Math 412 Winter 2023 Midterm Exam

Time: 120 mins.

(a) Answer each question in the space provided. If you require more space, you may use the blank page at the end of this exam, but you must clearly indicate in the provided answer space that you have done so.

(b) You may use any results proved in class, on the homework, or in the textbook, except for the specific question being asked. You should clearly state any facts you are using.

(c) Remember to show all your work.

(d) No calculators, notes, or other outside assistance allowed.

Best of luck!

uniqname: _____

ID number: _____

Question	Points	Score
1	12	
2	15	
3	12	
4	16	
5	12	
6	17	
7	16	
Total:	100	

1. (12 points) Write complete, precise definitions for, or precise mathematical characterizations of, each of the following italicized terms. Be sure to include any quantifiers as needed.

   (a) Two integers a and b are *relatively prime*

   Solution: if $\gcd(a, b) = 1$.

   (b) An *equivalence relation* on a set S is a rule used to compare elements of S satisfying...

   Solution:

   1. reflexivity: $x \equiv x$ for any $x \in S$,
   2. symmetry: $x \equiv y$ then $y \equiv x$ for any $x, y \in S$,
   3. transitivity: $x \equiv y$ and $y \equiv z$ then $x \equiv z$ for any $x, y, z \in S$,

   where $\equiv$ is the relation in study.

   (c) The *kernel* of a ring homomorphism

   Solution: The set of elements in the domain of the ring homomorphism that get mapped to zero of the codomain. To be more precise, if $\varphi : R \to S$ is a ring homomorphism, then the kernel of φ, denoted $\ker\varphi$ is the set

   $$\ker\varphi = \{x \in R \mid \varphi(x) = 0_S\}.$$

   (d) Let I be an ideal of a ring R and let $y \in R$. The *congruence class of y modulo I*

   Solution: is the set

   $$y + I = \{y + z \mid z \in I\}.$$

2. (15 points) In this problem, you do not need to justify your answers. Give an example of...

   (a) a positive integer n, and values $[a]_n$ and $[b]_n$ in $\mathbb{Z}_n$, neither or which is $[0]_n$, such that $[a]_n x = [b]_n$ has more than one solution.

   Solution: For example $n = 4$, $a = b = 2$. (it is neccesary that $\gcd(a, n)$ is not 1.)

   (b) an element that is a zero-divisor that is not nilpotent in the ring $\mathbb{Z}_{120}$.

   Solution: For example $[2]_{120}$.
   Any number that is not relatively prime to 120 is a zero-divisor in $\mathbb{Z}_{120}$. You showed in the homework that any number that is divisible by all prime divisors of 120 (that is, 2,3, and 5) is nilpotent. So any multiple of 30 is nilpotent.

   (c) Rings R and S, neither of which is the zero ring, and a ring homomorphism φ from R to S such that φ is neither injective nor surjective.

   Solution: For example $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2[x]$ such that $\varphi([a]_4) = \varphi([a]_2$.

   (d) Two polynomials, $f(x), g(x) \in \mathbb{Z}_2[x]$ such that $f([0]_2) = g([0]_2)$ and $f([1]_2) = g([1]_2)$ but $f(x) \neq g(x)$.

   Solution: For example $f(x) = 0$ and $g(x) = x^2 + x$.

   (e) a nonzero ring T and an ideal $I \subsetneq T$ such that T/I is a domain, but T is not a domain.

   Solution: For example $T = \mathbb{Z}_4$ and $T = \{[0]_4, [2]_4\}$.

3. (12 points) For each of the statements below, indicate clearly if the statement is TRUE or FALSE. Give a brief, one-sentence justification.

   (a) There is no surjective homomorphism from $\mathbb{Z}_8$ to $\mathbb{Z}_7$.

   Solution: True. Since 7 does not divide 8, there is NO homomorphism from $\mathbb{Z}_8$ to $\mathbb{Z}_7$.

   (b) Let $\mathbb{F}$ be a field and R a ring with R not the zero ring, and let $\varphi : \mathbb{F} \to R$ be a ring homomorphism. Then φ is injective.

   Solution: True. Recall that $\ker \varphi$ is an ideal. Thus the only two options for $\ker \varphi$ are $\{0_\mathbb{F}\}$ and $\mathbb{F}$. The second one is not possible since $\varphi(1_\mathbb{F}) = 1_R \neq 0_R$.

   (c) The set of all matrices with determinant equal to zero is an ideal in the ring $M_2(\mathbb{R})$, the set of all 2×2 matrices.

   Solution: False. For instance, matrixes $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ have determinant zero but their sum has determinant one.

(d) Let $f(x)$ be an irreducible polynomial in $\mathbb{Z}_7[x]$, and let $I = (f(x))$. Suppose that $f(x)$ does not divide $g(x)$. Then there exists a polynomial $h(x) \in \mathbb{Z}_7[x]$ such that

$$(g(x) + I)(h(x) + I) = [3]_7 + I$$

Solution: True. By the given information we get that $g(x)$ as a multiplicative inverse in the quotient ring. So, there is some $q(x) \in \mathbb{Z}_7[x]$ such that

$$(g(x) + I)(q(x) + I) = [1]_7 + I.$$

Multiply by $[3]_7$ both sides of the equation above to get the desired result.

4. (16 points) (a) Let $n(x)$ and $m(x)$ be two polynomials in $\mathbb{Q}[x]$ such that $\gcd(n(x), m(x)) = 1$. Prove that if $n(x)$ divides the product $m(x)p(x)$ for some $p(x) \in \mathbb{Q}[x]$, then $n(x)$ divides $p(x)$.

Solution: By the Bezout identity, there exist $u(x), v(x) \in \mathbb{Q}[x]$ such that

$$u(x)n(x) + v(x)m(x) = 1.$$

Multiplying both sides by $p(x)$ we have

$$u(x)n(x)p(x) + v(x)m(x)p(x) = p(x).$$

Note that $n(x)$ divides $m(x)p(x)$ implies that $m(x)p(x) = q(x)n(x)$ for some $q(x) \in \mathbb{Q}[x]$. Substituting this to the above equation, we obtain

$$n(x)(u(x)p(x) + v(x)q(x)) = p(x).$$

So, $n(x)$ divides $p(x)$, as desired.

For the rest of the problem, let $n(x) = x^4 - 3$ and $m(x) = x + 2$ be two polynomials in $\mathbb{Q}[x]$. You are given that:

$$x^4 - 3 = (x^3 - 2x^2 + 4x - 8)(x + 2) + 13$$
$$x + 2 = \left(\frac{1}{13}x + \frac{2}{13}\right) \cdot 13 + 0$$

(b) Use the reverse-engineered Euclidean algorithm to write 1 as a linear combination of $x^4 - 3$ and $x + 2$ with coefficients in $\mathbb{Q}[x]$.

Solution: Solve equation 1 for 13 and divide both sides by 1/13 in $\mathbb{Q}[x]$. The result is:

$$1 = \frac{1}{13}(x^4 - 3) - \frac{1}{13}(x^3 - 2x^2 + 4x - 8)(x + 2).$$

(c) Consider the system of congruences

$$\begin{cases} f(x) \equiv a(x) \pmod{m(x)} \\ f(x) \equiv b(x) \pmod{n(x)} \end{cases} \qquad (\clubsuit)$$

where $a(x)$ and $b(x)$ are arbitrary polynomials in $\mathbb{Q}[x]$. Prove that

$$f_0(x) = \frac{1}{13}a(x)(x^4-3) - \frac{1}{13}b(x)(x^3-2x^2+4x-8)(x+2)$$

is a solution to $\clubsuit$.

Solution: It is enough to show that

1. $m(x) = x+2$ divides $f_0(x) - a(x)$ and
2. $n(x) = x^4 - 3$ divides $f_0(x) - b(x)$.

For (1), recall by part (b) that $\frac{1}{13}(x^3-2x^2+4x-8)(x+2) = \frac{1}{13}(x^4-3)-1$ is divisible by $n(x) = x+2$. So,

$$f_0(x) - a(x) = a(x)(\frac{1}{13}(x^4-3)-1) - \frac{1}{13}b(x)(x^3-2x^2+4x-8)(x+2)$$

is divisible by $x+2$, as desired.

Similarly, for (2) notice that $1 + \frac{1}{13}(x^3-2x^2+4x-8)(x+2) = \frac{1}{13}(x^4-3)$ is divisible by $m(x) = x^4-3$. So,

$$f_0(x) - b(x) = \frac{1}{13}a(x)(x^4-1) - b(x)(1+\frac{1}{13}(x^3-2x^2+4x-8)(x+2)),$$

is divisible by x^4-3, as desired.

(d) Let $I = (n(x)m(x))$, that is, the ideal generated by $n(x)m(x)$. Show that every element in $f_0(x) + I$ is a solution to $\clubsuit$.

Solution: An element in $f_0(x) + I$ is of the form $f_0(x) + q(x)m(x)n(x)$ for some $q(x) \in \mathbb{Q}[x]$. Recall by part (c) that $f_0(x) - a(x)$ is divisible by $m(x)$ and $f_0(x) - b(x)$ is divisible by $n(x)$. Hence, $f_0(x) + q(x)m(x)n(x) - a(x) = (f_0 - a(x)) + q(x)m(x)n(x)$ and so

$$f_0(x) + q(x)m(x)n(x) \equiv a(x) \pmod{m(x)}.$$

Similarly

$$f_0(x) + q(x)m(x)n(x) \equiv b(x) \pmod{n(x)}$$

as desired.

5. (12 points) Let $(\mathbb{Z}_9^{2\times 2}, +, \cdot)$ be the ring of all two by two matrices with entries from $\mathbb{Z}_9$. Denote $\mathrm{Sym}_2(\mathbb{Z}_9)$ be the set of *symmetric* two by two matrices with entries from $\mathbb{Z}_9$. Recall that a matrix is symmetric if the entry in row i column j is equal to the entry in row j and column i.

   (a) Prove or disprove: the set $(\mathrm{Sym}_2(\mathbb{Z}_9), +, \cdot)$ is a subring of $(\mathbb{Z}_9^{2\times 2}, +, \cdot)$.

   Solution: False, $(\mathrm{Sym}_2(\mathbb{Z}_9)$ is not closed under multiplication. Below we abuse notation and write a to mean $[a]_9$.
   Note that $\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}$ and $\begin{bmatrix}0 & 1\\ 1 & 1\end{bmatrix}$ are both symmetric, yet their product is not:

$$\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 1\end{bmatrix} = \begin{bmatrix}0 & 2\\ 0 & 0\end{bmatrix}.$$

   (b) Prove or disprove: the symmetric matrix $\begin{bmatrix}[5]_9 & [4]_9\\ [4]_9 & [5]_9\end{bmatrix}$ is a zero divisor.

   Solution: True. The matrix $\begin{bmatrix}[1]_9 & [1]_9\\ [1]_9 & [1]_9\end{bmatrix}$ has

$$\begin{bmatrix}[5]_9 & [4]_9\\ [4]_9 & [5]_9\end{bmatrix}\begin{bmatrix}[1]_9 & [1]_9\\ [1]_9 & [1]_9\end{bmatrix} = \begin{bmatrix}[1]_9 & [1]_9\\ [1]_9 & [1]_9\end{bmatrix}\begin{bmatrix}[5]_9 & [4]_9\\ [4]_9 & [5]_9\end{bmatrix} = \begin{bmatrix}[0]_9 & [0]_9\\ [0]_9 & [0]_9\end{bmatrix}$$

   (c) Prove or disprove: the symmetric matrix $\begin{bmatrix}[5]_9 & [4]_9\\ [4]_9 & [5]_9\end{bmatrix}$ is a unit.

   Solution: False. Zero divisors are not units.

   (d) Prove or disprove: the symmetric matrix $\begin{bmatrix}[5]_9 & [4]_9\\ [4]_9 & [5]_9\end{bmatrix}$ is nilpotent.

   Solution: Notice that

$$\begin{bmatrix}[5]_9 & [4]_9\\ [4]_9 & [5]_9\end{bmatrix}^2 = \begin{bmatrix}[41]_9 & [40]_9\\ [40]_9 & [41]_9\end{bmatrix} = \begin{bmatrix}[5]_9 & [4]_9\\ [4]_9 & [5]_9\end{bmatrix}.$$

   Thus, for al $n \in \mathbb{N}$,

$$\begin{bmatrix}[5]_9 & [4]_9\\ [4]_9 & [5]_9\end{bmatrix}^n = \begin{bmatrix}[5]_9 & [4]_9\\ [4]_9 & [5]_9\end{bmatrix}$$

   Since this is never the zero matrix, this matrix is not nilpotent.

6. (17 points) (a) Prove that the ideal $(15, 21) \subseteq \mathbb{Z}$ is principal by finding an element c in $\mathbb{Z}$ that generates the ideal.

Solution: Claim $(3) = (15, 21)$. We will use the fact that since $\gcd(15, 21) = 3$, by the Bezout identity there exists $u, v \in \mathbb{Z}$ such that

$$15u + 21v = 3. \tag{1}$$

=> Take $3k \in (3)$ for some $k \in \mathbb{Z}$. Then by eq.(1), $3k = 15ku + 21kv \in (15, 21)$.
<= Take $15a + 21b \in (15, 21)$. Note $15a + 21b = 3 \cdot 5a + 3 \cdot 7b \in (3)$.

(b) Prove that the ideal $(2, x) \subseteq \mathbb{Z}_7[x]$ principal by finding an element $c(x)$ in $\mathbb{Z}_7[x]$ that generates the ideal.

Solution: Note that $\gcd(2, 7) = 1$ which makes 2 a unit in $\mathbb{Z}_7[x]$. Hence

$$\mathbb{Z}_7[x] = (2) \subseteq (2, x) \subseteq \mathbb{Z}_7[x] \to (2, x) = \mathbb{Z}_7[x].$$

Indeed, we could have used any unit (that is, $1, 2, 3, 4, 5$ or 6) to generate $\mathbb{Z}_7[x]$.

(c) Let a be an integer and n be a positive integer. Suppose that $[a]_n$ is a unit in $\mathbb{Z}_n$. Prove that the ideal $(a, n) \subseteq \mathbb{Z}$ is all of $\mathbb{Z}$.

Solution: $[a]_n$ a unit in $\mathbb{Z}_n$ implies that $\gcd(a, n) = 1$. Hence, by the Bezout identity there exist $u, v \in \mathrm{Z}$ such that $ua + vn = 1$. Hence, $1 \in (a, n)$ which implies that all the ring is in (a, n), as desired.

(d) Let $\mathbb{F}$ be a field and let $I = (f(x))$ be an ideal in $\mathbb{F}[x]$. Suppose that $g(x) + I$ is a unit in $\mathbb{F}[x]/I$. Prove that the ideal $(f(x), g(x)) \subseteq \mathbb{F}[x]$ is all of $\mathbb{F}[x]$.

Solution: $g(x) + I$ a unit in $\mathbb{F}[x]/I$ implies that $\gcd(f(x), g(x)) = 1$. Hence, by the Bezout identity there exist $u(x), v(x) \in \mathrm{Z}$ such that $u(x)f(x) + v(x)g(x) = 1$. Hence, $1 \in (f(x), g(x))$ which implies that all the ring is in $(f(x), g(x))$, as desired.

(e) Find all 4 units and their inverses in $\mathbb{Z}_3[x]/(x(x + 1))$.

Solution: Elements in $\mathbb{Z}_3[x]/(x(x + 1))$ are all of the form $(a + bx) + I$ where $I = (x(x + 1))$ and $a, b \in \mathbb{Z}_3$. From there, all the units are

- $1 + I$ with inverse $1 + I$,
- $2 + I$ with inverse $2 + I$,
- $2 + x + I$ with inverse $2 + x + I$,
- $1 + 2x + I$ with inverse $1 + 2x + I$.

7. (16 points) Let $f(x), g(x) \in \mathbb{F}[x]$, where $\mathbb{F}$ is a field, and let $\alpha \in \mathbb{F}$. Let $I = (x - \alpha)$.

(a) Prove that $f(x)$ is congruent to $g(x)$ mod I if and only if $f(\alpha) = g(\alpha)$.

Solution: $\implies$ Let $f(x) \equiv g(x) \text{mod} I$. Then $f(x) - g(x) = h(x)(x - \alpha)$ for some $h(x) \in \mathrm{F}[x]$. Evaluating at $x = \alpha$ we have $f(\alpha) - g(\alpha) = 0$, and so $f(\alpha) = g(\alpha)$, as desired.
$\impliedby$ Suppose that $f(\alpha) = g(\alpha)$. Then $(f - g)(\alpha) = 0$, so α is a root of the polynomial $(f - g)(x)$. Thus by the factor theorem, $x - \alpha$ divides $(f - g)(x)$. So there exists some $h(x)$ such that

$$(f - g)(x) = (x - \alpha)h(x).$$

Thus $f(x) \equiv g(x) \mod (x - \alpha)$.

(b) Let $\mathbb{F} = \mathbb{Z}_7$. Let $\alpha = [1]_7$ and let $f(x) = x^5 + 3x^4 + 2x^3 + 1$. Find an element of $f(x) + I$ of degree 1.

Solution: We want $g(x)$ of degree one such that $x^5 + 3x^4 + 2x^3 + 1 - g(x) = q(x)(x - [1]_7)$, for some $q(x) \in \mathbb{Z}_7[x]$. By the fact that we proved in part (a), we want a polynomial $g(x)$ such that $g([1]_7) = f([1])_7$. Evaluating gives that $f([1]_7) = 0$, so we seek a degree 1 polynomial that is $[0]_7$ when evaluated at $[1]_7$; $g(x) = x - [1]_7$ works.

(c) Let $I = (x - \alpha)$. Prove that the map

$$\varphi : \mathbb{F}[x]/I \to \mathbb{F}$$
$$\varphi(f(x) + I) = f(\alpha)$$

is well-defined.

Solution: Take $f(x) \neq g(x) \in \mathbb{F}[x]$ such that $f(x) + I = g(x) + I$. By part (a), $f(\alpha) = g(\alpha)$. Then

$$\varphi(f(x) + I) = f(\alpha) = g(\alpha) = \varphi(g(x) + I).$$

(d) Is I a maximal ideal? Justify your answer with a proof.

Solution: True. Suppose for contradiction that there exists another element $g(x) \in \mathbb{F}[x]$ that strictly includes I. This implies that $g(x) \notin I$. By the long division algorithm, we can assume that $g(x)$ has degree less that $\deg(x - \alpha)$. This implies that $g(x)$ is some nonzero constant element in $\mathbb{F}$, say, $g(x) = c$. Since the latter one is a field, and every nonzero ememement in the field is a unit, we get that c is a unit in $\mathbb{F}$. Units of $\mathbb{F}[x]$ are all the units of $\mathbb{F}$, and hence, $\mathbb{F}[x] = (c) \subseteq (x - \alpha, c) \subseteq \mathbb{F}[x]$. So, $(x - \alpha, c) = \mathbb{F}[x]$, which shows that $I = (x - \alpha)$ is a maximal ideal in $\mathbb{F}[x]$.
Alternate proof: As we showed in class, every element in R is congruent modulo I to an element of degree strictly less than $(x - \alpha)$, which is degree 1. So every element in R is congruent modulo I to an element of degree 0 (or the element $[0]_7$). Furthermore, each constant in $\mathbb{Z}_7$ is congruent to itself modulo I. Thus $R/I \cong \mathbb{Z}_7$, which is a field. By a result on the homework, I is maximal if and only if R/I is a field. s

(e) Is I a prime ideal? Justify your answer.

Solution: True, by a result on a homework that all maximal ideals are prime and part (d).