MATH 333 — FINAL EXAM

May 23, 2016

NAME: Solutions

1. You do not need to give full proofs; short justifications are fine just like on midterm 2.

   (a) Give an example of an integral domain that is not a field.

   The ring $\mathbb{Z}$ is an integral domain that is not a field. This has been our typical example from class.

   (b) Give an example of a ring R and a subring S where S is not an ideal.

   Let $R = \mathbb{Q}$ and $S = \mathbb{Z}$. We know $\mathbb{Z}$ is a ring and a subset of $\mathbb{Q}$, so it is a subring. It is not an ideal because for example $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z}$.

   (c) Give an example of a maximal ideal $\mathfrak{m}$ in a ring R of your choice.

   Let $p \in \mathbb{Z}$ be a prime number. Then $p\mathbb{Z}$ is a maximal ideal as was shown in class.

   (d) Give an example of a prime ideal $\mathfrak{p}$ in a ring R so that $\mathfrak{p}$ is not a maximal ideal.

   Let $\langle x \rangle \subset \mathbb{Z}[x]$. We have $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$, which is an integral domain but not a field. Thus $\langle x \rangle$ is a prime ideal but not a maximal ideal.

2. Let $a = 2340$ and $b = 7007$. Find $d = \gcd(a, b)$ and express d as a linear combination of a and b.

   We use the Euclidean algorithm here:

$$\begin{aligned} 7007 &= 2(2340) + 2327 \\ 2340 &= 1(2327) + 13 \\ 2327 &= 13(179) \end{aligned}$$

   Thus, $\gcd(2340, 7007) = 13$. We also have

$$\begin{aligned} 13 &= 2340 + (-1)2327 \\ &= 2340 + (-1)(7007 + (-2)(2340)) \\ &= 3(2340) + (-1)(7007). \end{aligned}$$

Name: ____

3. Let R and S be rings. Consider the set $I = \{(r, 0_S) : r \in R\} \subset R \times S$.

   (a) Prove that I is an ideal.

   Proof. Observe that $0_{R\times S} = (0_R, 0_S) \in I$. Let $(r_1, 0_S), (r_2, 0_S) \in I$ and $(r, s) \in R \times S$. We have $(r_1, 0_S) + (r_2, 0_S) = (r_1 + r_2, 0_S) \in I$, $(r, s)(r_1, 0_S) = (rr_1, 0_S) \in I$ and $(r_1, 0_S)(r, s) = (r_1 r, 0_S) \in I$. Thus, I is an ideal. □

   (b) Show that the map $\varphi : R \times S \to S$ defined by $\varphi((r, s)) = s$ is a surjective ring homomorphism.

   Proof. Let $s \in S$. We have $\varphi((0_R, s)) = s$ so φ is surjective.
   Let $(r_1, s_1), (r_2, s_2) \in R \times S$. We have

$$\begin{aligned}\varphi((r_1, s_1) + (r_2, s_2)) &= \varphi((r_1 + r_2, s_1 + s_2)) \\ &= s_1 + s_2 \\ &= \varphi((r_1, s_1)) + \varphi((r_2, s_2))\end{aligned}$$

   and

$$\begin{aligned}\varphi((r_1, s_1)(r_2, s_2)) &= \varphi((r_1 r_2, s_1 s_2)) \\ &= s_1 s_2 \\ &= \varphi((r_1, s_1))\varphi((r_2, s_2)).\end{aligned}$$

   Thus, φ is a surjective ring homomorphism. □

   (c) Show that $(R \times S)/I \cong S$.

   Proof. Since we have $\varphi : R \times S \to S$ from part (b) is a surjective ring homomorphism, if we show $\ker \varphi = I$ we are done by the first isomorphism theorem. Let $(r, 0_S) \in I$. We have $\varphi((r, 0_S)) = 0_S$ so $(r, 0_S) \in \ker \varphi$. Thus, $I \subset \ker \varphi$. Now let $(r, s) \in \ker \varphi$. This implies that $s = \varphi((r, s)) = 0_S$, so $(r, s) = (r, 0_S) \in I$. Hence, $\ker \varphi \subset I$ and so $I = \ker \varphi$ as claimed. □

4. Let $R = \mathbb{R}[x]$ and consider the subset $S = \{f \in R : f(2) = 0\}$. Is S a subring of R? Be sure to justify your answer.

Proof. Observe that 0_R is the zero polynomial, which clearly induces the zero function on $\mathbb{R}$ so $0_R(s) = 0$ and thus $0_R \in S$. Let $f, g \in S$. We have $(f + g)(2) = f(2) + g(2) = 0$ and $fg(2) = f(2)g(2) = 0 \cdot 0 = 0$ so $f + g, fg \in S$. Observe that if $f = \sum_{j=0}^{n} a_j x^j$, then $-f = \sum_{j=0}^{n} (-a_j)x^j$. From this we see that for any $r \in \mathbb{R}$, the polynomial function $-f : \mathbb{R} \to \mathbb{R}$ is given by $(-f)(r) = -f(r)$ for all $r \in \mathbb{R}$. Thus, we have $(-f)(2) = -f(2) = -0 = 0$ so $-f \in S$. Hence, S is a subring of R. □

5. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>1}$. Prove that if $\gcd(a, n) = 1$ then the equation $[a]_n x = [b]_n$ has a solution in $\mathbb{Z}/n\mathbb{Z}$.

Proof. Assume $\gcd(a, n) = 1$. Then there exists $s, t \in \mathbb{Z}$ so that $as + nt = 1$. Multiplying this by b gives $a(bs) + n(bt) = b$. Considering this equation in $\mathbb{Z}/n\mathbb{Z}$ we see $[a(bs)]_n = [b]_n$, i.e., $x = [bs]_n$ is a solution to the equation. □

6. (a) Let R and S be rings and $\varphi : R \to S$ a ring homomorphism. Prove that if $I \subset S$ is an ideal, then $\varphi^{-1}(I) = \{r \in R : \varphi(r) \in I\}$ is an ideal in R.

Proof. We know that $0_S \in I$ because I is an ideal. Since $\varphi(0_R) = 0_S$, we have $0_R \in \varphi^{-1}(I)$. Let $r_1, r_2 \in \varphi^{-1}(I)$ and $r \in R$. We have $\varphi(r_1), \varphi(r_2) \in I$ by definition. Observe that $\varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2) \in I$ because $\varphi(r_1), \varphi(r_2) \in I$ and I is an ideal. Since $\varphi(r_1 - r_2) \in I$, we have $r_1 - r_2 \in \varphi^{-1}(I)$ by definition. Similarly, we have $\varphi(rr_1) = \varphi(r)\varphi(r_1) \in I$ because $\varphi(r_1) \in I$, $\varphi(r) \in S$ and I is an ideal. Thus, $rr_1 \in \varphi^{-1}(I)$. The same argument shows $r_1 r \in \varphi^{-1}(I)$ and so $\varphi^{-1}(I)$ is an ideal in R. □

(b) Let $\mathfrak{p}$ be a prime ideal in S. Prove that $\varphi^{-1}(\mathfrak{p}) = \{r \in R : \varphi(r) \in \mathfrak{p}\}$ is a prime ideal in S.

Proof. We know from part (a) that $\varphi^{-1}(\mathfrak{p})$ is an ideal, so it only remains to show it is prime. Let $ab \in \varphi^{-1}(\mathfrak{p})$. This gives that $\varphi(a)\varphi(b) = \varphi(ab) \in \mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal, we have $\varphi(a) \in \mathfrak{p}$ or $\varphi(b) \in \mathfrak{p}$, i.e., $a \in \varphi^{-1}(\mathfrak{p})$ or $b \in \varphi^{-1}(\mathfrak{p})$. Thus, $\varphi^{-1}(\mathfrak{p})$ is a prime ideal if $\mathfrak{p}$ is. □

7. Let F be a field, $f \in F[x]$ a non-constant polynomial, and consider the principal ideal $I = \langle f \rangle$.

(a) Prove that for any coset $h + I$ there is a polynomial $r \in F[x]$ with $\deg r < \deg f$ or $r = 0_F$ so that $h + I = r + I$.

Proof. Let $h + I \in F[x]/I$. The division algorithm allows us to write $h = fq + r$ with $\deg r < \deg f$ or $r = 0_F$. Observe since $I = \langle f \rangle$ we have $fq \in I$. Thus, $h + I = r + I$, as claimed. □

For the rest of this problem consider the case where $F = \mathbb{Z}/2\mathbb{Z}$ and $f = x^2 + x + [1]_2$.

(b) Does f have any roots in $\mathbb{Z}/2\mathbb{Z}$? Is f irreducible? Be sure to justify your answer.
Observe that $f([0]_2) = [1]_2$ and $f([1]_2) = [1]_2$ so f has no roots in $\mathbb{Z}/2\mathbb{Z}$. If f were reducible it would necessarily be the product of two linear factors, which would imply f has a root. Thus, f is irreducible.

(c) Use part (a) to determine all the elements of $S = F[x]/\langle f \rangle$. (This should not require any division!) Write out addition and multiplication tables for S.

We have from part (a) that the elements of this quotient ring are precisely $[0]_2 + I, [1]_2 + I, x + I$, and $x + [1]_2 + I$. We drop the brackets for the tables.

$+$	$0+I$	$1+I$	$x+I$	$x+1+I$
$0+I$	$0+I$	$1+I$	$x+I$	$x+1+I$
$1+I$	$1+I$	$0+I$	$x+1+I$	$x+I$
$x+I$	$x+I$	$x+1+I$	$0+I$	$1+I$
$x+1+I$	$x+1+I$	$x+I$	$1+I$	$0+I$

$\cdot$	$0+I$	$1+I$	$x+I$	$x+1+I$
$0+I$	$0+I$	$0+I$	$0+I$	$0+I$
$1+I$	$0+I$	$1+I$	$x+I$	$x+1+I$.
$x+I$	$0+I$	$x+I$	$x+1+I$	$1+I$
$x+1+I$	$0+I$	$x+1+I$	$1+I$	$x+I$

where we have used that $(x+I)(x+I) = x^2+I = x+1+I$ since $x^2+x+1+I = 0+I$ and $-x-1+I = x+1+I$ since we are working over $\mathbb{Z}/2\mathbb{Z}$, $(x+I)(x+1+I) = (x^2+x+I) = (x+1+x+I) = 1+I$, and $(x+1+I)(x+1+I) = (x^2+2x+1+I) = (x+1+1+I) = x+I$.

(d) Is S isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$? Be sure to justify your answer.

One can verify from the tables that S is a field. Note that $\mathbb{Z}/4\mathbb{Z}$ is not a field as $[2]_4$ is a zero divisor and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not a field because $([0]_2, [1]_2)$ is a zero divisor as $([0]_2, [1]_2)([1]_2, [0]_2) = ([0]_2, [0]_2)$. Thus, S cannot be isomorphic to either of these rings.