MTH 310, Section 001
Abstract Algebra I and Number Theory

Sample 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. Justify all of your answers. 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.] Use the Euclidean Algorithm to determine $(272, 1479)$.

Solution: We observe that

$$\begin{aligned} 1479 &= 272(5) + 119 \\ 272 &= 119(2) + 34 \\ 119 &= 34(3) + 17 \\ 34 &= 17(2) + 0 \end{aligned}$$

We conclude that $(1479, 272) = (272, 119) = (119, 34) = (34, 17) = (17, 0) = 17$.

(b) [5pts.] Prove that for integers a, b, c, we have $((a, b), c) = (a, (b, c))$.

Solution: Let $d = (a, b)$, $e = (d, c)$, $f = (b, c)$, $g = (a, f)$. The goal is to show that $e = g$. We observe that $e|d$ and $e|c$; since $d|a$ and $d|b$, we see that $e|a$ and $e|b$, so that indeed e divides all of a, b, c. In particular, since $e|b$ and $e|c$, we have that $e|f$, since f is the gcd of b and c. But then since $e|a$ and $e|f$, we have $e \leq g$, since g is the gcd of a and f.

Doing the same argument in the other direction implies that $g \leq e$. Ergo $e = g$.

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.] If $p > 3$ is a prime number, prove that $p^2 + 2$ is necessarily composite. [Hint: Consider the possible remainders when p is divided by 3.]

Solution: Recall that by the Division Algorithm, an arbitrary integer may be written as one of $3k, 3k + 1$, and $3k + 2$. But indeed since p is prime and not 3 or -3, we may rule out $p = 3k$, so we have that either $p = 3k + 1$ or $p = 3k + 2$. Then we see that either

$$\begin{aligned} p^2 + 2 &= (3k + 1)^2 + 2 \\ &= 9k^2 + 6k + 1 + 2 \\ &= 3(3k^2 + 2k + 1) \end{aligned}$$

or

$$\begin{aligned} p^2 + 2 &= (3k+2)^2 + 2 \\ &= 9k^2 + 12k + 4 + 2 \\ &= 3(3k^2 + 4k + 2) \end{aligned}$$

In either case we observe that p^2+2 is necessarily divisible by 3, hence composite.

Problem 3.

Consider the ring $\mathbb{Z}_8$.

(a) [5pts.] Give a complete list of subrings of $\mathbb{Z}_8$.

Solution: Any subring must contain $\{0\}$. The set $S_1 = \{0\}$ is a perfectly good subring. Any subset S_2 which contains 1 must also contain $1 + 1 = 2$, $1 + 2 = 3$, and so on, and thus must be all of $\mathbb{Z}_8$. So $S_2 = \mathbb{Z}_8$ is another subring, and no further subrings can contain 1. Indeed, since $3 + 3 + 3 = 1$, $-(5+5+5) = -(-1) = 1$, and $-(7) = 1$, we perceive that by closure of subrings under addition and taking additive inverses, no subring S of R may contain any of $1, 3, 5, 7$.

Suppose a subring S of R contains 2. Then it also contains $2+2 = 4$, $2+2+2 = 6$, and $2 + 2 + 2 + 2 = 0 = 8$. Indeed, it is easy to check that $S_3 = \{0, 2, 4, 6\}$ is a subring, and therefore the only proper subring containing 2. Because $6 + 6 = 2$, it is also the only proper subring of $\mathbb{Z}_8$ containing 6. Finally, we observe that $S_4 = \{0, 4\}$ is a subring; it is clearly additively and multiplicatively closed, it contains 0, and 4 is its own multiplicative inverse.

(b) [5pts.] What are the solutions to $x^3 + x^2 + x + 1 = 0$ in $\mathbb{Z}_8$?

Solution: We observe that

$$\begin{aligned} 0^3 + 0^2 + 0 + 1 &= 1 \neq 0 \\ 1^3 + 1^2 + 1 + 1 &= 4 \neq 0 \\ 2^3 + 2^2 + 2 + 1 &= 15 \neq 0 \\ 3^3 + 3^2 + 3 + 1 &= 40 = 0 \\ 4^3 + 4^2 + 4 + 1 &= 85 \neq 0 \\ 5^3 + 5^2 + 5 + 1 &= 156 \neq 0 \\ 6^3 + 6^2 + 6 + 1 &= 260 \neq 0 \\ 7^3 + 7^2 + 7 + 1 &= 400 = 0 \end{aligned}$$

We see that the solutions are 3 and 7.

Problem 4.

(a) [5pts.] Let R be a ring. What does it mean for an element $a \in R$ to be a zero divisor?

> **Solution:** We say that $a \in R$ is a zero divisor if $a \neq 0$ and there exists some nonzero $c \in R$ such that either $ca = 0_R$ or $ac = 0_R$.

(b) [5pts.] Prove that if ab is a zero divisor in a ring R, then at least one of a and b is a zero divisor.

> **Solution:** First we observe that neither a nor b is 0_R, since by assumption ab is not. Suppose that ab is a zero divisor. Then there is some nonzero $c \in R$ such that $c(ab) = 0_R$ or $(ab)c = 0_R$. In the first case, we have that $(ca)b = 0_R$. So either $ca = 0_R$ or b is a zero divisor. In the case that $ca =)_R$ we see that since c and a are nonzero, it follows that a is a zero divisor. SO at least one of a and b is a zero divisor. The case $(ab)c = 0_R$ is similar.

Problem 5.

Decide whether the following two subsets of $\mathbb{R}$ are subrings of $\mathbb{R}$.

(a) [5pts.] $S = \{a\sqrt{2} : a \in \mathbb{Z}\}$

> **Solution:** No; it is not multiplicatively closed. We see that $\sqrt{2} \times \sqrt{2} = 2$ is not an element of S.

(b) [5pts.] $T = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$

> **Solution:** Yes. Recall that it suffices to show that T is closed under subtraction and multiplication. We observe that
>
> $$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2}$$
>
> $$(a + b\sqrt{2}) \times (c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2}.$$

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.