SECOND MIDTERM
MATH 100B, UCSD, WINTER 24

You have 80 minutes.

There are 7 problems, and the total number of points is 90. Show all your work. *Please make your work as clear and easy to follow as possible.*

Name:_____

Signature:_____

Student ID #:_____

Section instructor:_____

Section Time:_____

Problem	Points	Score
1	15	
2	15	
3	10	
4	10	
5	20	
6	10	
7	10	
8	10	
9	10	
10	10	
Total	90	

1. (15pts) *Give the definition of an irreducible element of an integral domain.*

Let R be an integral domain and let a be a non-zero element of R that is not invertible.
We say that $a \in R$ is irreducible if whenever $a = bc$ then one of b or c is invertible.

(ii) *Give the definition of a prime element of an integral domain.*

Let R be an integral domain and let $p \in R$ be a non-zero element of R. We say that p is prime if $\langle p \rangle$ is a prime ideal.

(iii) *Give the definition of a principal ideal domain.*

Let R be an integral domain. We say that R is a PID if every ideal is principal.

2. (15pts) *Let a and b be two elements of an integral domain. Show that the following are equivalent'*
(i) *a divides b.*
(ii) $b \in \langle a \rangle$
(iii) $\langle b \rangle \subset \langle a \rangle$.

Suppose that (i) holds. Then we may find $q \in R$ so that $b = qa$. In this case $b \in \langle a \rangle$. Thus (i) implies (ii). Now suppose that (ii) holds. Then we may find $q \in R$ such that $b = qa$. But then a divides b. Thus (ii) implies (i). It follows that (i) and (ii) are equivalent.
Suppose that (ii) holds. Then $\langle a \rangle$ is an ideal that contains b. As $\langle b \rangle$ is the smallest ideal that contains b we must have $\langle b \rangle \subset \langle a \rangle$. Thus (ii) implies (iii). Now suppose that (iii) holds. Note that

$$b = 1 \cdot b \in \langle b \rangle \subset \langle a \rangle.$$

Thus $b \in \langle a \rangle$. Hence (iii) implies (ii). It follows that (ii) and (iii) are equivalent.
Hence (i), (ii) and (iii) are all equivalent.

3. (10pts) *Show that if R is a PID and a and b are two elements of R then the greatest common divisor d of a and b exists and that we may find r and $s \in R$ such that $d = ra + sb$.*

Consider the ideal I generated by a and b, $\langle a, b\rangle$. As R is a PID, $I = \langle d\rangle$. As $d \in I$, $d = ra + sb$, for some r and s in R. As $a \in I = \langle d\rangle$, d divides a. Similarly d divides b. Suppose that d' divides a and d' divides b. Then $\langle a, b\rangle \subset \langle d'\rangle$. But then $d'|d$.

4. (10pts) *Show that the Gaussian integers $\mathbb{Z}[i]$ are a Euclidean domain.*

Define a function

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

by sending $a + bi$ to its norm, which is by definition $a^2 + b^2$.
We check the axioms for a Euclidean domain.
Note first that if z is a complex number, then the absolute value of z, defined as the square root of the product of z with its complex conjugate $\bar{z}$, is closely related to the norm of z.
In fact if z is a Gaussian integer $x + iy$, then

$$|z|^2 = z\bar{z} = x^2 + y^2 = d(z).$$

On the other hand, suppose we use polar coordinates, rather than Cartesian coordinates, to represent a complex number,

$$z = re^{i\theta}.$$

Then $r = |z|$.
For any pair z_1 and z_2 of complex numbers, we have

$$|z_1 z_2| = |z_1||z_2|.$$

Indeed this is clear if we use polar coordinates. Now suppose that both z_1 and z_2 are Gaussian integers. If we square both sides of the equation above, we get

$$d(z_1 z_2) = d(z_1)d(z_2).$$

As the absolute value of a Gaussian integer is always at least one, (1) follows easily.
To prove (2), it helps to think about this problem geometrically. First note that one may think of the Gaussian integers as being all points in the plane with integer coordinates. Fix a Gaussian integer α. To obtain all multiples of $\alpha = re^{i\theta}$, that is, the principal ideal $\langle\alpha\rangle$, it suffices to take this lattice, rotate it through an angle of θ and stretch it by an amount r. With this picture, it is clear that given any other Gaussian integer β, there is a multiple of α, call it $q\alpha$, such that the square of the distance between β and $q\alpha$ is at most $r^2/2$. Indeed let $\gamma = \beta/\alpha$. Pick a Gaussian integer q such that the square of the distance between γ and q is at most $1/2$. Then the distance between $\beta = \gamma\alpha$ and $q\alpha$ is at most $r^2/2$. Thus we may write

$$\beta = q\alpha + r,$$

(different r of course) such that $d(r) < d(\alpha)$.

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*

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

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

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

It follows that if $f(x)$ is reducible then it has an integer root $-b$.
Note that $be = 2$. Thus $b = \pm 1, \pm 2$. It is easy to check that ∓ 1 and ∓ 2 are not roots, so that $f(x)$ is irreducible.

6. (10pts) *State Eisenstein's criteria. Prove that the polynomial* $f(x)$ $10x^{10}-9x^9+21x^8-15x^7-33x^6+30x^8+24x^5+6x^4-9x^3-3x^2+9x+3$, 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 $p = 3$. Then 3 does not divide the leading coefficient 10, 3 divides every other coefficient and 9 does not divide the constant coefficient 3. Thus $f(x)$ is irreducible, by Eisenstein's criteria applied with $p = 3$.

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 roots.
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.

Bonus Challenge Problems

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.

9. (10pts) *Construct a field with p^2 elements.*

We simply have to construct an irreducible quadratic polynomial over $\mathbb{F}_p$. If $p = 2$ then $x^2 + x + 1$ will do, as neither 0 nor 1 is a root.
Otherwise we may assume that p is odd. Consider $x^2 - a$. This is irreducible if $x^2 - a$ does not have a root. This is the same as to say that a is not a square.
There are p choices for a. The squares are of the form $b^2 = (-b)^2$. As p is odd $b \neq -b$ and so there are $(p-1)/2$ squares.
Thus $x^2 - a$ is irreducible, for some choice of a. As $\mathbb{F}_p[x]$ is a UFD, it follows that $x^2 - a$ is a prime. Thus

$$\langle x^2 - a \rangle$$

is a prime ideal. The quotient is a field and it has p^2 elements, since an element of the quotient is uniquely represented by a linear polynomial $ax + b$ and there are p^2 choices for a and b.

10. (10pts) *Show that the polynomial*

$$f = x^3y + x^2y^2 + y^3 - y^2 - x - y + 1 \in \mathbb{C}[x, y]$$

is irreducible.

We consider f as an element of $(\mathbb{C}(x))[y]$, so that we write f as polynomial in y,

$$f = y^3 - (x^2 - 1)y^2 + (x^3 - 1)y + (1 - x).$$

Then f belongs to the ring $(\mathbb{C}[x])[y]$ and the content of f is one, as the coefficient of y^3 is 1.
Note that $p = x - 1 \in \mathbb{C}[x]$ is a prime in the ring $\mathbb{C}[x]$. This prime does not divide the leading coefficient, it does divide the other coefficients but the square does not divide the constant coefficient.
Thus f is irreducible, by Eisenstein.