MTH 310, Section 001
Abstract Algebra I and Number Theory

Midterm 2

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.] What does it mean for two rings R and S to be isomorphic?

> **Solution:** Two rings R and S are isomorphic if there exists a map $f : R \to S$ such that f is a bijection and $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

(b) [5pts.] Let R be a ring and $R^* \subset R \times R$ be the subring $R^* = \{(r, r) : r \in R\} \subset R \times R$. Prove the map $\phi : R \to R^*$ which takes $\phi(r) = (r, r)$ is an isomorphism.

> **Solution:** We observe that ϕ is clearly a bijection. Moreover $\phi(a) + \phi(b) = (a, a) + (b, b) = (a + b, a + b) = \phi(a + b)$ and $\phi(a)\phi(b) = (a, a) \times (b, b) = (ab, ab) = \phi(ab)$.

Problem 2.

(a) [5pts.] Let R be a commutative ring, and let $\phi : R[x] \to R$ be the map

$$\phi(a_n x^n + \cdots + a_1 x + a_0) = a_0$$

that takes each polynomial to its constant term. Prove that ϕ is a surjective homomorphism of rings.

> **Solution:** Certainly ϕ is surjective since any constant polynomial maps to itself in R. Moreover, we see that given $a_n x^n + \cdots + a_1 x + a_0$ and $b_m x^m + \cdots + b_0$ in $R[x]$, the constant term of the sum is $a_0 + b_0$ and the constant term of their product is $a_0 b_0$, we see that $\phi(a_n x^n + \cdots + a_1 x + a_0) + \phi(b_m x^m + \cdots + b_0) = a_0 + b_0 = \phi((a_n x^n + \cdots + a_1 x + a_0) + (b_m x^m + \cdots + b_0))$ and $\phi(a_n x^n + \cdots + a_1 x + a_0) \times \phi(b_m x^m + \cdots + b_0) = a_0 \times b_0 = \phi((a_n x^n + \cdots + a_1 x + a_0)(b_m x^m + \cdots + b_0))$.

(b) [5pts.] Let R be a commutative ring, and let $f(x) \in R[x]$. Give an example to show that the polynomial function

$$\begin{aligned} f : R &\to R \\ a &\mapsto f(a) \end{aligned}$$

is not necessarily a homomorphism.

> **Solution:** Consider $f(x) = x + 1$ in $\mathbb{Q}[x]$. We see that $f(0) = 1 \neq 0$. Homomorphisms take the additive identity to itself, so the polynomial function induced by f cannot be a homomorphism.

Problem 3.

(a) [5pts.] State the Rational Root Theorem.

Solution: Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. If $\frac{r}{s}$ is a root of $f(x)$ such that r and s are coprime integers, then $r|a_0$ and $s|a_n$.

(b) [5pts.] Decide whether the following polynomials are irreducible in $\mathbb{Q}[x]$, justifying your answers.

- $f(x) = x^4 + 3x + 1$
- $g(x) = x^{372} + 3x^{87} - 9x^{19} + 15x^{13} + 21$
- $h(x) = x^4 + 7x^2 + 1$

Solution: We see that $g(x)$ is irreducible by Eisenstein's Criterion with $p = 3$. For $f(x)$, we reduce modulo 2, obtaining $\bar{f}(x) = x^4 + x + 1$. This has no root in $\mathbb{Z}_2$, so if it factors it factors as the product of two irreducible quadratics. But there is only one irreducible quadratic in $\mathbb{Z}_2$, to wit $x^2 + x + 1$, and $(x^2 + x + 1)(x^2 + x + 1) = x^4 + x^2 + 1 \neq x^4 + x + 1$. So $\bar{f}(x)$ is irreducible in $\mathbb{Z}_2[x]$, hence in $\mathbb{Q}[x]$.

For $h(x)$, we observe that by the Rational Root Theorem, the only possible rational roots of $h(x)$ are ± 1. Since $h(1) = h(-1) = 9$, h has no rational roots and thus no linear factors in $\mathbb{Q}[x]$. So if h factors it factors as two quadratics; since factorization over $\mathbb{Q}$ implies factorization over $\mathbb{Z}$ we may take these to be monic. Suppose that $(x^4 + 7x^2 + 1) = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd$. Then $c = -a$, leaving us with equations

$$\begin{aligned} b - a^2 + d &= 7 \\ a(b - d) &= 0 \\ bd &= 1 \end{aligned}$$

We see that either $b = d = 1$ or $b = d = -1$. If $b = d = 1$, we have $a^2 = -5$; if $b = d = -1$ we have $a^2 = -9$. In either event there are no solutions. So $h(x)$ is irreducible.

Problem 4.

Let F be a field.

(a) [4pts.] Define the greatest common divisor $f(x)$ and $g(x)$ of two polynomials in $F[x]$.

Solution: The greatest common divisor of $f(x)$ and $g(x)$ is the unique monic polynomial of largest degree that divides both $f(x)$ and $g(x)$.

(b) [3pts.] What is the greatest common divisor of $x^3 + 1$ and $x^4 + x^3 + x^2$ in $\mathbb{Z}_2[x]$?

Solution: We have $x^3+1 = (x+1)(x^2+x+1)$ and $x^4+x^3+x^2 = x^2(x^2+x+1)$. So the greatest common divisor is x^2+x+1.

(c) [3pts.] What is the greatest common divisor of x^3+1 and $x^4+x^3+x^2$ in $\mathbb{Q}[x]$?

Solution: We have $x^3+1 = (x+1)(x^2-x+1)$ and $x^4+x^3+x^2 = x^2(x^2+x+1)$. We perceive that the greatest common divisor is the constant polynomial 1.

Problem 5.

Consider the polynomial $p(x) = x^2+1$ in $\mathbb{Z}_3[x]$.

(a) [4pts.] Is $p(x)$ irreducible in $\mathbb{Z}_3[x]$?

Solution: Yes; we observe that $p(0) = 1$ and $p(1) = p(2) = 2$, so $p(x)$ has no root in $\mathbb{Z}_3$ and therefore no linear factor. Hence it is irreducible.

(b) [4pts.] Write out the multiplication table for $\mathbb{Z}_3[x]/(x^2+1)$.

Solution:

The elements of $\mathbb{Z}_3[x]$ are $\{[0],[1],[2],[x],[x+1],[x+2],[2x],[2x+1],[2x+2]\}$. Here is the table:

×	[0]	[1]	[2]	[x]	[x+1]	[x+2]	[2x]	[2x+1]	[2x+2]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[x]	[x+1]	[x+2]	[2x]	[2x+1]	[2x+2]
[2]	[0]	[2]	[1]	[2x]	[2x+2]	[2x+1]	[x]	[x+2]	[x+1]
[x]	[0]	[x]	[2x]	[2]	[x+2]	[2x+2]	[1]	[x+1]	[2x+1]
[x+1]	[0]	[x+1]	[2x+2]	[x+2]	[2x]	[1]	[2x+1]	[2]	[x]
[x+2]	[0]	[x+2]	[2x+1]	[2x+2]	[1]	[x]	[x+1]	[2x]	[2]
[2x]	[0]	[2x]	[x]	[1]	[2x+1]	[x+1]	[2]	[2x+2]	[x+2]
[2x+1]	[0]	[2x+1]	[x+2]	[x+1]	[2]	[2x]	[2x+2]	[x]	[1]
[2x+2]	[0]	[2x+2]	[x+1]	[2x+1]	[x]	[2]	[x+2]	[1]	[2x]

(c) [2pts.] Prove that the ring you constructed is not isomorphic to $\mathbb{Z}_9$.

Solution: The ring we constructed is a field, and in particular has eight units; $\mathbb{Z}_9$ has four units.

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.