ is a homomorphism, we know $\phi(1_R) = 1_S$, so in particular $1_R \notin \ker\phi$. Thus, $\ker\phi \neq R$. Now by problem 2(b) the only other possibility is for $\ker\phi = \langle 0_R \rangle$. Thus we have $R \cong \phi(R)$ and hence $\phi(R)$ is a field. ■

10. An ideal $\wp$ in a commutative ring R is said to be a *prime ideal* if $\wp \neq R$ and whenever $ab \in \wp$, then $a \in \wp$ or $b \in \wp$.

(a) Let $p \in \mathbb{Z}$ be a prime number. Show that $\langle p \rangle$ is a prime ideal.

Proof: Let $bc \in \langle p \rangle$. This means that $p|bc$. However, using that p is a prime we have that $p|b$ or $p|c$ and thus either $b \in \langle p \rangle$ or $c \in \langle p \rangle$ as desired. ■

(b) Show that if $\wp$ is a prime ideal, then $R/\wp$ is an integral domain.

Proof: Since R is a commutative ring, it only remains to show that there are no zero-divisors in $R/\wp$. Suppose that there exists $\overline{a}$ and $\overline{b}$ in $R/\wp$ so that $\overline{a} \cdot \overline{b} = \overline{0}$. In particular, this is equivalent to the fact that $ab \in \wp$. However, since $\wp$ is a prime ideal, it must be that a or b is in $\wp$, i.e., $\overline{a}$ or $\overline{b}$ is $\overline{0}$. Thus there are no zero-divisors and hence $R/\wp$ is an integral domain. ■

(c) Show that if $R/\wp$ is an integral domain, then $\wp$ is a prime ideal.

Proof: Suppose $R/\wp$ is an integral domain and let $ab \in \wp$. Then we have that $\overline{ab} = \overline{a} \cdot \overline{b} = \overline{0}$. However, using that $R/\wp$ is an integral domain shows that either $\overline{a}$ or $\overline{b}$ is $\overline{0}$, i.e., $a \in \wp$ or $b \in \wp$. Thus $\wp$ is a prime ideal. ■