SECOND MIDTERM
MATH 103B, UCSD, SPRING 16

You have 50 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:________________________________

Problem	Points	Score
1	15	
2	10	
3	20	
4	10	
5	15	
6	15	
7	10	
8	10	
Total	85	

1. (15pts) (i) *Give the definition of a commutative ring.* A ring is a triple $(R, +, .)$ where $(R, +)$ is an abelian group, multiplication is a binary operation which is associative and the distributive laws holds, that is

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{and} \qquad (b + c) \cdot a = b \cdot a + c \cdot a,$$

where a, b and c are any elements of the ring.

(ii) *Give the definition of a zero-divisor.* Elements a and b of a ring are zero-divisors if they are non-zero and $a \cdot b = 0$.

(iii) *Give the definition of an integral domain.* A commutative ring, with unity, $1 \neq 0$ with no integral divisors.

2. (10pts) *Find the orders of the following quotient groups:*

(i)

$$\frac{\mathbb{Z}_4 \times \mathbb{Z}_{12}}{\langle 2 \rangle \times \langle 2 \rangle}$$

The order of $\mathbb{Z}_4 \times \mathbb{Z}_{12}$ is $4 \cdot 12 = 48$. The order of $\langle 2 \rangle \times \langle 2 \rangle$ is $2 \cdot 6 = 12$. The order of the quotient is the number of left cosets which by Lagrange is $48/12 = 4$.

(ii)

$$\frac{\mathbb{Z}_4 \times \mathbb{Z}_{12}}{\langle (2,2) \rangle}.$$

The order of $\mathbb{Z}_4 \times \mathbb{Z}_{12}$ is $4 \cdot 12 = 48$. The order of $\langle (2,2) \rangle$ is the order $(2,2)$ which is 6. The order of the quotient is the number of left cosets which by Lagrange is $48/6 = 8$.

3. (20pts) *Determine whether the given operations are defined on the set and whether they give a ring. If we don't get a ring, explain why. If we do get a ring, state whether the ring is commutative, whether it has unity and whether it is a field.*

(i) $n\mathbb{Z}$ with the usual addition and multiplication.

Yes, this is a subring of the integers, since the sum of two multiples of n is a multiple of n and the product of two multiples of n is a multiple of n. It is commutative, it won't contain 1 unless $n = \pm 1$ and it is never a field, since even if $n = \pm 1$, $2 \in n\mathbb{Z} = \mathbb{Z}$ does not have an inverse.

(ii) $\mathbb{Z}^+$, all non-negative integers, with the usual addition and multiplication.

No this is not a ring. It is not a group under addition. The problem is that the positive integers won't have additive inverses. For example, 2 does not have an additive inverse.

4. (10pts) *Let R be a ring of characteristic 3. Compute and simplify $(a+b)^6$ for $a,\ b \in R$.*

By the binomial theorem we have

$$\begin{aligned}(a+b)^6 &= a^6 + 6 \cdot a^5 b + 15 \cdot a^4 b^2 + 20 \cdot a^3 b^3 + 15 \cdot a^2 b^4 + 6 \cdot a b^5 + b^6 \\ &= a^6 + 20 \cdot a^3 b^3 + b^6 \\ &= a^6 + 2 \cdot a^3 b^3 + b^6,\end{aligned}$$

since the characteristic is 3.

5. (15pts)
(i) *What is the remainder when you divide* 9^{42} *by* 13*?*
As 13 is prime, Fermat implies that

$$9^{12} = 1 \mod 13.$$

$42 = 36 + 6 = 3 \cdot 12 + 6$. So

$$\begin{aligned} 9^{42} &= (9^{12})^3 \cdot 9^6 \\ &= 9^6 \\ &= 3^{12} \\ &= 1 \mod 13. \end{aligned}$$

(ii) *What is the remainder when you divide* 8^{63} *by* 21*?*
$\varphi(21) = \varphi(3)\varphi(7) = (3-1)(7-1) = 12$.
As 8 is coprime to 21, Euler implies that

$$8^{12} = 1 \mod 21.$$

Therefore

$$\begin{aligned} 8^{63} &= 8^{60} \cdot 8^3 \\ &= (8^{12})^5 \cdot 8^3 \\ &= 8^3 \\ &= 2^9 \\ &= 2^4 \cdot 2^5 \\ &= 16 \cdot 32 \\ &= (-5) \cdot 11 \\ &= -55 \\ &= 8. \end{aligned}$$

6. (15pts) *Show that the rings $2\mathbb{Z}$ and $5\mathbb{Z}$ are not isomorphic.*
Suppose not. Let

$$\phi\colon 2\mathbb{Z} \longrightarrow 5\mathbb{Z},$$

be a ring isomorphism. Let $a = \phi(2)$. As ϕ is an additive group homomorphism, we have

$$\begin{aligned}\phi(4) &= \phi(2+2)\\ &= \phi(2)+\phi(2)\\ &= a+a\\ &= 2a.\end{aligned}$$

As ϕ is a ring homomorphism, we also have

$$\begin{aligned}\phi(4) &= \phi(2\cdot 2)\\ &= \phi(2)\cdot\phi(2)\\ &= a\cdot a\\ &= a^2.\end{aligned}$$

Thus $a^2 = 2a$. As $5\mathbb{Z} \subset \mathbb{C}$ we can intepret a as a complex solution of the polynomial equation

$$x^2 = 2x.$$

We know the complex solutions to this equation, $x = 0$ and $x = 2$. As $2 \notin 5\mathbb{Z}$ we must have $a = 0$. But then

$$\phi(0) = 0 = \phi(2)$$

so that ϕ is not one to one. But then ϕ is not an isomorphism.

Bonus Challenge Problems

7. (10pts) *Let H be a subgroup of a group G. Prove the following are equivalent*

(1) $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.
(2) $gHg^{-1} = H$ for all $g \in G$.
(3) $gH = Hg$ for all $g \in G$.

See the lecture notes.

8. (10pts) *Show if n is a natural number with prime factorisation*

$$n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$$

then

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-2}) \dots (p_m^{k_m} - p_m^{k_m-1}).$$

See the lecture notes.