FINAL EXAM
MATH 100B, UCSD, WINTER 17

You have three hours.

There are 9 problems, and the total number of points is 140. 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	25	
2	15	
3	20	
4	15	
5	15	
6	20	
7	10	
8	10	
9	10	
10	25	
11	10	
12	10	
13	10	
14	10	
Total	140	

1. (25pts) (i) *Give the definition of an irreducible element of an integral domain.*

We say that $a \in R$ is irreducible if it is non-zero, not invertible, and whenever $a = bc$ then one of b or c is invertible.

(ii) *Give the definition of a prime ideal.*

An ideal $I \subset R$ is prime if $I \neq R$ and whenever $ab \in I$ then either $a \in I$ or $b \in I$.

(iii) *Give the definition of a maximal ideal.*

An ideal $I \subset R$ is maximal if $I \neq R$ and whenever $I \subset J \subset R$ is an ideal then either $J = I$ or $J = R$.

(iv) *Give the definition of the content of a polynomial.*

If $f(x) \in R[x]$ and R is a UFD then the content of f is the gcd of the coefficients of f.

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

A ring R is a UFD, if every non-zero element of R, which is not a unit, has a factorisation into primes, which is unique up to order and associates.

2. (15pts) (i) *Let R be a commutative ring and let a be an element of R. Prove that the set*

$$\{ ra \mid r \in R \}$$

is an ideal of R.

Call this set I. I is non-empty as $0 = 0 \cdot a \in I$. If x and y are in I, then $x = ra$ and $y = sa$ some r and s. In this case $x + y = ra + sa = (r + s)a \in I$. Similarly if $x \in I$ and $s \in R$, then $x = ra$, some r and $sx = s(ra) = (rs)a \in I$. Thus I is non-empty and closed under addition and scalar multiplication. It follows that I is an ideal.

(ii) *Show that a commutative ring R is a field if and only if the only ideals in R are the zero-ideal $\{0\}$ and the whole ring R.*

Suppose that R is a field and let I be a non-zero ideal of R. Pick $a \in I$, not equal to zero. As R is a field, a is a unit. Let b be the inverse of a. Then $1 = ba \in I$. Now pick $r \in R$. Then $r = r \cdot 1 \in I$. Thus $I = R$.
Now suppose that R has no non-trivial ideals. Pick a non-zero element $a \in R$. It suffices to find an inverse of a. Let I be the ideal generated by a. Then I has the form above. $a = 1 \cdot a \in I$. Thus I is not the zero ideal. By assumption $I = R$ and so $1 \in I$. But then $1 = ba$, some $b \in R$ and b is the inverse of a. Thus R is field.

(iii) *Let $\phi\colon F \longrightarrow R$ be a ring homomorphism, where F is a field. Prove that ϕ is injective.*

Let K be the kernel. As $\phi(1) = 1$, $1 \notin K$. As K is an ideal, and F is field, it follows that K is the zero ideal. But then ϕ is injective.

3. (20pts) (i) *Let R be a commutative ring and let I be an ideal. Show that R/I is an integral domain if and only if I is a prime ideal.*

Let a and b be two elements of R and suppose that $ab \in I$, whilst $a \notin I$. Let $x = a + I$ and $y = b + I$. Then $x \neq I = 0$.

$$\begin{aligned} xy &= (a+I)(b+I) \\ &= ab + I \\ &= I = 0. \end{aligned}$$

As R/I is an integral domain and $x \neq 0$, it follows that $b + I = y = 0$. But then $b \in I$. Hence I is prime.
Now suppose that I is prime. Let x and y be two elements of R/I, such that $xy = 0$, whilst $x \neq 0$. Then $x = a + I$ and $y = b + I$, for some a and b in R. As $xy = I$, it follows that $ab \in I$. As $x \neq I$, $a \notin I$. As I is a prime ideal, it follows that $b \in I$. But then $y = b + I = 0$. Thus R/I is an integral domain.

(ii) *Let R be an integral domain and let I be an ideal. Show that R/I is a field if and only if I is a maximal ideal.*

Note that there a surjective ring homomorphism

$$\phi \colon R \longrightarrow R/I$$

which sends an element $r \in R$ to the left coset $r + I$. Furthermore there is a correspondence between ideals J of R/I and ideals K of R which contain I. Indeed, given an ideal J of R/I, let K be the inverse image of J. As $0 \in J$, $I \subset K$. Given $I \subset K$, let $J = \phi(I)$. It is easy to check that the given maps are inverses of each other. The zero ideal corresponds to I and R/I corresponds to R. Thus I is maximal if and only if R/I only contains the zero ideal and R/I.
On the other hand R/I is a field if and only if the only ideals in R/I are the zero ideal and the whole of R/I.

4. (15pts) *Let R be a principal ideal domain and let a and b be two non-zero elements of R. Show that the gcd d of a and b exists and prove that there are elements r and s of R such that*

$$d = ra + sb.$$

Let $I = \langle a, b\rangle$. As R is a PID, $I = \langle d\rangle$, for some $d \in R$. As $d \in I = \langle a, b\rangle$, there are r and $s \in R$, such that $d = ra + sb$. It remains to prove that d is the gcd.
As $a \in I = \langle d\rangle$, d divides a. Similarly d divides b. Thus d is a common divisor. Now suppose that d' is also a common divisor of a and b. Then a, $b \in \langle d'\rangle$. Thus $d \in I = \langle a, b\rangle \subset \langle d'\rangle$. Thus $d \in \langle d'\rangle$ and d' divides d. Thus d is a greatest common divisor.

5. (15pts) *Find all irreducible polynomials of degree at most four over the field* $\mathbb{F}_2$.

Any linear polynomial is irreducible. There are two such x and $x+1$. A general quadratic has the form $f(x) = x^2 + ax + b$. $b \neq 0$, else x divides $f(x)$. Thus $b = 1$. If $a = 0$, then $f(x) = x^2 + 1$, which has 1 as a zero. Thus $f(x) = x^2 + x + 1$ is the only irreducible quadratic.
Now suppose that we have an irreducible cubic $f(x) = x^3 + ax + bx + 1$. This is irreducible if and only if $f(1) \neq 0$, which is the same as to say that there are an odd number of terms. Thus the irreducible cubics are $f(x) = x^3 + x^2 + 1$ and $x^3 + x + 1$.
Finally suppose that $f(x)$ is a quartic polynomial. The general irreducible is of the form $x^4 + ax^3 + bx^2 + cx + 1$. $f(1) \neq 0$ is the same as to say that either two of a, b and c are equal to zero or they are all equal to one. Suppose that

$$f(x) = g(x)h(x).$$

If $f(x)$ does not have a root, then both g and h must have degree two. If either g or h were reducible, then again f would have a linear factor, and therefore a root. Thus the only possibilty is that both g and h are the unique irreducible quadratic polynomials.
In this case

$$f(x) = (x^2 + x + 1)^2 = x^4 + x^2 + 1.$$

Thus $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$, and $x^4 + x + 1$ are the three irreducible quartics.

6. (20pts) (i) *Let R be a UFD and let $g(x)$ and $h(x) \in R[x]$ be two polynomials whose content is one. Show that the content of the product $f(x) = g(x)h(x) \in R[x]$ is also equal to one.*

Suppose not. As R is a UFD, it follows that there is a prime p that divides the content of $f(x)$. We may write

$$g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \qquad \text{and} \qquad h(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0.$$

As the content of g is one, at least one coefficient of g is not divisible by p. Let i be the first such, so that p divides a_k, for $k < i$ whilst p does not divide a_i. Similarly pick j so that p divides b_k, for $k < j$, whilst p does not d divide b_j.
Consider the coefficient of x^{i+j} in f. This is equal to

$$a_0 b_{i+j} + a_1 b_{i+j-1} + \cdots + a_{i-1}b_{j+1} + a_i b_j + a_{i+1}b_{j+1} + \ldots a_{i+j}b_0.$$

Note that p divides every term of this sum, except the middle one $a_i b_j$. Thus p does not divide the coefficient of x^{i+j}. But this contradicts the definition of the content.

(ii) *Prove that if R is a UFD then so is the polynomial ring $R[x_1, x_2, \ldots, x_n]$.*

By Gauss's Lemma, if S is a UFD, then so is $S[x]$. We proceed by induction on n. The case $n = 1$ is Gauss' Lemma. So suppose that the result is true for $n - 1$. Set

$$S = R[x_1, x_2, \ldots, x_{n-1}].$$

Then S is a UFD, by induction on n. By Gauss' Lemma $S[x_n]$ is a UFD. But it is easy to see that

$$R[x_1, x_2, \ldots, x_n] \simeq S[x_n],$$

and the result follows by induction.

7. (10pts) *State Eisenstein's criteria. Prove that the polynomial* $f(x)$

$5x^{13}-9x^{12}+15x^{11}+18x^{10}-24x^9+6x^8+9x^7-3x^6-18x^5+6x^4+9x^3-3x^2+12x+3,$

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

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial. Suppose that there is a prime p which does not divide the leading coefficient of f, whilst it does divide the other coefficients, and such that p^2 does not divide the constant coefficient. Then f is irreducible over $\mathbb{Q}$.
Apply Eisenstein with $p = 3$.

8. (10pts) *Show that the Gaussian integers* $\mathbb{Z}[i]$ *is 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 $a^2 + b^2$.
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.
We turn to (2). 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 $d(r) < d(\alpha)$.

9. (10pts) *Let p be a prime. Prove that*

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

is irreducible over $\mathbb{Q}$.

By Gauss' Lemma, it suffices to prove that $f(x)$ is irreducible over $\mathbb{Z}$. First note that

$$f(x) = \frac{x^p - 1}{x - 1},$$

as can be easily checked. Consider the change of variable

$$y = x + 1.$$

As this induces an automorphism

$$\mathbb{Z}[x] \longrightarrow \mathbb{Z}[x]$$

by sending x to $x+1$, this will not alter whether or not f is irreducible. In this case

$$\begin{aligned} f(y) &= \frac{(y+1)^p - 1}{y} \\ &= y^{p-1} + \binom{p}{1} y^{p-2} + \binom{p}{2} y^{p-3} + \cdots + \binom{p}{p-1} \\ &= y^{p-1} + py^{p-2} + \cdots + p. \end{aligned}$$

Note that $\binom{p}{i}$ is divisible by p, for all $1 \leq i < p$, and the constant coefficient is not divisible buy p^2, so that we can apply Eisenstein to $f(y)$, using the prime p.

Bonus Challenge Problems

10. (25pts) (i) *Give the definition of a module.*

A module M is an abelian group, together with a commutative ring R, with a scalar multiplication

$$R \times M \longrightarrow M$$

such that for all m and $n \in M$ and r, $s \in R$,

(1) $1 \cdot m = m$.
(2) $(rs)m = r(sm)$.
(3) $(r + s)m = rm + sm$.
(4) $r(m + n) = rm + rn$.

(ii) *Give the definition of a submodule.*

If M is an R-module then a subset N is called a submodule if it is a module with the inherited operations of addition and scalar multiplication.

(iii) *Give the definition of a Noetherian module.*

A module is Noetherian if every submodule is finitely generated.

(iv) *Give the definition of a bilinear map.*

If M, N and P are three R-modules over a ring R a function

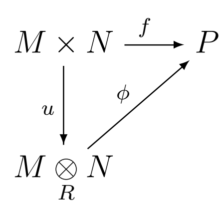
$$f\colon M \times N \longrightarrow P$$

is called bilinear if it is linear in either factor, so that

$$\begin{aligned} f(m_1 + m_2, n) &= f(m_1, n) + f(m_2, n) \qquad & f(rm, n) &= rf(m, n) \\ f(m, n_1 + n_2) &= f(m, n_1) + f(m, n_2) \qquad & f(m, rn) &= rf(m, n). \end{aligned}$$

(v) *Give the definition of the tensor product of two modules.*

Let M and N be two R-modules. The tensor product of M and N is an R-module $M \underset{R}{\otimes} N$, together with a bilinear map $u\colon M \times N \longrightarrow M \underset{R}{\otimes} N$ such that u is universal in the following sense Given any other bilinear map $f\colon M \times N \longrightarrow P$ there is a unique induced R-linear map $\phi\colon M \underset{R}{\otimes} N \longrightarrow P$ such that the following diagram commutes



10. (10pts) *Prove that a module over a Noetherian ring is Noetherian if and only if it is* finitely generated.

I claim that if
$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$
is a short exact sequence of modules then N is Noetherian if and only if M and P are Noetherian. One way around is clear. If N is Noetherian, then M is automatically Noetherian as it is a submodulde of N. If P' is submodule of P, then N' the inverse image of P' is a submodule of N. Then a finite set of generators of N' pushes forward to generators of P'.
Now suppose that M and P are Noetherian. Suppose that we have an ascending chain of submodules of N. By taking their images in P and their inverse images in M, we get two ascending chains of submodules, one inside M and the other inside P. By assumption both must stabilise. But then it is easy to see that the original sequence in N must also stabilise. Hence the claim.
By the claim, the short exact sequence
$$0 \longrightarrow R^{n-1} \longrightarrow R^n \longrightarrow R \longrightarrow 0,$$
and induction on n, it follows that R^n is Noetherian. Picking generators for M, it follows that M is a quotient of R^n, a Noetherian module. But then M is Noetherian.

11. (10pts) *Prove Hilbert's Basis Theorem.*

Let R be a Noetherian ring and let $I \subset R[x]$ be an ideal. It suffices to prove that I is finitely generated. Let $J \subset R$ be the set of leading coefficients of elements of I. It is easy to check that J is an ideal of R. As R is Noetherian, J is finitely generated. Suppose that $J = \langle a_1, a_2, \dots, a_k \rangle$. Pick $f_i \in I$ with leading coefficient a_i and let m be the maximum of the degrees d_i of f_i.

Pick $f \in I$. I claim that there is an element $g \in \langle f_1, f_2, \dots, f_k \rangle$ such that $f - g$ has degree at most m. The proof proceeds by induction on the degree d of f. If this is less than m there is nothing to prove. Otherwise it suffices, by induction on the degree, to decrease the degree by one. Suppose the leading coefficient of f is a. As $a \in J$, there are $r_1, r_2, \dots, r_k \in R$ such that

$$a = \sum r_i a_i.$$

But the coefficient of x^n in

$$f(x) - g(x) = f(x) - \sum r_i x^{d-d_i} f_i(x)$$

is zero by construction.

Let $h(x) = f(x) - g(x) \in I$. Then h has degree less than m. Let M be the R-module consisting of all polynomials of degree less than m. Then $h \in I \cap M$ and M is generated by $1, x, x^2, \dots, x^{m-1}$. In particular M is finitely generated. As R is Noetherian, M is Noetherian. As $I \cap M$ is a submodule of M, it follows that $I \cap M$ is finitely generated. Pick generators $h_1, h_2, \dots, h_l$. Then h is a linear combination of $h_1, h_2, \dots, h_l$ and so f is a linear combination of $f_1, f_2, \dots, f_k$ and $h_1, h_2, \dots, h_l$. It follows that these are generators of I.

12. (10pts) *If M is an R-module, then prove that there is a natural isomorphism*

$$R \underset{R}{\otimes} M \simeq M.$$

We are going to show that M satisfies the properties of the tensor product. First we need to exhibit a bilinear map,

$$u\colon R \times M \longrightarrow M$$

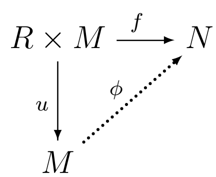
The definition of u is almost forced, send (r, m) to rm. This is clearly a bilinear map. Now suppose we are given a bilinear map

$$f\colon R \times M \longrightarrow N.$$

Define

$$\phi\colon M \longrightarrow N$$

by sending m to $f(1, m)$. We check that the diagram,



commutes. Suppose that $(r, m) \in R \times M$. Then

$$\begin{aligned} \phi \circ u(r, m) &= \phi(rm) \\ &= f(1, rm) \\ &= rf(1, m) \\ &= f(r, m), \end{aligned}$$

where we applied bilinearity of f twice. Thus the diagram commutes. Finally we check that ϕ is R-linear. Suppose that m_1, $m_2 \in M$. Then

$$\begin{aligned} \phi(m_1 + m_2) &= f(1, m_1 + m_2) \\ &= f(1, m_1) + f(1, m_2) \\ &= \phi(m_1) + \phi(m_2). \end{aligned}$$

Now suppose that $r \in R$ and $m \in M$. Then

$$\begin{aligned} \phi(rm) &= f(1, rm) \\ &= rf(1, m) \\ &= r\phi(m). \end{aligned}$$

Thus ϕ is R-linear. Thus M satisfies all the properties of a tensor product and the result is clear.

13. (10pts) *Identify*

$$\mathbb{Q}/\mathbb{Z} \underset{\mathbb{Z}}{\otimes} \mathbb{Q}/\mathbb{Z}.$$

0.
Consider

$$\frac{a}{b} \otimes \frac{c}{d},$$

where a, b, c and d belong to $\mathbb{Z}$.
We compute the product

$$d(\frac{a}{bd} \otimes \frac{c}{d}),$$

in two different ways. By linearity on the left we get

$$\frac{a}{b} \otimes \frac{c}{d}.$$

By linearity on the right we get

$$\frac{a}{bd} \otimes c = \frac{a}{bd} \otimes 0 = 0.$$

Thus

$$\frac{a}{b} \otimes \frac{c}{d} = 0.$$

As every element of the tensor product is a finite linear combination of these elements, it follows that the tensor product is zero.