Math 476
Exam 4

Instructions: You will have 55 minutes to complete this exam. The credit given on each problem will be proportional to the amount of correct work shown. Answers without supporting work will receive little credit.
Work your exam on separate sheets of paper. Be sure to number each problem and put your name on each page.

1. (12 points) Recall that in constructing the field of quotients of in integral domain D, we first defined the set $S = \{(a,b) : a,d \in D, b \neq 0\}$ and then defined an equivalence relation $\equiv$ on S via $(a,b) \equiv (c,d)$ if $ad = bc$. We then defined $\mathbb{F}$ as the set of equivalence classes of A under $\equiv$. Finally, we defined addition and multiplication in $\mathbb{F}$ via $a/b + c/d = (ad+bc)/(bd)$ and $a/b \cdot c/d = (ac)/(bd)$.

   Prove that the addition operation on $\mathbb{F}$ is well defined.

   Proof: Suppose that $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$. Then, by definition of equivalence in S, (1) $ab' = ba'$, and (2) $cd' = dc'$.

   Notice that $(ad+bc)(b'd') = adb'd' + bcb'd'$ (by the distributive property)

   $= ab'dd' + cd'bb'$ (since D is a domain, it is commutative), which, using (1) and (2) above, $= ba'dd' + dc'bb'$.

   $= a'd'(bd) + b'c'(bd)$ (again using commutativity), or, by the distributive property, $= (a'd' + b'c')(bd)$.

   That is, $(ad+bc)(b'd') = a'd' + b'c')(bd)$. Then $(ad+bc)/(bd) = (a'd'+b'c')/(b'd')$. Hence the addition operation is well defined. □.

2. Prove **one** of the following:

   (a) (15 points) Let $\mathbb{F}$ be a field, $a \in \mathbb{F}$, and $f(x) \in \mathbb{F}[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

   Proof: Applying the Division Algorithm to divide $f(x)$ by $x-a$, we have $f(x) = q(x)(x-a) + r(x)$ with $r(x) = 0$ or $deg, r(x) < deg\, x - a$.

   Notice that since $x - a$ has degree 1, then $r(x)$ must be a constant.

   Next, using the result of the division above, we compute $f(a) = q(a)(a-a) + r(a) = q(a)(0) + r(a)$. Therefore, $f(a) = r(a)$.

   However, since $r(x)$ is a constant, $r(x) = r(a)$. Hence $f(a) = r(x)$ is the remainder in the division of $f(x)$ by $x - a$. □.

   (b) (15 points) Let $\mathbb{F}$ be a field. Then $\mathbb{F}[x]$ is a principle ideal domain.

   Proof: First, by Theorem 16.1, since $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is an integral domain. Let I be an ideal of $\mathbb{F}[x]$.

   Case 1: If $I = \{0\}$, then $I = \langle 0 \rangle$, thus I is a principal ideal.

   Case 2: Suppose $I \neq \{0\}$. Let $g(x)$ be a polynomial of minimal degree in I. Notice that since $g(x) \in I$, then $\langle g(x) \rangle \subset I$. (Recall: $\langle g(x) \rangle = \{q(x)g(x) : q(x) \in \mathbb{F}[x]\}$, and since $g(x) \in I$, then $q(x)g(x) \in I$ for all $q(x) \in \mathbb{F}[x]$.)

   Let $f(x) \in I$. Using the Division Algorithm, we may write $f(x) = q(x)g(x) + r(x)$ with $r(x) = 0$ or $deg\, r(x) < deg\, g(x)$.

   Notice that, $f(x) \in I$ and $q(x)g(x) \in I$. Therefore, $r(x) = f(x) - q(x)g(x) \in I$. Since $g(x)$ was chosen to have minimal degree in I, we cannot have $deg\, r(x) < deg\, g(x)$. Hence $r(x) = 0$. That is, $f(x) = q(x)g(x)$.

   Thus $f(x) \in \langle g(x) \rangle$. Therefore, $I \subset \langle g(x) \rangle$. Hence $I = \langle g(x) \rangle$.

   Since we have shown that every ideal in $\mathbb{F}[x]$ is principal, then $\mathbb{F}[x]$ is a principal ideal domain. □.

3. Prove **one** of the following:

   (a) (15 points) Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $deg, f(x) \geq 1$. Let $\overline{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p. If $\overline{f}(x)$ is irreducible over $\mathbb{Z}_p$ and $deg\,\overline{f}(x) = deg\,f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

   Proof: Suppose, in order to obtain a contradiction, that $f(x)$ is reducible over $\mathbb{Q}$. Then, since $f(x) \in \mathbb{Z}[x]$, by Theorem 17.2, $f(x)$ is also reducible over $\mathbb{Z}$. Therefore, there are polynomials $g(x), h(x) \in \mathbb{Z}[x]$ with $f(x) = g(x)h(x)$, $deg\,g(x) < deg\,f(x)$, and $deg\,h(x) < deg\,f(x)$.

   Let $\overline{g}(x)$ and $\overline{h}(x)$ be the polynomials obtained from $g(x)$ and $h(x)$ by reducing their coefficients modulo p.

   Since $deg\,f(x) = deg\,\overline{f}(x)$, we must have $deg\,\overline{g}(x) \leq deg\,g(x) < deg\,\overline{f}(x) = \text{deg } f(x)$, and $\overline{h}(x) \leq deg\,h(x) < deg\,\overline{f}(x) = deg\,f(x)$.

   But $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$, thus $\overline{f}(x)$ is reducible over $\mathbb{Z}_p$, which is a contradiction.

   Hence, contrary to our initial assumption, $f(x)$ is irreducible over $\mathbb{Q}$. □.

   (b) (15 points) Let $f(x) \in \mathbb{Z}[x]$, let $g(x) \in \mathbb{Q}[x]$, and suppose k is the smallest positive integer such that $f(x) = kg(x)$. Prove that $f(x)$ is reducible over $\mathbb{Z}$ if and only if $g(x)$ is reducible over $\mathbb{Q}$.

   Proof:

   "$\Rightarrow$": Suppose $f(x)$ is reducible over $\mathbb{Z}$. Then $f(x) = p(x)q(x)$ for polynomials $p(x), q(x) \in \mathbb{Z}[x]$ with $deg\,p(x) < deg\,f(x)$ and $deg\,q(x) < deg\,f(x)$. Also, as defined, $k > 0$, so, computing in $\mathbb{Q}[x]$, we have $\frac{1}{k}f(x) = \frac{1}{k}p(x)q(x)$.

   Therefore, $g(x) = \left(\frac{1}{k}p(x)\right)q(x)$. Notice that the degrees have not changed, and that $\frac{1}{k}p(x) \in \mathbb{Q}[x]$. Hence $g(x)$ is reducible over $\mathbb{Q}$.

   "$\Leftarrow$": Suppose $g(x)$ is reducible over $\mathbb{Q}$. Then $g(x) = s(x)t(x)$ for polynomials $s(x), t(x) \in \mathbb{Q}[x]$ with $deg\,s(x) < deg\,g(x)$ and $deg\,t(x) < deg\,q(x)$. Also, as defined, $k > 0$, so we have $kg(x) = f(x) = k \cdot s(x)t(x)$.

   Therefore, $f(x)$ is reducible over $\mathbb{Q}$. Hence, by Theorem 17.2, since $f(x) \in \mathbb{Z}[x]$, $f(x)$ is also reducible over $\mathbb{Z}$. □.

4. (12 points) Let $f(x) = x^4 + 4$. Write $f(x)$ as a product of irreducible factors over $\mathbb{Z}_5$.

   Notice that over $\mathbb{Z}_5$, $f(0) = 4$, $f(1) = 5 \equiv 0$, $f(2) = 20 \equiv 0$, $f(3) = 85 \equiv 0$, and $f(4) = 260 \equiv 0$.

   Therefore, $x = 1$, $x = 2$, $x = 3$, and $x = 4$ are zeros of $f(x)$ in $\mathbb{Z}_5$. Hence, by the Factor Theorem, $(x-1)$, $(x-2)$, $(x-3)$, and $(x-4)$ are factors of $f(x)$. Since we are working in $\mathbb{Z}_5$, we may rewrite these factors as: $(x+4)$, $(x+3)$, $(x+2)$, and $(x+1)$.

   Claim: $f(x) = (x+1)(x+2)(x+3)(x+4)$ is a complete factorization for $f(x)$. Note that $(x+1)(x+2)(x+3)(x+4) = (x^2+3x+2)(x^2+7x+12) = (x^2+3x+2)(x^2+2x+2) = x^4+3x^3+2x^2+2x^3+6x^2+4x+2x^2+6x+4 = x^4+5x^3+10x^2+10x+4 = x^4+4$.

   Since all these factors are linear, no further factorization is possible.

5. Show that each of the following polynomials is irreducible over $\mathbb{Q}$.

   (a) (7 points) $f(x) = x^5 + 6x^4 - 9x^3 + 12x - 15$

   Notice that if we take $p = 3$, then $3 \not| 1$, $3|6$, $3|-9$, $3|12$ and $p|-15$, but since $p^2 = 9$, $p^2 \not| -15$. Hence, by Eisenstein's Criterion, $f(x)$ is irreducible over $\mathbb{Q}$.

   (b) (7 points) $g(x) = 2x^3 - 3x^2 + 7x - 2$

   We will use the Mod$-p$ irreducibility test. Note that taking $p = 2$ would reduce the degree of $\overline{g}(x)$, so we try $p = 3$.

   Then $\overline{g}(x) = 2x^3 + 0x^2 + x + 1$. Notice that $\overline{g}(0) = 1$, $\overline{g}(1) = 4 \equiv 1$, and $\overline{g}(2) = 16 + 2 + 1 = 19 \equiv 1$. Therefore, $\overline{g}(x)$ has no zeros over $\mathbb{Z}_3$. Hence, by Theorem 17.1, $\overline{g}(x)$ is irreducible over $\mathbb{Z}_3$.

   Thus $g(x)$ is irreducible over $\mathbb{Q}$ by the Mod-3 irreducibility test.

(c) (7 points) $h(x) = \frac{3}{5}x^4 + x - \frac{7}{5}$

We begin by finding an equivalent polynomial in $\mathbb{Z}[x]$. Multiplying by the *lcm* of the denominators gives $k(x) = 5 \cdot h(x) = 3x^4 + 5x - 7$.

Next, we apply the Mod-2 irreducibility test to $k(x)$. Then $\overline{k}(x) = x^4 + x + 1$. Notice that $\overline{k}(0) = 1$ and $\overline{k}(1) = 1$, so $\overline{k}(x)$ has no zeros over $\mathbb{Z}_2$. However, since our polynomial has degree 4, Theorem 17.1 does not apply. We must check to see if there is an irreducible quadratic factor.

Recall that the quadratic polynomials in $\mathbb{Z}_2$ are: $x^2, x^2+1, x^2+x, x^2+x+1$. Of these, the only irreducible quadratic is x^2+x+1 (the others have a zero and hence are products of linear factors). Using the division algorithm, we see that $x^4+x+1 = (x^2+x+1)(x^2+x)+1$. Thus x^2+x+1 is not a factor of x^4+x+1 over $\mathbb{Z}_2$.

Thus x^4+x+1 is irreducible over $\mathbb{Z}_2$. Therefore, $k(x) = 3x^4+5x-7$ is irreducible over $\mathbb{Q}$ by the Mod-2 irreducibility test. Hence the original polynomial $h(x)$ is also irreducible over $\mathbb{Q}$.

6. (a) (5 points) List all polynomials with degree less than or equal to 3 in $\mathbb{Z}_2[x]$.

$0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+x, x^3+x^2+1, x^3+x^2+x+1$

(b) (5 points) Find all *irreducible* cubic polynomials in $\mathbb{Z}_2[x]$.

From above, the cubic polynomials in $\mathbb{Z}_2[x]$ are: $x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x+1$

Notice that x^3, x^3+x, x^3+x^2, and x^3+x^2+x have $x=0$ as a root.

Similarly, x^3+1 and x^3+x^2+x+1 have $x=1$ as a root. The remaining polynomials: x^3+x+1 and x^3+x^2+1 are irreducible over $\mathbb{Z}_2[x]$.

(c) (8 points) Let $p(x)$ be one of the polynomials you found in part (b) above. List the elements in $\mathbb{F} = \mathbb{Z}_2[x]/\langle p(x)\rangle$ in standard additive form.

We will take $p(x) = x^3+x+1$ (the results of taking $p(x) = x^3+x^2+1$ are similar). Let $I = \langle p(x)\rangle$.

Then the elements of $\mathbb{F} = \mathbb{Z}_2[x]/\langle p(x)\rangle$ are:

$\{0+I, 1+I, x+I, (x+1)+I, x^2+I, (x^2+1)+I, (x^2+x)+I, (x^2+x+1)+I\}$

(d) (8 points) Find a generator and use it to construct the conversion table from multiplicative to additive form in $\mathbb{F}^*$(you do not need to construct the other half of the conversion table).

Recall that $\mathbb{F} = \mathbb{Z}_2[x]/\langle p(x)\rangle$ can be thought of as the polynomials in $\mathbb{Z}_2[2]$ of degree ≤ 2 with respect to the equation $x^3+x+1=0$, or $x^3 = x+1$. Then the following gives a conversion table from multiplicative to additive form in $\mathbb{F}^*$:

Multiplicative Form	Additive form
1	1
x	x
x^2	x^2
x^3	$x+1$
x^4	x^2+x
x^5	x^2+x+1
x^6	x^2+x

(e) (5 points) How many proper subfields does the field $\mathbb{F}$ constructed above have?

First notice that $\mathbb{F} = GF(8) = GF(2^3)$. Then, by Theorem 22.3, $\mathbb{F}$ has a unique subfield of order p^m for every divisor m of 3. Since the only divisors of 3 are 1 and 3, and 3 would not yield a proper subfield, the only subfield of $\mathbb{F}$ is $GF(2)$.