MTH 310, Section 001
Abstract Algebra I and Number Theory

Midterm 1

Instructions: You have 50 minutes to complete the exam. There are five problems, worth a total of fifty points. You may not use any books or notes. Partial credit will be given for progress toward correct proofs.

Write your solutions in the space below the questions. If you need more space use the back of the page. Do not forget to write your name in the space below.

Name: ______________________________

Question	Points	Score
1	10	
2	10	
3	10	
4	10	
5	10	
Total:	50	

Problem 1.

(a) [5pts.] State the Division Algorithm.

> **Solution:** Let $a, b \in \mathbb{Z}$ with $b > 0$. There are integers q and r such that $0 \leq r < q$ and $a = bq + r$.

(b) [5pts.] Prove that the cube a^3 of an integer a must be of one the forms $9k$, $9k + 1$, and $9k + 8$. [Hint: Start by applying the Division Algorithm with $q = 3$.]

> **Solution:** Any integer a may be written as one of $3q$, $3q + 1$, $3q + 2$. In each of the three cases we have:
>
> $$(3q)^3 = 27q^3 = 9(3q^3)$$
>
> $$(3q + 1)^3 = 27q^3 + 27q^2 + 9q + 1 = 9(3q^3 + 3q^2 + q) + 1$$
> $$(3q + 2)^3 = 27q^3 + 54q^2 + 18q + 8 = 9(3q^3 + 6q^2 + 3q) + 8$$

Problem 2.

(a) [5pts.] State the Fundamental Theorem of Arithmetic.

> **Solution:** Every integer $n \in \mathbb{Z}$ may be factored as a product of primes $n = p_1 p_2 \dots p_r$ which is unique in the sense that if $n = q_1 q_2 \dots q_s$ is a second prime factorization, $r = s$ and up to reordering $q_i = \pm p_i$

(b) [5pts.] Let p be a prime integer. If $p | a^n$ for some a, does it follow that $p^n | a^n$?

> **Solution:** Yes. Recall that if a prime p divides a product $c_1 c_2 \dots c_n$, then $p | c_i$ for some $1 \leq i \leq n$. So in particular if $p | a \cdot a \cdot \dots \cdot a$, then in particular $p | a$. Hence $p^n | a^n$.

Problem 3.

(a) [5pts.] Suppose R is a ring with identity. What does it mean to say that an element a of R is a unit?

> **Solution:** A nonzero element a of R is a unit if there exists $u \in R$ such that $ua = 1_R = au$.

(b) [5pts.] Let R be a four-element ring with identity $\{0, 1, a, b\}$ such that a and b are both units. Write down the full multiplication table for R. [Hint: What is ab?]

Solution: There are exactly four interesting products, namely a^2, ab, ba, b^2. Consider the product ab. Since a and b are units, they are in particular not zero divisors. So $ab \neq 0$. Suppose that $ab = a$. Then if u is the multiplicative inverse of a, we have $uab = ua$, implying that $b = 1$. As this is untrue, we see that ab cannot be a. Similarly it cannot be b. Ergo $ab = 1$. Likewise $ba = 1$ and a and b are multiplicative inverses. Now consider a^2. Since a is not its own multiplicative inverse, $a^2 \neq 1$. If $a^2 = a$, multiplying by b on both sides shows that $a = 1$, which is untrue. So $a^2 = b$. Similarly $b^2 = a$. Hence we conclude that $ab = ba = 1$, $a^2 = b$, and $b^2 = a$.

Problem 4.

(a) [5pts.] Define a subring of a ring R.

Solution: A subring S of R is a subset of R which is a ring with the same operations of addition and multiplication.

(b) [5pts.] Is $S = \{(a, b) : a + b = 0\}$ a subring of $\mathbb{Z} \times \mathbb{Z}$?

Solution: No; it is not multiplicatively closed. We observe that S contains $(1, -1)$ and $(2, -2)$, but their product $(2, 2)$ is not in S.

Problem 5.

Consider the ring $\mathbb{Z}_{12}$.

(a) [5pts.] What are the units and zero divisors in $\mathbb{Z}_{12}$?

Solution: The units in $\mathbb{Z}_1 2$ are the elements a such that $(a, 12) = 1$, namely $1, 5, 7, 11$. The zero divisors are everything else nonzero, namely $2, 3, 4, 6, 8, 9, 10$.

(b) [5pts.] What are the solutions to the equation $x^2 + 2x = 0$ in $\mathbb{Z}_{12}$?

Solution: Checking this by hand we see that $0, 4, 6, 10$ are solutions.

This page is for scratch work. Feel free to tear it off. Do not write anything you want graded on this page unless you indicate *very clearly* that this is the case on the page of the corresponding problem.