FIRST MIDTERM
MATH 100B, UCSD, WINTER 17

You have 50 minutes.

There are 5 problems, and the total number of points is 70. Show all your work. *Please make your work as clear and easy to follow as possible.*

Name: ______________________________

Signature: ______________________________

Problem	Points	Score
1	15	
2	10	
3	15	
4	10	
5	20	
6	10	
7	10	
Total	70	

1. (15pts) *Give the definition of a subring.*

A subring S of a ring R is a subset which is a ring with the inherited rules of addition and multiplication.

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

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

$$\phi(x+y) = \phi(x) + \phi(y) \qquad \phi(xy) = \phi(x)\phi(y) \qquad \phi(1) = 1.$$

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

An ideal I in a ring R is maximal if whenever $I \subset J$ is an ideal in R then either $J = I$ or $J = R$.

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) *Let I and J be two ideals in a ring R. Show that*
(i) *$I \cap J$ is an ideal.*

$0 \in I$ and $0 \in J$ so that $0 \in I \cap J$. Thus $I \cap J$ is non-empty. Suppose that a and $b \in I \cap J$. Then a and $b \in I$ and a and $b \in J$. It follows that $a+b \in I$ and $a+b \in J$ so that $a+b \in I \cap J$. Thus $I \cap J$ is closed under addition. Finally suppose that $r \in R$ and $a \in I \cap J$. Then $a \in I$ and $a \in J$. Thus $ra \in I$ and $ra \in J$. It follows that $ra \in I \cap J$ so that $I \cap J$ is an ideal.

(ii) *$I + J$ is an ideal.*

$0 = 0+0 \in I+J$ so that $I+J$ is non-empty. If x and $y \in I+J$ then we can find a and $c \in I$ and b and $d \in J$ such that $x = a+b$ and $y = c+d$. Note that $a+c \in I$ and $b+d \in J$. Then $x+y = (a+b)+(c+d) = (a+c)+(b+d) \in I+J$. Thus $I+J$ is closed under addition. Suppose that $x \in I+J$ and $r \in R$. Then $x = a+b$, where $a \in I$ and $b \in J$. Note that $ra \in I$ and $rb \in J$. We have $rx = r(a+b) = ra+rb \in I+J$. Thus $I+J$ is an ideal.

(iii) *Give an example to show that $I \cup J$ is not necessarily an ideal.*

Let $R = \mathbb{Z}$, let $I = \langle 2 \rangle$ and $J = \langle 3 \rangle$. Then $I \cup J$ is the set of integers divisible by either 2 or 3. Therefore 2 and 3 belong to the union but not $5 = 2+3$. Thus $I \cup J$ is not closed under addition.

4. (10pts) *Let R be a division ring and let $\phi\colon R \longrightarrow S$ be a ring homomorphism. Show that ϕ is injective.*

Let $I = \operatorname{Ker}\phi$. Then I is an ideal. $\phi(1) = 1$ so that $1 \notin I$.
Suppose that $a \in I$ and $a \neq 0$. As R is a division ring, a is invertible and so we may find $b \in R$ such that $ba = 1$. As I is an ideal, it follows that $ba \in I$ so that $1 \in I$, a contradiction.
It follows that $I = \{0\}$. As ϕ is a group homomorphism with trivial kernel, it follows that ϕ is injective.

5. (20pts) *Let X be a set, let R be a ring and let F be the ring of all functions from X to R with pointwise addition and multiplication.*
(i) *Show that $f \in F$ is invertible if and only if $f(x) \in R$ is invertible, for all $x \in X$.*

Suppose that f is invertible, with inverse g, so that $fg = gf = 1$. If $x \in X$ then

$$1 = (fg)(x) = f(x)g(x) \qquad \text{and} \qquad 1 = (gf)(x) = g(x)f(x)$$

so that $g(x)$ is the inverse of $f(x)$. In particular $f(x)$ is invertible.
Now suppose that $f(x)$ is invertible, for all $x \in X$. Define a function $g \colon X \longrightarrow R$ by sending x to the inverse of $f(x)$. In this case

$$(fg)(x) = f(x)g(x) = 1 \qquad \text{and} \qquad (gf)(x) = g(x)f(x) = 1.$$

Thus $fg = gf = 1$ and so g is the inverse of f.

(ii) *Let Y be a subset of X and let G be the ring of all functions from Y to R. Show that the map $\phi \colon F \longrightarrow G$ which sends a function $f \colon X \longrightarrow R$ to its restriction to Y is a ring homomorphism.*

If f and $g \in F$ then

$$\phi(f+g) = (f+g)|_Y = f|_Y + g|_Y = \phi(f) + \phi(g) \qquad \text{and}$$
$$\phi(fg) = (fg)|_Y = (f|_Y)(g|_Y) = \phi(f)\phi(g).$$

On the other hand, it is clear that the constant function 1, restricts to the constant function 1. Thus $\phi(1) = 1$ and ϕ is a ring homomorphism.

(iii) *If* $X = [0, 1]$*,* $R = \mathbb{R}$ *and* $I \subset F$ *is the set of functions vanishing at* $1/2$ *then show that* I *is a maximal ideal.*

If $Y = \{1/2\}$ and ϕ is the ring homomorphism above then the kernel of ϕ is I. G is a copy of $\mathbb{R}$, since a function on Y is determined by its value at $1/2$. By the Isomorphism Theorem, $F/I \simeq \mathbb{R}$. But an ideal is maximal if and only if the quotient ring is a field. Therefore I is maximal.

(iv) *If* $X = [0, 1]$*,* $R = \mathbb{R}$ *and* $J \subset F$ *is the set of functions vanishing at both* $1/3$ *and* $2/3$ *then show that* I *is not a prime ideal.*

Let

$$f(x) = \begin{cases} 0 & \text{if } x = 1/3 \\ 1 & \text{otherwise} \end{cases} \qquad g(x) = \begin{cases} 0 & \text{if } x = 2/3 \\ 1 & \text{otherwise.} \end{cases}$$

Then f and $g \notin J$ but $fg \in J$. Thus J is not prime.

Bonus Challenge Problems

6. (10pts) *Let R be the ring of all 2×2 matrices with entries in $\mathbb{Z}_p$, p a prime. Let G be the subset of all 2×2 matrices with non-zero determinant. How many elements does G have?*

We just want to count the number of invertible 2×2 matrices with entries in the field $\mathbb{Z}_p$. Now a square matrix is invertible if and only if its rows are a basis.

So we just want to count the number of ordered bases of the vector space $\mathbb{Z}_p^2$. We have to pick two independent vectors. We pick them one at a time. We are free to pick any vector for the first vector, except zero. So there are $p^2 - 1$ choices of the first vector. For the second vector we just have to make sure we don't pick a multiple of the first vector. There are p different multiples of the first vector, so there are $p^2 - p$ choices for the second vector.

Thus there are $(p^2 - 1)(p^2 - p)$ elements of G.

7. (10pts) *Construct a field with 49 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 7.
It is clear that I is an ideal and $I \neq R$. The quotient ring R/I has 49 elements, since there are seven 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 7 does not divide at least one of a or b.
Now the possible congruences of a square modulo 7 are 0, $1 = 1^2 = 6^2$, $4 = 2^2 = 5^2$ and $2 = 3^2 = 4^2$. It follows that if 7 divides an integer of the form $x^2 + y^2$ then 7 must divide x and y.
Therefore 7 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 7 we may find x and y such that

$$1 = xc + 7y.$$

As $7 \in I \subset J$, 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 field if and only if it is an integral domain, 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

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

7 divides

$$ac - bd \qquad \text{and} \qquad ad + bc.$$

Adding and subtracting these together we get that 7 divides

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

7 divides

$$(2a+b)c - (2b-a)d \qquad \text{and} \qquad (2a+b)d + (2b-a)c,$$

and 7 divides

$$(a+2b)c - (b-2a)d \qquad \text{and} \qquad (a+2b)d + (b-2a)c.$$

By assumption 7 does not divide both a and b. In this case 7 divides a but not b, or vice-versa, of the same is true replacing the pair (a,b) by $(a+b, b-a)$, $(2a+b, 2b-a)$, $(a+2b, b-2a)$. Now finish as in the lecture notes.