MATH 580 — FINAL EXAM

March 15, 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 8 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	18	
2	14	
3	5	
4	5	
5	18	
6	10	
7	15	
8	15	
TOTAL	100	

1. (3 points each) **(a)** Let F be a field and $f(x) \in F[x]$. Define the splitting field of $f(x)$.

See page 99.

(b) Let X, Y, and Z be sets with $Z \subset Y$ and $g : X \to Y$ a map. Define $f^{-1}(Z)$.

See page 376.

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

See page 87.

(d) Define the term field.

See page 39.

(e) Let a and b be integers. Define the greatest common divisor of a and b.

See page 13.

(f) Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Define $a \equiv b (\operatorname{mod} n)$.

See page 20.

2. (2 points each) Give examples of the following. These are no partial credit, so no explanation is necessary.

(a) An integral domain that is not a field.

The ring $\mathbb{Z}$ is an integral domain that is not a field. For example, $2^{-1} \notin \mathbb{Z}$.

(b) A field with finitely many elements.

The ring $\mathbb{Z}/5\mathbb{Z}$ is a field.

(c) A field with infinitely many elements.

The ring $\mathbb{Q}$ is a field with infinitely many elements.

(d) An infinite ring that is NOT an integral domain.

The ring $(\mathbb{Z}/4\mathbb{Z})[x]$ is an infinite ring (x to any positive power is in this ring) and it is not an integral domain because $\overline{2}x \cdot \overline{2}x = \overline{0}$ but $\overline{2}x \neq \overline{0}$.

(e) An integral domain that is NOT a field but contains $\mathbb{Q}$. (Think Chapter 3!)

The ring $\mathbb{Q}[x]$ is an integral domain that contains $\mathbb{Q}$, but it is not a field because for example x does not have an inverse.

(f) An injective function that is NOT surjective.

The map $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = 2n$ is an injective map but is not surjective.

(g) A surjective function that is NOT injective.

The map $f : \{1, 2\} \to \{1\}$ defined by $f(1) = 1 = f(2)$ is a surjective function that is not injective.

3. (5 points) Let $z \in \mathbb{C}$. Recall that we denoted the real part of z by $\mathrm{Re}(z)$. Prove that

$$\mathrm{Re}(z) = \frac{z + \overline{z}}{2}.$$

Proof: Write $z = a + bi$ with $a, b \in \mathbb{R}$. Note that $\mathrm{Re}(z) = a$. Then we have

$$\begin{aligned} \frac{z+\overline{z}}{2} &= \frac{a + bi + a - bi}{2} \\ &= \frac{2a}{2} \\ &= a. \qquad \blacksquare \end{aligned}$$

4. (5 points) Let R be an integral domain with $\mathbb{Z} \subset R$. Show that if $2^5 x = 2^3 y$, then $4x = y$.

Proof: Note that the statement $2^5 x = 2^3 y$ is equivalent to the statement that $2^5 x - 2^3 y = 0$. We can factor out a 2^3 on the left hand side to obtain the equation $2^3(4x - y) = 0$. Since $2^3 \neq 0$ since $\mathbb{Z} \subset R$, we can use the fact that R is an integral domain to conclude that $4x - y = 0$, i.e., $4x = y$. ■

5. (6 points each) There are 6 separate questions in this problem. Pick any three of them that you choose and ignore the other three. Please indicate CLEARLY which three you want graded, otherwise I will grade the first three.

(a) Prove or disprove: Let $a, b, c \in \mathbb{Z}$. If $a|(b + c)$ then $a|b$ or $a|c$.

This statement is false. Let $a = 6$, $b = 3 = c$. Then $6|(3 + 3)$ but $6 \nmid 3$.

(b) Let p be a prime number. Prove that if $p|(a_1 a_2 \cdots a_n)$, then $p|a_i$ for some $1 \leq i \leq n$. (You may use the fact that if $p|ab$ then $p|a$ or $p|b$.)

Proof: We prove the statement by inducition on n. The base case of $n = 2$ is true by the fact you are allowed to use, namely, if $p|ab$, then $p|a$ or $p|b$. Now suppose that for some positive integer k we know that if $p|(a_1 \cdots a_k)$, then $p|a_j$ for some $1 \leq j \leq k$. Suppose $p|(b_1 \cdots b_k b_{k+1})$ for some integers b_i $(1 \leq i \leq k + 1)$. In particular, we see that $p|ab$ for $a = b_1$ and $b = b_2 \cdots b_{k+1}$. Thus, but the case of $n = 2$ we know that $p|b_1$ or $p|(b_2 \cdots b_{k+1})$. Applying the induction hypothesis to the case that $p|(b_2 \cdots b_{k+1})$ we see that $p|b_j$ for some $2 \leq j \leq k+1$. Combining this with the case that $p|b_1$, we have the result by induction. ■

(c) Let $f(x) \in \mathbb{Q}[x]$. Prove that if you divide $f(x)$ by $(x - 2)$ then you obtain a remainder of $f(2)$. (This requires a proof, it is NOT acceptable to simply say "This is true by Proposition....")

Proof: Applying the division algorithm and dividing $f(x)$ by $(x - 2)$ we see that there exists unique $q(x)$ and $r(x)$ in $\mathbb{Q}[x]$ with $\deg(r(x)) < 1$ so that

$$f(x) = (x - 2)q(x) + r(x).$$

The fact that $\deg(r(x)) < 1$ implies that $\deg(r(x)) = 0$ and so $r(x)$ is a constant, say $r(x) = c \in \mathbb{Q}$. Rewriting the equation we have

$$f(x) = (x - 2)q(x) + c.$$

Plug in $x = 2$ to obtain $f(2) = c$. ■

(d) Prove that if $f(x) \equiv g(x) (\bmod p(x))$ and $g(x) \equiv h(x) (\bmod p(x))$, then $f(x) \equiv h(x) (\bmod p(x))$.

Proof: The fact that $f(x) \equiv g(x) (\bmod p(x)$ implies that there exists a polynomial $s(x)$ so that $p(x)s(x) = f(x) - g(x)$. Similarly, we have that there exists a polynomial $t(x)$ so that $p(x)t(x) = g(x) - h(x)$. Adding these two equations we obtain $p(x)(s(x) + t(x)) = f(x) - h(x)$, i.e., $p(x)|(f(x) - h(x))$. Thus, $f(x) \equiv h(x) (\bmod p(x))$. ■

(e) Prove that $\mathbb{Q}[\sqrt{-3}]$ is a field. You may use the fact that $\mathbb{Q}[\sqrt{-3}] \subset \mathbb{C}$ and $\mathbb{C}$ is a field.

Proof: By the fact listed we need only to show that $\mathbb{Q}[\sqrt{-3}]$ is a subring of $\mathbb{C}$ that is also a field. Let $a + b\sqrt{-3}$ and $c + d\sqrt{-3}$ be elements of $\mathbb{Q}[\sqrt{-3}]$.
closed under addition: $(a + b\sqrt{-3}) + (c + d\sqrt{-3}) = (a + c) + (b + d)\sqrt{-3} \in \mathbb{Q}[\sqrt{-3}]$ since $a + c$ and $b + d$ are in $\mathbb{Q}$.
closed under multiplication: $(a+b\sqrt{-3})(c+d\sqrt{-3}) = (ac-3bd)+(ad+bc)\sqrt{-3} \in \mathbb{Q}[\sqrt{-3}]$ since $ac - 3bd$ and $ad + bc$ are both in $\mathbb{Q}$.
additive identity: $0 = 0 + 0\sqrt{-3} \in \mathbb{Q}[\sqrt{-3}]$ since $0 \in \mathbb{Q}$.
multiplicative identity: $1 = 1 + 0\sqrt{-3} \in \mathbb{Q}[\sqrt{-3}]$ since 0 and 1 are in $\mathbb{Q}$.
additive identity: $-a - b\sqrt{-3} \in \mathbb{Q}[\sqrt{-3}]$ since $-a$ and $-b$ are in $\mathbb{Q}$.
Thus we have that $\mathbb{Q}[\sqrt{-3}]$ is a subring of $\mathbb{C}$. Let $a + b\sqrt{-3} \in \mathbb{Q}[\sqrt{-3}]$ be such that not both a and b are 0. Then

$$\begin{aligned}
\frac{1}{a + b\sqrt{-3}} &= \frac{a - b\sqrt{-3}}{a^2 - 3b^2} \\
&= \left(\frac{a}{a^2 - 3b^2}\right) + \left(\frac{-b}{a^2 - 3b^2}\right)\sqrt{-3} \in \mathbb{Q}[\sqrt{-3}]
\end{aligned}$$

since $\dfrac{a}{a^2 - 3b^2}$ and $\dfrac{-b}{a^2 - 3b^2}$ are in $\mathbb{Q}$. Thus we have that $\mathbb{Q}[\sqrt{-3}]$ is a field. ■.

(f) Suppose $f : X \to Y$, $g : Y \to Z$, and $h = g \circ f$. Prove that if h is surjective, then g is surjective.

Let $z \in Z$. Using that h is surjective, we have that there exists an $x \in X$ so that $h(x) = z$. The fact that h is a composition allows us to write $g(f(x)) = z$, i.e., $g(y) = z$ for $y = f(x)$. Thus g is surjective. ■

6. (3+7 points) **(a)** State the fundamental theorem of algebra.

Suppose $f(x) \in \mathbb{C}[x]$ is a polynomial of degree $n \geq 1$. Then $f(x)$ has a root in $\mathbb{C}$.

(b) Use induction and the fundamental theorem of algebra to prove that if $f(x) \in \mathbb{C}[x]$, then $f(x)$ can be factored into linear factors.

Proof: We proceed by induction on the degree of $f(x)$. Suppose $f(x)$ has degree 1. Then $f(x) = ax + b$ for some $a, b \in \mathbb{C}$ with $a \neq 0$. Thus is already a linear factor. Now suppose that for some $k \in \mathbb{N}$ we have that all polynomials of degree k in $\mathbb{C}[x]$ can be factored into linear factors. Let $f(x)$ be a polynomial of degree $k + 1$. Using the fundamental theorem of algebra we have that there is a root α of $f(x)$ in $\mathbb{C}$. Thus, $(x - \alpha)$ must be a factor of $f(x)$. So there exists a polynomial $g(x) \in \mathbb{C}[x]$ of degree k so that $f(x) = (x - \alpha)g(x)$. Now by our inductive hypothesis we can factor $g(x)$ into linear factors. In particular, $f(x)$ is then factored into linear factors. Thus, by induction, we have that all polynomials in $\mathbb{C}[x]$ of degree greater then or equal to 1 can be factored into linear factors in $\mathbb{C}[x]$. ■

7. (3 points each) Let $R = (\mathbb{Z}/11\mathbb{Z})\,[x]/(x^3 + \overline{3})$.

(a) Is R a field? Justify your answer!.

R is not a field. In fact, it is not an integral domain. The polynomial $x^3 + \overline{3}$ has $\overline{2}$ as a root as $(\overline{2})^3 + \overline{3} = \overline{11} = \overline{0}$. In particular, we have that $x^3 + \overline{3} = (x - \overline{2})(x^2 + \overline{2}x + \overline{4})$. Thus, we have the zero divisors $\overline{x-2}$ and $\overline{x^2 + 2x + 4}$.

(b) Compute $\overline{5x^2 + 7x + 4} + \overline{10x^2 - 3x + 1}$.

$$\begin{aligned} \overline{5x^2 + 7x + 4} + \overline{10x^2 - 3x + 1} &= \overline{15x^2 + 4x + 5} \\ &= \overline{4x^2 + 4x + 5}. \end{aligned}$$

(c) Compute $(\overline{2x^2 + 3}) \cdot (\overline{x^3 + 5x^2 + 6})$.

$$\begin{aligned} (\overline{2x^2 + 3}) \cdot (\overline{x^3 + 5x^2 + 6}) &= (\overline{2x^2 + 3}) \cdot (\overline{5x^2 + 3}) \\ &= \overline{80x + 10x^2 + 9} \\ &= \overline{10x^2 + 3x + 9}. \end{aligned}$$

(d) Find a polynomial $r(x)$ of degree less then or equal to 2 so that $\overline{g(x)} = \overline{r(x)}$ where $g(x) = x^6 + 10x^3 + 5$.

$$\begin{aligned} \overline{g(x)} &= \overline{(x^3)^2 + 10x^3 + 5} \\ &= \overline{3^2 + 10(3) + 5} \\ &= \overline{44} \\ &= \overline{0}. \end{aligned}$$

(e) How many elements are in the ring R?

All polynomials of the form $ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}/11\mathbb{Z}$ are in this ring. Thus there are 11^3 elements in this ring.

8. (3+4+8 points) **(a)** Write down the 6^{th} roots of unity.

Let $\omega = e^{\frac{2\pi i}{6}}$. Then the 6^{th} roots of unity are given by $1, \omega, \omega^2, \omega^3, \omega^4, \omega^5$.

(b) List the roots of $f(x) = x^6 - 2$.

The roots are given by mutliplying $\sqrt[6]{2}$ by the 6^{th} roots of unity, i.e., the roots are $\sqrt[6]{2}\omega^j$ for $0 \leq j \leq 5$.

(c) Find the splitting field of $f(x)$. Be sure to prove the field you find is the splitting field. It may help to write your 6^{th} root of unity in the form $a + bi$ for appropriate $a, b \in \mathbb{R}$.

Note that we can write

$$\omega = e^{\frac{\pi i}{3}} = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \frac{1}{2} + \frac{\sqrt{3}}{2}i.$$

This leads to the following claim. Let K be the splitting field of $f(x)$.

Claim: $K = \mathbb{Q}[\sqrt[6]{2}, \sqrt{3}i]$.

Proof: Note that since K is the splitting field, all the roots of $f(x)$ are necessarily in K. Thus $\sqrt[6]{2} \in K$ and $\omega \in K$. Using that K is a field and $\mathbb{Q} \subset K$, we see that $\omega \in K$ implies that $\sqrt{3}i \in K$ as well. Thus we have $\mathbb{Q}[\sqrt[6]{2}, \sqrt{3}i] \subset K$. Now we must show the reverse containment. The reverse containment is true provided that we can show $f(x)$ splits over $\mathbb{Q}[\sqrt[6]{2}, \sqrt{3}i]$ since K is necessarily the smallest field that $f(x)$ splits over. Note that since $\sqrt{3}i \in \mathbb{Q}[\sqrt[6]{2}, \sqrt{3}i]$, we can use that $\mathbb{Q}[\sqrt[6]{2}, \sqrt{3}i]$ is a field to obtain that $\omega \in \mathbb{Q}[\sqrt[6]{2}, \sqrt{3}i]$. This in turn implies that $\omega^j \in \mathbb{Q}[\sqrt[6]{2}, \sqrt{3}i]$ for $0 \leq j \leq 5$. Since $\sqrt[6]{2} \in \mathbb{Q}[\sqrt[6]{2}, \sqrt{3}i]$, we have that $\sqrt[6]{2}\omega^j \in \mathbb{Q}[\sqrt[6]{2}, \sqrt{3}i]$ for $0 \leq j \leq 5$, i.e., $f(x)$ splits over $\mathbb{Q}[\sqrt[6]{2}, \sqrt{3}i]$. Thus we have the claim. $\blacksquare$.