FINAL EXAM
MATH 100B, UCSD, WINTER 24

You have three hours.

There are 9 problems, and the total number of points is 135. 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	25	
2	10	
3	15	
4	20	
5	10	
6	15	
7	20	
8	10	
9	10	
10	25	
11	10	
12	10	
13	10	
14	10	
15	10	
Total	135	

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

A ring is an integral domain if it is commutative and whenever $ab = 0$ then either $a = 0$ or $b = 0$.

(ii) *Give the definition of a ring homomorphism.*

A ring homomorphism is a function $\phi\colon R \longrightarrow S$ such that

$$\phi(1) = 1 \qquad \phi(a+b) = \phi(a) + \phi(b) \qquad \text{and} \qquad \phi(ab) = \phi(a)\phi(b).$$

for all a and $b \in R$.

(iii) *Give the definition of associate elements of a ring.*

a and $b \in R$ are associates if a divides b and b divides a.

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

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

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

A integral domain R is a Euclidean domain if there is a function

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

which satisfies, for every pair of non-zero elements a and b of R,

(1)
$$d(a) \leq d(ab).$$

(2) There are elements q and r of R such that

$$b = aq + r,$$

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

2. (10pts) (i) *Prove that the kernel of a ring homomorphism* $\phi\colon R \longrightarrow S$ *is an ideal, not equal to* R.

Let $I = \operatorname{Ker}\phi$. Then $0 \in I$ as $\phi(0) = 0$; in particular I is non-empty. If a and $b \in I$ then $\phi(a) = 0$ and $\phi(b) = 0$. Therefore $\phi(a + b) = \phi(a) + \phi(b) = 0 + 0 = 0$. Thus $a + b \in I$ and so I is closed under addition. If $a \in I$ and $r \in R$ then $\phi(ra) = \phi(r)\phi(a) = \phi(r)0 = 0$. Thus $ra \in I$ and so I is an ideal.
$\phi(1) = 1 \neq 0$ so that $1 \notin I$ and $I \neq R$.

(ii) *Let* $I \subset R$ *be an ideal of a ring* R *such that* $I \neq R$. *Show that there is a (natural) well-defined multiplication on the set of left cosets* R/I.

Suppose that x and y are two left cosets. Then $x = a+I$ and $y = b+I$ and we try to define $xy = ab + I$. To check that this makes sense, suppose that $x = a' + I$ and $y = b' + I$. Then we may find i and $j \in J$ such that $a' = a + i$ and $b' = b + j$. It follows that

$$\begin{aligned} a'b' &= (a + i)(b + j) \\ &= ab + aj + ib + ij \\ &= ab + k. \end{aligned}$$

Note that $aj \in I$ as $j \in I$, $ib \in I$ as $i \in I$ and $ij \in I$ as i and $j \in I$. Thus $k \in I$ so that $a'b' + I = ab + I$ and the multiplication is well-defined.

3. (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.

4. (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.

5. (10pts) *Show that every Euclidean domain is a PID.*

Let I be an ideal in a Euclidean domain. We want to show that I is a principal ideal. If I is the zero ideal then $I = \langle 0 \rangle$. Otherwise, pick $a \neq 0$ an element of I, such that $d(a)$ is minimal. I claim that $I = \langle a \rangle$. Suppose not. Clearly $\langle a \rangle \subset I$, so that there must be an element $b \in I$ such that $b \notin \langle a \rangle$.
We may write

$$b = qa + r,$$

where $d(r) < d(a)$ and by assumption $r \neq 0$. But $r = b - qa \in I$, and $d(r) < d(a)$, which contradicts our choice of a.

6. (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.

7. (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.

8. (10pts) (i) *State Eisenstein's criteria. Prove that the polynomial* $f(x)$

$$5x^{13}-21x^{12}+35x^{11}+42x^{10}-56x^{9}+14x^{8}+21x^{7}-7x^{6}-42x^{5}+14x^{4}+21x^{3}-7x^{2}+28x+7$$

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 $\mathbb{Q}$.
We apply Eisenstein with $p = 7$. 7 does not divide the leading coefficient, it does divide the other coefficients and 7^2 does not divide the constant coefficient. Thus the$f(x)$ is an irreducible element of $\mathbb{Q}[x]$.

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

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

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 an R-linear map.*

An R-linear map is a function $\phi \colon M \longrightarrow N$ between two R-modules such that

$$\phi(m + n) = \phi(m) + \phi(n) \qquad \text{and} \qquad \phi(rm) = r\phi(m)$$

for all m and $n \in M$ and $r \in R$.

(iii) *Give the definition of a finitely generated module.*

M is finitely generated if there is a finite set X such that

$$M = \langle X \rangle.$$

(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

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "u"'] & P \\ M \underset{R}{\otimes} N \arrow[ur, "\phi"] & \end{tikzcd}$$

11. (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.

12. (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.

13. (10pts) *Let m and n be integers. Identify $\mathbb{Z}_m \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_n$.*

Let d be the gcd of m and n. I claim that

$$\mathbb{Z}_m \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_n \simeq \mathbb{Z}_d.$$

The proof proceeds in two steps. First observe that

$$\begin{aligned} m(1 \otimes 1) &= m \otimes 1 \\ &= 0 \otimes 1 \\ &= 0. \end{aligned}$$

Similarly $n(1 \otimes 1) = 0$. As $\mathbb{Z}$ is a PID, we may find r and s such that

$$d = rm + sn.$$

Thus

$$\begin{aligned} d(1 \otimes 1) &= (rm + sn)1 \otimes 1 \\ &= r(m(1 \otimes 1) + s(n(1 \otimes 1)) \\ &= 0. \end{aligned}$$

Thus $\mathbb{Z}_m \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_n$ is surely isomorphic to a subgroup of $\mathbb{Z}_d$. It remains to check that no smaller multiple of $1 \otimes 1$ is zero. The best way to prove this is to use the universal property. Let

$$f \colon \mathbb{Z}_m \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_d$$

be the map that sends (a, b) to ab. As d divides both m and n, this map is indeed well-defined. On the other hand it is clearly bilinear. By the universal property, it induces an R-linear map

$$\phi \colon \mathbb{Z}_m \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_n \longrightarrow \mathbb{Z}_d.$$

This map sends $1 \otimes 1$ to $f(1, 1)$, that is, 1. Hence if $k(1 \otimes 1) = 0$, then k is zero in $\mathbb{Z}_d$ and so d divides k. The result follows.

14. (10pts) *Let A be a complex square matrix with characteristic polynomial $(x-1)^3(x+2)^5$ and minimal polynomial $(x-1)^2(x+2)^3$. What are all of the possible Jordan canonical forms (aka Jordan normal forms) for A?*

A is an 8×8 matrix, as the characteristic polynomial has degree 8. The entries on the main diagonal are the zeroes of the characteristic polynomial. Thus there are 3 ones and 5 minus twos.
As the minimal polynomial has $(x-1)^2$ as a factor it follows that there is a 2×2 (and no larger) Jordan block with 1 on the main diagonal. As the minimal polynomial has $(x+2)^3$ as a factor it follows that there is a 3×3 (and no larger) Jordan block with -2 on the main diagonal. Consider the Jordan blocks with eigenvalue -2. There is one of size 3×3. Otherwise there is one 2×2 Jordan block, or two 1×1 Jordan blocks.
Now consider the Jordan blocks with eigenvalue 1. There is one of size 2×2. The only possibility is that there is one more of size 1×1. There are thus two possibilities, the first, one 3×3 and one 2×2 Jordan block with eigenvalue -2, the second, one 3×3 and two 1×1 Jordan block with eigenvalue -2:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 \end{pmatrix}$$

15. (10pts) *Describe all conjugacy classes*

$$\mathrm{GL}_3(\mathbb{F}_2).$$

For each conjugacy class give the order and the minimal polynomial of an element.

The characteristic polynomial is a monic cubic polynomial and zero is not a root:

$$(x+1)^3 = x^3 + x^2 + x + 1 \qquad x^3 + x^2 + 1 \qquad \text{and} \qquad x^3 + x + 1$$

Recall that the last two polynomials are irreducible.
The minimal polynomial divides the characteristic polynomial and has the same roots.
Thus the minimal polynomial is $x + 1$, $(x + 1)^2$, or $(x + 1)^3$, with characteristic polynomial $(x+1)^3$ or x^3+x^2+1 or x^3+x+1, with the same characteristic polynomial.
The first possibility corresponds to the identity matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

This corresponds to three copies of the companion matrix of $x+1$. The order is 1. If we have the second possibility then we have one copy of the companion matrix of $x + 1$ and one copy of the companion matrix of $x^2 + 1$,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

The order is 2. If we have the third possibility then we have the companion matrix of $x^3 + x^2 + x + 1$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

The order is 4. If we have the fourth or fifth possibility then we have the companion matrix of $x^3 + x^2 + 1$ and $x^3 + x + 1$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

The order is 7 in both cases.