SECOND MIDTERM
MATH 100B, UCSD, WINTER 17

You have 50 minutes.

There are 6 problems, and the total number of points is 80. Show all your work. *Please make your work as clear and easy to follow as possible.*

Name:_____

Signature:_____

Section instructor:_____

Section Time:_____

Problem	Points	Score
1	15	
2	15	
3	10	
4	10	
5	20	
6	10	
7	10	
8	10	
Total	80	

1. (15pts) *Give the definition of associate elements of an integral domain.*

Elements a and b of an integral domain R are associates if a divides b and b divides a.

(ii) *Give the definition of a Euclidean domain.*

An integral domain is a Euclidean domain if there is a function

$$d\colon R - \{0\} \longrightarrow \mathbb{N} \cup \{0\}$$

such that if a and b are non-zero elements of R then $d(a) \leq d(ab)$ and we may find q and r such that

$$b = aq + r$$

where either $r = 0$ or $d(r) < d(a)$.

(iii) *Give the definition of a unique factorisation domain.*

An integral domain R is a UFD if every non-zero non-invertible element of R is a product of primes and this decomposition is unique, up to order and associates.

2. (15pts) *Let a and b be two elements of an integral domain. Show that the following are equivalent*
(i) a and b are associates.
(ii) there is an invertible element u of R such that $a = ub$.
(iii) $\langle a \rangle = \langle b \rangle$.

Note that a divides b if and only if $b = qa$ for some $q \in R$ if and only if $b \in \langle a \rangle$ if and only if $\langle b \rangle \subset \langle a \rangle$.
Thus (i) and (iii) are clearly equivalent.
If $a = ub$ then b divides a. But if $vu = 1$ then

$$b = 1 \cdot b = (vu)b = va,$$

so that a divides b. Thus (ii) implies (i).
Now suppose that a and b are associates. As b divides a we may find q such that $a = qb$. As a divides b we may find p such that $b = pa$. In this case

$$\begin{aligned} b &= pa \\ &= p(qb) \\ &= (pq)b. \end{aligned}$$

Cancelling, we get that $pq = 1$. Thus p and q are invertible. Hence (i) implies (ii).

3. (10pts) *Show that every Euclidean domain is a PID.*

Let I be an ideal in a Euclidean domain. If I is the zero ideal then $I = \langle 0 \rangle$ so that I is principal.
Otherwise I contains non-zero elements. Pick a non-zero element a of I such that $d(a)$ is minimal. Suppose that $b \in I$. By definition of a Euclidean domain we may find q and r such that

$$b = qa + r,$$

and either $r = 0$ or $d(r) < d(a)$. Note that

$$r = b - qa \in I,$$

so that if $r \neq 0$ then $d(r) \geq d(a)$, by our choice of a.
It follows that $r = 0$. But then a divides b and $b \in \langle a \rangle$. Thus $I = \langle a \rangle$.

4. (10pts) *Let F be a field. Show that $F[x]$ is a Euclidean domain.*

Define a function

$$d\colon F[x] - \{0\} \longrightarrow \mathbb{N} \cup \{0\},$$

by sending a polynomial to its degree.
If f is a polynomial of degree m and g is a polynomial of degree n then fg is a polynomial of degree $m+n$. Thus $d(fg) \geq d(f)$.
We now show that we can find q and r such that

$$g = qf + r,$$

and either $r = 0$ or the degree of r is less than the degree of f.
We proceed by induction on the degree n of g. If $n < m$ then take $q = 0$ and $r = g$. Then $r = g \neq 0$ and $d(r) < d(f)$.
Otherwise we may assume that $n \geq m$. If the leading coefficient of f is a and the leading coefficient of g is b then let $q_0 = cx^{n-m}$, where $c = b/a$. Then

$$g_1 = g - q_0 f$$

has degree less than n. Thus by induction on the degree we can find q_1 and r such that

$$g_1 = q_1 f + r,$$

where either $r = 0$ or $d(r) < d(f)$.
But

$$\begin{aligned} g &= q_0 f + g_1 \\ &= qf + r, \end{aligned}$$

where $q = q_0 + q_1$.
Thus $F[x]$ is a Euclidean domain.

5. (20pts) (i) *Carefully state Gauss' Lemma.*

If $f(x) \in \mathbb{Z}[x]$ is an irreducible element of $\mathbb{Z}[x]$ then it is an irreducible element of $\mathbb{Q}[x]$.

(ii) *Prove that the polynomial*

$$f(x) = x^3 + 2x + 5$$

is an irreducible element of $\mathbb{Q}[x]$.

It suffices to show that it is an irreducible element of $\mathbb{Z}[x]$. Suppose not. As the content of f is one, we can write $f = gh$, where g and h are polynomials with integer coefficient of degree at least one.
We may suppose that the degree of g is at most the degree of h. As the degree of f is three, it follows that g has degree one and h has degree two, so that

$$g(x) = ax + b \qquad \text{and} \qquad h(x) = cx^2 + dx + e.$$

As $ac = 1$ we may suppose that $a = c = \pm 1$. Possibly multiplying g and h by -1 we may assume that $a = c = 1$, so that

$$(x + b)(x^2 + dx + e) = x^3 + 2x + 5.$$

As the coefficient of x^2 is zero, we must have $b + d = 0$. Thus we have

$$(x + b)(x^2 - bx + e) = x^3 + 2x + 5.$$

As $be = 5$, $b = \pm 1$ and $e = \pm 5$ or vice-versa. But $2 = -b^2 + e$, so that $e = 2 + b^2$.
If $b = \pm 1$ then $e = 3$, impossible. If $b = \pm 5$ then $c = 27$, impossible.
Thus $f(x)$ is irreducible.

6. (10pts) *State Eisenstein's criteria. Prove that the polynomial* $f(x)$ $6x^{10}-25x^9+35x^8-15x^7-55x^6+30x^8+40x^5+10x^4-25x^3-5x^2+25x+5$, is an irreducible element of $\mathbb{Q}[x]$.

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with integer coefficients. If p is a prime that does not divide the leading coefficient, p divides every other coefficient and p^2 does not divide the constant coefficient then $f(x)$ is an irreducible element of $\mathbb{Q}[x]$.
Let $p = 5$. Then 5 does not divide the leading coefficient 6, 5 divides every other coefficient and 25 does not divide the constant coefficient 5. Thus $f(x)$ is irreducible, by Eisenstein's criteria applied with $p = 5$.

Bonus Challenge Problems

7. (10pts) *Find all irreducible polynomials of degree at most three over the field with three elements.*

It suffices to find all monic polynomials and then multiply by 2 to get the other polynomials. Every non-zero constant is invertible.
Every degree one polynomial is irreducible; these are

$$x, \qquad x+1, \qquad x+2, \qquad 2x, \qquad 2x+1 \qquad \text{and} \qquad 2x+2.$$

A quadratic or cubic polynomial is irreducible if and only if it has no zeroes.
Suppose that $f(x) = x^2 + ax + b$ is a monic quadratic. 0 is not a zero if and only if $b \neq 0$. 1 is not a zero if and only if $1 + a + b \neq 0$. 2 is not a zero if and only if $1 + 2a + b \neq 0$. If $b = 1$ we must have $a \neq 1$ and $2a \neq 1$ so that $a = 0$. If $b = 2$ then $a \neq 0$ and $2a \neq 0$, so that $a = 1$ or 2. Thus the irreducible quadratics are

$$x^2{+}1, \quad x^2{+}x{+}2, \quad x^2{+}2x{+}2, \quad 2x^2{+}2, \quad 2x^2{+}x{+}1 \quad \text{and} \quad x^2{+}x{+}2.$$

Now consider a monic cubic $f(x) = x^3 + ax^2 + bx + c$. 0 is not a zero if and only if $c \neq 0$. 1 is not a zero if and only if $1 + a + b + c \neq 0$. 2 is not a zero if and only if $2 + a + 2b + c \neq 0$. If $c = 1$ we must have $a + b \neq 1$ and $a + 2b \neq 0$ so that $a = 0$ and $b = 2$, or $a = 1$ and $b = 2$ or $a = 2$ and $b = 0$. If $c = 2$ then $a + b \neq 0$ and $a + 2b \neq 2$ so that $a = 0$ and $b = 2$ or $a = 1$ and $b = 0$ or $b = 1$ or $a = 2$ and $b = 2$. Thus the irreducible monic cubics are

$$x^3{+}2x{+}1, \qquad x^3{+}x^2{+}2x{+}1, \qquad x^3{+}2x^2{+}1 \qquad \text{and} \qquad x^3{+}2x^2{+}x{+}1,$$

$$x^3{+}2x{+}2, \qquad x^3{+}x^2{+}2, \qquad x^3{+}x^2{+}x{+}2 \qquad \text{and} \qquad x^3{+}2x^2{+}x{+}2.$$

If multiply these by two we get the other irreducible cubics.

8. (10pts) *Prove that if R is a UFD then $R[x]$ is a UFD.*

First consider trying to factor $f(x) \in R[x]$ into irreducibles. We can write $f(x) = cg(x)$ where $c \in R$ and the content of $g(x)$ is one. As we can factor c into irreducibles, it suffices to factor $g(x)$ into irreducibles, so we may assume that the content of $f(x)$ is one.
If $f(x)$ is not irreducible then we can find f_1 and g_1 of positive degree such that $f(x) = f_1 g_1$. As the degrees of f_1 and g_1 are smaller than the degree of f it follows that f_1 and g_1 are products of irreducibles, by induction on the degree. Thus every element of $R[x]$ is a product of irreducibles.
Now we turn to proving that irreducible implies prime. Suppose that $f(x) \in R[x]$ is irreducible. Then the content of $f(x)$ is one. It follows by Gauss' Lemma that $f(x) \in F[x]$ is irreducible, so that $f(x) \in F[x]$ is prime.
Suppose that f divides gh. As $f(x) \in F[x]$ is prime it follows that it must divide one of the factors. Suppose it divides $g(x)$ in the polynomial ring $F[x]$. Then we can write $g(x) = f(x)k_1(x)$, where $k_1(x) \in F[x]$. If we clear denominators and cancel then $g(x) = f(x)k(x)$ where $k(x) \in R[x]$ is a multiple of $k_1(x)$. But then $f(x)$ divides $g(x)$ in the polynomial ring $R[x]$. Thus $f(x)$ is a prime in $R[x]$.
Thus $R[x]$ is a UFD.