SECOND MIDTERM
MATH 18.703, MIT, SPRING 13

You have 80 minutes. This test is closed book, closed notes, no calculators.

There are 6 problems, and the total number of points is 100. Show all your work. *Please make your work as clear and easy to follow as possible.* Points will be awarded on the basis of neatness, the use of complete sentences and the correct presentation of a logical argument.

Name:________________________________

Signature:________________________________

Student ID #:________________________________

Problem	Points	Score
1	15	
2	15	
3	15	
4	15	
5	20	
6	15	
7	10	
8	10	
Presentation	5	
Total	100	

1. (15pts) Give the definition of a ring.

Solution: A ring is a set R, together with two binary operations, known as addition, denoted $+$, and multiplication, denoted $\cdot$, such that that $(R, +)$ is an abelian group, and multiplication is associative and there is a unit for multiplication. Finally we require the distributive law, that is given a, b and $c \in R$,

$$a(b+c) = ab + ac \qquad \text{and} \qquad (b+c)a = ba + ca.$$

(ii) Give the definition of an integral domain.

Solution:
A ring R is an integral domain if multiplication is commutative and there are no zero divisors, that is

$$ab = 0$$

implies that either $a = 0$ or $b = 0$.

(iii) Give the definition of a prime ideal.

Solution: A subset I of R is said to be a prime ideal if it is an additive subgroup and for all a and b in R,

$$ab \in I$$

if and only if either a or b is in I.

2. (15pts) (i) State the Sylow Theorems.

Solution: Let G be a group of order of order n and let p be a prime dividing n.
Then the number of Sylow p-subgroups is equal to one modulo p, divides n and any two Sylow p-subgroups are conjugate.

(ii) Prove that if G is a group of order pq, where p and q are distinct primes, then G is not simple.

Solution:
We may assume that $p < q$. Let n_q be the number of Sylow q-subgroups. Then $n_q = 1$ or $n_q \geq q + 1$ and n_q divides n. Therefore n_q divides p so that $n_q = 1$. But then there is a unique subgroup Q of order q and so Q is normal in G.

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.

Solution: Suppose that b and c are in I. Then $b = ra$ and $c = sa$, for some r and s in R. In this case

$$\begin{aligned} b + c &= ra + sa \\ &= (r + s)a \in I. \end{aligned}$$

Similarly $-b = (-r)a \in I$. Thus I is an additive subgroup as it is non-empty and closed under addition and scalar multiplication. Finally suppose that $b \in I$ and that $s \in R$. Then $sb = s(ra) = (rs)a$. Thus I is closed under multiplication by R and so I is an ideal.

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

Solution:

Suppose that R is a field and let I be an ideal of R, not the zero ideal. Pick $a \in I$, $a \neq 0$. As R is a field, a is a unit, that is, there is an element $b \in R$ such that $ba = 1$. But $ba \in I$, as $a \in I$. Thus $1 \in I$. Now pick any element $r \in R$. Then $r = r \cdot 1 \in I$. Thus $I = R$.

Now suppose that the only ideals in R are the zero ideal and the whole of R. Let $a \in R$ be a non-zero element of R. Let $I = \langle a \rangle$. Then I is an ideal of R. As $a = 1 \cdot a \in I$, it follows that I is not the zero ideal. By hypothesis it follows that $I = R$. But then $1 \in I$ and so $1 = ra$, for some $r \in R$. But then a is a unit. As a is arbitrary, R is a field.

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

Solution:

Let $I = \operatorname{Ker} \phi$. Then I is an ideal of R. $\phi(1) = 1 \neq 0$ so that $I \neq R$. Thus $I = \{0\}$. Suppose that $\phi(a) = \phi(a)$. Then $\phi(a - b) = 0$, so that $b - c \in I = \{0\}$. Hence $b - c = 0$ and so $b = c$. But then ϕ is injective.

4. (15pts) (i) Let R be an integral domain. If $ab = ac$, for $a \neq 0$, b, $c \in R$, then show that $b = c$.

Solution: We have
$$a(b - c) = ab - ac = 0.$$
As $a \neq 0$ and R is an integral domain, $b - c = 0$, so that $b = c$.

(ii) Show that every finite integral domain is a field.

Solution:
It suffices to prove that every non-zero element a of a finite integral domain R has an inverse. Let
$$f \colon R \longrightarrow R$$
be the function $f(x) = ax$. Suppose that $f(b) = f(c)$. Then $ab = ac$ so that $a(b - c) = 0$. As $a \neq 0$ and R is an integral domain $b = c$. Thus f is injective. As R is finite, it follows that f is surjective. Thus there is an element $b \in R$ such that $ba = f(b) = 1$. But then a is a unit and R is a field.

5. (20pts) (i) Let R be a ring and let I be an ideal. Show that R/I is a domain if and only if I is a prime ideal.

Solution:
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 a 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 p be a prime number. Show that the ring $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ is a field.

Solution: Almost by definition $p\mathbb{Z} = \langle p \rangle$ is a prime ideal. Thus $\mathbb{Z}_p$ is an integral domain. On the other hand this ring is certainly finite and so it is a field.

6. (15pts) (i) State the (first) Isomorphism Theorem.

Solution: Let

$$\phi\colon R \longrightarrow S$$

be a surjective ring homomorphism, with kernel I. Then S is isomorphic to the quotient R/I.

(ii) Let X be a set and let R be a ring. Let F be the set of all functions from X to R. Let $x \in X$ be a point of X and let I be the ideal of all functions in F vanishing at x. Prove that I is a prime ideal iff R is a domain.

Solution:
Define a map

$$\phi\colon F \longrightarrow R$$

by sending $f \in F$ to its value at x, $f(x) \in R$. It is easy to check that ϕ is a ring homomorphism. Given $r \in R$, let f be the constant function with value r. Then $\phi(f) = r$. Hence ϕ is surjective. Suppose that $\phi(f) = 0$. Then $f(x) = 0$, that is, f vanishes at x. Thus the kernel of ϕ is I. By the Isomorphism Theorem $F/I \simeq R$. Thus I is prime iff R is an integral domain.

Bonus Challenge Problems

7. (10pts) Let m and n be coprime integers. Prove that

$$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \oplus \mathbb{Z}_n.$$

Solution: Let $I = \langle m \rangle$ and $J = \langle n \rangle$. Consider the canonical maps

$$R \longrightarrow R/I \qquad \text{and} \qquad R \longrightarrow R/J.$$

These are ring homomorphisms. By the universal property of the direct sum, the map

$$\phi \colon \mathbb{Z} \longrightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n,$$

defined by sending $a \in \mathbb{Z}$ to $(a+I, b+J)$ is a ring homomorphism. The kernel of ϕ is equal to $I \cap J$. Clearly $\langle mn \rangle \subset I \cap J$. I claim that we have equality. Suppose that $a \in I \cap J$. Then $a = bm$ and $a = cn$. As m and n are coprime, there are integers r and s such that $rm + sn = 1$. Thus

$$\begin{aligned} a &= a \cdot 1 \\ &= a(rm + sn) \\ &= ram + san \\ &= (rc)nm + sbmn \\ &= (rc + sb)mn. \end{aligned}$$

Thus $a \in \langle mn \rangle$ and the claim follows. By the Isomorphism Theorem, there is an injective ring homomorphism

$$\mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n.$$

As both sides are of cardinality mn, this map must in fact be an isomorphism.

8. (10pts) Construct a field with nine elements.

Solution:

Let $R = \mathbb{Z}[i]$ be the ring of Gaussian integers. Let M be the ideal of all Gaussian integers of the form $a + bi$, where both a and b are divisible by three. Then R/M is easily seen to have nine elements.

Indeed as a group, $\mathbb{Z}[i]$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$. In fact define a map by sending $a + bi$ to (a, b). Under this identification, M corresponds to the subgroup $3\mathbb{Z} \times 3\mathbb{Z}$ and the quotient is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Thus it suffices to prove that R/M is a field, that is, 0that M is maximal. Suppose not. Then there would be an ideal I, such that $M \subset I \subset \mathbb{Z}[i]$, where both inclusions are strict. Pick $a + bi \in I$ not in M.

Consider $a^2 + b^2$. As this is equal to $(a - bi)(a + bi)$, $a^2 + b^2$ is an integer belonging to I. On the other hand, 3 does not divide one of a or b and as the only squares modulo three are 0 and 1, in fact $a^2 + b^2$ is not divisible by 3. Thus I contains a number congruent to 1 modulo 3 (either $a^2 + b^2$ or its inverse). As M contains 3, then so does I and so I contains 1. But then $I = \mathbb{Z}[i]$. It follows that M is indeed maximal.