FIRST MIDTERM
MATH 100B, UCSD, WINTER 24

You have 80 minutes.

There are 6 problems, and the total number of points is 85. 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	10	
3	15	
4	20	
5	10	
6	15	
7	10	
8	10	
Total	85	

1. (15pts) *Give the definition of the Gaussian integers.*

All complex numbers of the form $a + bi$ where a and b are integers.

(ii) *Give the definition of a zero divisor.*

A non-zero element a of a ring R is a zero divisor if there is a non-zero element b of R such that either $ab = 0$ or $ba = 0$.

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

An ideal I of a ring R is a prime ideal if whenever there are two elements of R such that $ab \in I$ then either $a \in I$ or $b \in I$.

2. (10pts) *Let R and S be two rings.*
(i) *Show that $R \oplus S$ is a ring, where addition and multiplication are defined by*

$$(r_1, s_1)+(r_2, s_2) = (r_1+r_2, s_1+s_2) \qquad \text{and} \qquad (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

It was proved in 100A that $R \oplus S$ is an additive group. The element $(1, 1)$ clearly plays the role of the identity. The fact that multiplication is associative follows similarly to the proof that addition is commutative. We check the distributive rule. Suppose that $x = (a, b)$, $y = (c, d)$, and $z = (e, f) \in R \oplus S$. Then

$$\begin{aligned} x(y + z) &= (a, b)\left((c, d) + (e, f)\right) \\ &= (a, b)(c + e, d + f) \\ &= (a(c + e), b(d + f)) \\ &= (ac + ae, bd + bf) \\ &= (ac + ae, bd + bf) \\ &= (ac, bd) + (ae, bf) \\ &= (a, b)(c, d) + (a, b)(e, f) \\ &= xy + xz. \end{aligned}$$

Similarly the other way around. Thus the distributive law holds.

(ii) *Show that the function*

$$\phi \colon R \oplus S \longrightarrow R \qquad \text{given by} \qquad (r, s) \longrightarrow r$$

is a ring homomorphism.

We already saw in 100A that ϕ is a group homomorphism. $\phi(1, 1) = 1$ and so ϕ sends the identity to the identity. Let $x = (a, b)$ and $y = (c, d)$. We have

$$\begin{aligned} \phi(x)\phi(y) &= \phi(a, b)\phi(c, d) \\ &= ac \\ &= \phi(ac, bd) \\ &= \phi((a, d)(c, d)) \\ &= \phi(xy). \end{aligned}$$

Thus ϕ is a ring homomorphism.

3. (15pts) (i) *Let R be a commutative ring and let a be an element of R. Prove that the set*

$$\{\, ra \,|\, r \in R \,\}$$

is an ideal of R.

$a = 1 \cdot a \in \langle a \rangle$ and so $\langle a \rangle$ is non-empty. Suppose that x and y belong to $\langle a \rangle$. Then we may find r and $s \in R$ such that $x = ra$ and $y = sa$. In this case

$$\begin{aligned} x + y &= ra + sa \\ &= (r + s)a \in \langle a \rangle. \end{aligned}$$

Now suppose that $s \in R$ and $x \in \langle a \rangle$. Then we may $r \in R$ such that $x = ra$. In this case

$$\begin{aligned} sx &= s(ra) \\ &= (sr)a \in \langle a \rangle. \end{aligned}$$

Thus $\langle a \rangle$ 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) *Let R be a ring and let*

$$I_1 \subset I_2 \subset I_3 \subset \cdots \subset I_n \subset \cdots,$$

be an ascending chain of ideals.
(i) *Show that the union*

$$I = \bigcup_{n=1}^{\infty} I_n$$

is an ideal.

We have to show that I is non-empty and closed under addition and multiplication by any element of R.
I is clearly non-empty. For example it contains I_1, which is non-empty. Suppose that a and b belong to I. Then there are two natural numbers m and n such that $a \in I_m$ and $b \in I_n$. Let k be the maximum of m and n. Then a and b are elements of I_k, as I_m and I_n are subsets of I_k. It follows that $a + b \in I_k$, as I_k is an ideal and so $a + b \in I$. Finally suppose that $a \in I$ and $r \in R$. Then $a \in I_n$, for some n. In this case $ra \in I_n \subset I$. Thus I is an ideal.

(ii) *Show that $I = R$ if and only if $I_n = R$ some $n \in \mathbb{N}$.*

One direction is clear. If $I_n = R$ then

$$R = I_n \subset I \subset R$$

so that $I = R$.
Now suppose that $I = R$. Then $1 \in I$. But then $1 \in I_n$, some n and so $a = a \cdot 1 \in I$, for any $a \in R$. Thus $I = R$.

6. (15pts) (i) *Let I and J be two ideals in a ring R. Show that*

$$\frac{R}{I \cap J}$$

is isomorphic to a subring of

$$\frac{R}{I} \oplus \frac{R}{J}.$$

The natural maps

$$R \longrightarrow \frac{R}{I} \qquad \text{and} \qquad R \longrightarrow \frac{R}{J}$$

induce a ring homomorphism

$$\phi\colon R \longrightarrow \frac{R}{I} \oplus \frac{R}{J} \qquad \text{given by} \qquad r \longrightarrow (r + I, r + J).$$

We identify the kernel $K = \operatorname{Ker} \phi$. If $r \in I \cap J$ then $r \in I$ and so $r + I = I$. Similarly $r + J = J$ and so $r \in K$. Now suppose that $r \in K$. Then $r + I = I$ and $r + J = J$. As $r + I = I$ it follows that $r \in I$. Similarly $r \in J$. Thus $K = I \cap J$.
Note that the image of ϕ is a subring and that ϕ is surjective onto its image. The first isomorphism theorem implies that

$$\frac{R}{I \cap J}$$

is isomorphic to a subring of

$$\frac{R}{I} \oplus \frac{R}{J}.$$

(ii) *Show that* $\mathbb{Z}_{mn}$ *and* $\mathbb{Z}_m \oplus \mathbb{Z}_n$ *are isomorphic rings if and only if* m *and* n *are coprime.*

Note that $\mathbb{Z}_m \simeq \mathbb{Z}/\langle m \rangle$. It is clear that

$$\langle mn \rangle \subset \langle m \rangle \cap \langle n \rangle$$

since a multiple of mn is surely a multiple of m and a multiple of n. Suppose that m and n are coprime and that $a \in \langle m \rangle \cap \langle n \rangle$. Then $a = bm$ and $a = cn$. As m and n are coprime, by Euclid's algorithm, there are two integers r and s such that

$$1 = rm + sn.$$

Multiplying by a, we have

$$\begin{aligned} a &= rma + sna \\ &= (rc)mn + (sb)mn \\ &= (rc + sb)mn. \end{aligned}$$

Thus $a \in \langle mn \rangle$ and so $\langle mn \rangle = \langle m \rangle \cap \langle n \rangle$.
It follows that $\mathbb{Z}_{mn}$ is isomorphic to a subring of $\mathbb{Z}_m \oplus \mathbb{Z}_n$. But the cardinality of both sides is mn and so $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \oplus \mathbb{Z}_n$ are isomorphic rings.
Now suppose that m and not n are not coprime. Then the lowest common multiple l of mn and is less than mn.
The characteristic of $\mathbb{Z}_{mn}$ is mn but the characteristic of $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is at most l, since

$$l \cdot (1, 1) = (l, l) = (0, 0).$$

Thus $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \oplus \mathbb{Z}_n$ are not isomorphic.

Bonus Challenge Problems

6. (10pts) *Let R be a commutative ring with the property that given $a \in R$ there is a natural number $n > 1$ such that $a^n = a$.*
Show that every prime ideal is maximal.

Let I be a prime ideal. Then the ring R/I is an integral domain. Note that if $x \in R/I$ then $x = a + I$, some $a \in R$ and so there is a natural number $n > 1$ such that $x^n = x$.
If $x \neq 0$ then we may cancel x as R/I is an integral domain. It follows that $x^m = 1$, where $m = n - 1 \geq 1$. Let $y = x^l$, where $l = n - 2 \geq 0$. Then

$$\begin{aligned} xy &= xx^l \\ &= x^{l+1} \\ &= x^m \\ &= 1. \end{aligned}$$

Thus y is the inverse of x. In particular x is invertible and so R/I is a field.
But then I is maximal.

7. (10pts) *Construct a field with* 121 *elements.*

We just mimic the construction in the book and the lecture notes. Let I be the set of Gaussian integers R of the form $a+bi$ where both a and b are divisible by 11.
It is clear that I is an ideal and $I \neq R$. The quotient ring R/I has 121 elements, since there are eleven possible residues for both the real and imaginary parts. Note that R/I is a field if and only if I is maximal.
We first follow the book. Suppose that $I \subset J$ is an ideal, not equal to I. Then we can find $a+bi \in J$ but not in I. It follows that 11 does not divide at least one of a or b.
Now the possible congruences of a square modulo 11 are 0, $1 = 1^2 = (10)^2$, $4 = 2^2 = 9^2$ and $9 = 3^2 = 8^2$, $5 = 4^2 = 7^2$ and $3 = 5^2 = 6^2$. It follows that if 11 divides an integer of the form $x^2 + y^2$ then 11 must divide both x and y.
Therefore 11 does not divide $c = a^2 + b^2$. As

$$c = (a+bi)(a-bi),$$

it follows that c belongs to J but not to I. As c is coprime to 11 we may find x and y such that

$$1 = xc + 11y.$$

As $11 \in I \subset J$, it follows that $1 \in J$. Thus $J = R$ and so I is maximal.
Instead we can follow the lecture notes. We sketch the details. As R/I is finite it is a field if and only if it is an integral domain. But R/I is an integral domain if and only if I is prime.
Suppose that $(a+bi)(c+di) \in I$ but $a+bi \notin I$. As

$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i,$$

11 divides

$$(ja+b)c - (jb-a)d \qquad \text{and} \qquad (ja+b)d + (jb-a)c,$$

and 11 divides

$$(a+jb)c - (b-ja)d \qquad \text{and} \qquad (a+jb)d + (b-ja)c,$$

and the other way around with j switched between a and b.
By assumption 11 does not divide both a and b. In this case 11 divides a but not b, or vice-versa, or the same is true replacing the pair (a,b) by one of $(a+b, b-a)$, $(2a+b, 2b-a)$, $(a+2b, b-2a)$, $(3a+b, 3b-a)$ and $(a+3b, b-3a)$. Now finish as in the lecture notes.