MTH 310, Section 001
Abstract Algebra I and Number Theory

Sample 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. 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.] Let R and S be rings. What does it mean for a map $f : R \to S$ to be an isomorphism?

> **Solution:** We say that f is an isomorphism if f is a bijection and $f(a+b) = f(a)+f(b)$ and $f(ab) = f(a)f(b)$.

(b) [5pts.] Let $f : \mathbb{R}[x] \to \mathbb{R}[x]$ be the derivative map, given by

$$f(a_0 + a_1 x + \cdots + a_n x^n) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

Is f an isomorphism?

> **Solution:** No; observe that $f(x+1) = 1$ and $f(x+2) = 1$ but $f((x+1)(x+2)) = f(x^2+3x+2) = 2x+3 \neq (1)(1)$. So f does not preserve multiplication and is not a homomorphism.

Problem 2.

(a) [5pts.] State Eisenstein's Criterion.

> **Solution:** Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. If there is a prime p such that p divides $a_0, a_1, \ldots a_{n-1}$, p does not divide a_n, and p^2 does not divide a_0, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

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

- $f(x) = x^{273} + 11$
- $g(x) = x^5 + 2x + 1$
- $h(x) = x^3 + 16x^2 + 9x + 1$

> **Solution:** We see that $f(x)$ is irreducible by Eisenstein's Criterion with $p = 11$. For $h(x)$ we reduce to $\mathbb{Z}_2[x]$, obtaining $\bar{h}(x) = x^3 + x + 1$. This is irreducible in $\mathbb{Z}_2[x]$ since it is a degree three polynomial with no roots in $\mathbb{Z}_2$. Ergo $h(x)$ is also irreducible in $\mathbb{Q}[x]$.
>
> Finall consider $g(x)$. By the Rational Root Theorem, any rational root $\frac{r}{s}$ of $g(x)$ with $(r,s) = 1$ has the property that r divides the constant term of $g(x)$ and s divides the leading term of $g(x)$, both of which are 1. So the only possible rational roots are ± 1. But $g(1) = 4$ and $g(-1) = -2$, so in fact $g(x)$ has no rational roots and therefore no linear factors over $\mathbb{Q}[x]$. Hence if $g(x)$ factors, it factors as a quadratic and a cubic; since factoring in $\mathbb{Q}[x]$ is the same as factoring in $\mathbb{Z}[x]$, we can assume that both factors are monic. If we have $x^5 + 2x + 1 =$

$(x^2+ax+b)(x^3+cx^2+dx+e) = x^5+(a+c)x^4+(b+ac+d)x^3+(e+ad+bc)x^2+(ae+bd)x+be$. First we see that $a+c=0$, so $c=-a$. This leaves us with the equations

$$\begin{aligned} b-a^2+d &= 0 \\ e+ad-ab &= 0 \\ ae+bd &= 2 \\ be &= 1 \end{aligned}$$

We see that either $b=e=1$ or $b=e=-1$. If $b=e=1$, we have $a+d=2$ and $a^2=d+1$, so $0=a^2-d-1=a^2+a-3$, which does not have any solutions in the integers. If $b=e=-1$, we have $a+d=-2$ and $a^2=d-1$, so $0=a^2-d+1=a^2+a+3$, which also does not have any solutions in the integers. So $g(x)$ does not factor in $\mathbb{Z}[x]$, and therefore also does not factor in $\mathbb{Q}[x]$.

Problem 3.

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

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

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

(b) [4pts.] Write out the addition and multiplication tables for $R=\mathbb{Z}_3[x]/(x^2+2x+2)$.

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

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

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

(c) [2pts.] Is R a field?

Solution: Yes; $p(x)$ is irreducible. [Alternately, we can see from the table that every element of R has a muliplicative inverse.]

Problem 4.

(a) [3pts.] State the Remainder Theorem.

Solution: Let $f(x)$ be a polynomial in $F[x]$ for F a field. If $f(x)$ is divided by $(x-a)$, the remainder is $f(a)$.

(b) [4pts.] Give an example of a nonzero polynomial $f(x)$ in $\mathbb{Z}_3[x]$ which induces the zero polynomial function on $\mathbb{Z}_3$.

Solution: Consider $f(x) = x(x-1)(x-2)$, which has the property that $f(a) = 0$ for every $a \in \mathbb{Z}_3$ and therefore induces the zero polynomial function.

(c) [3pts.] What is the smallest possible degree such a nonzero polynomial can have?

Solution: A polynomial that induces the zero polynomial on $\mathbb{Z}_3$ has a root at every element of $\mathbb{Z}_3$ hence three roots. Such a polynomial must have degree at least three.

Problem 5.

Let F be a field and $h : F \to R$ a homomorphism of rings.

(a) [5pts.] Show that if there is some $c \neq 0_F$ such that $h(c) = 0_R$, then h is necessarily the zero homomorphism.

Solution: If $c \neq 0$, then since F is a field, there is an element c^{-1} such that $cc^{-1} = 1$. Let a be any element of F, then $h(a) = h(acc^{-1}) = h(a)h(c)h(c^{-1}) = h(a)(0_R)h(c^{-1}) = 0_R$. So h is the zero homomorphism.

(b) [5pts.] Show that h is either injective or the zero homomorphism.

Solution: Suppose that h is not injective, so that there are some $a, b \in F$ with $a \neq b$ and $h(a) = h(b)$. Then $a - b \neq 0$ and $h(a - b) = h(a) - h(b) = 0$, so by part (a), h is the zero homomorphism. Hence h is either injective or is the zero homomorphism.

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.