Math 412 Winter 2022 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	15	
5	15	
6	18	
7	13	
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) Let I be an ideal of a commutative ring R, and let x and y be arbitrary elements of R. Then *x is congruent to y modulo I*

   Solution: if $x - y \in I$

   (b) The map $\varphi : R \to S$ is a *ring homomorphism*

   Solution: if it satisifies the following three properties:

   - $\varphi(1_R) = 1_S$
   - For all $a, b \in R$, $\varphi(a + b) = \varphi(a) + \varphi(b)$
   - For all $a, b \in R$, $\varphi(ab) = \varphi(a)\varphi(b)$

   Failure to use quantifiers resulted in a loss of points.

   (c) An element $a \in R$ is a *unit of R*

   Solution: if there exists a $b \in R$ such that $ab = ba = 1_R$.
   (Recall: to be a unit, an element must have a left AND right inverse. We saw an example in the homework of an element that has a right inverse but not a left one: differentiation in the ring of linear transformations on polynomials.)

   (d) Suppose R is a commutative ring and $c_1, \ldots, c_t$ are elements of R. Then the *ideal generated by $c_1, \ldots, c_t$*, denoted $(c_1, \ldots, c_t)$,

   Solution:
   $$\{r_1c_1 + r_2c_2 + \cdots + r_tc_t | r_1, \ldots, r_t \in R\}$$

2. (15 points) For each of the statements below, indicate clearly if the statement is true or false, and give a short justification.

   (a) Every nonzero element of a commutative ring R is either a zerodivisor or a unit.

   Solution: False. Consider the ring $\mathbb{Z}$ and $2 \in \mathbb{Z}$. This element is neither a unit nor a zerodivisor. A different example is the ring $\mathbb{R}[x]$ and the element $x \in \mathbb{R}[x]$.

   (b) Every homomorphism from a field $\mathbb{F}$ to a nonzero ring is surjective.

   Solution: False. The inclusion of a subring is a ring homomorphism. Then $\mathbb{Q} \to \mathbb{R}$ is a ring homomorphism that is not surjective since $\sqrt{2}$ is not in the image.

   (c) Suppose φ is a homomorphism from $\mathbb{Q} \to \mathbb{R}$. Then $\varphi(q) = q$ for all $q \in \mathbb{Q}$.

   Solution: True. Let φ be one such ring homomorphism, then $\varphi(1) = 1$. From this, it follows that for all $k \in \mathbb{Z}$, $\varphi(k) = k$. Indeed, we have proved that $\varphi(0) = 0$. If $k > 0$, then $k = 1 + \ldots + 1$, then $\varphi(k) = \varphi(1) + \ldots + \varphi(1) = 1 + \ldots + 1 = k$. If $k < 0$ we argue in a similar way with -1, since $\varphi(-1) = -\varphi(1) = -1$. Finally, for $k \in \mathbb{Z}$ and $k \neq 0$, $\varphi(k^{-1}) = \varphi(k)^{-1}$. Therefore, for $\frac{a}{b} \in \mathbb{Q}$, with $a, b \in \mathbb{Z}$, $\varphi(\frac{a}{b}) = \varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = ab^{-1} = \frac{a}{b}$.

   (d) The polynomial $x^3 + 2x^2 + 4$ is irreducible in $\mathbb{Z}_5[x]$.

   Solution: False. Since $\mathbb{Z}_5$ is a field, we know that a polynomial of degree 2 or 3 is irreducible if and only if it has no roots. By inspection, we see that $[2]_5$ and $[4]_5$ are roots.

   (e) There does not exist a homomorphism from $\mathbb{Z}_{30} \to \mathbb{Z}_6$ with kernel $([7]_{30})$.

   Solution: True. Since $\gcd(7, 30) = 1$, $[7]_{30}$ is a unit. This means that $[1]_{30} \in ([7]_{30})$, and then $\varphi([1]_{30}) = [0]_6$, which contradicts the fact that φ is a ring homomorphism.

3. (12 points) For each question below, give an example with the required properties, or explain why no such example exists. Justify your answer.

   (a) A ring that has prime characteristic and is not an integral domain.

   Solution:

   - $\mathbb{Z}_2 \times \mathbb{Z}_2$ is characteristic 2 because $(1,1) + (1,1) = (0,0)$, but is not a domain because $(1,0) \cdot (0,1) = (0,0)$.
   - $\mathbb{Z}_p[x]/(f(x))$ for any prime number p and any reducible polynomial $f(x)$, such as $\mathbb{Z}_7[x]/(x^2)$. This ring is characteristic p, and any divisors of $f(x)$ will be a zerodivisor in this quotient ring.

   (b) An ideal I in a commutative ring R such that I cannot be generated by a single element

   Solution: An example we saw on the homework is the ideal $(5, x) \subset \mathbb{Z}[x]$.
   Recall that both $\mathbb{Z}$ and $\mathbb{F}[x]$ where $\mathbb{F}$ is a field (such as $\mathbb{Q}$ or $\mathbb{R}$) are rings in which every ideal can be generated by a single element, so you cannot find an example in one of those rings.

   (c) A ring that has a commutative subring and a non-commutative subring.

   Solution: Let $M_2(\mathbb{R})$ be the ring of 2×2 matrices with real entries. This ring is non-commutative, since, for example,

   $$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

   The whole ring is also a subring, so $M_2(\mathbb{R})$ is a non-commutative subring. The subset of diagonal matrices is a subring and it is commutative.

   (d) A ring R and ideals I, J such that the ring homomorphism

   $$\begin{aligned} & \varphi : R \to R/I \times R/J \\ \text{defined by} \quad & \varphi(r) = (r + I, r + J) \end{aligned}$$

   is not surjective.

   Solution: Let $R = \mathbb{Z}$, $I = (2)$ and $J = (4)$. The map φ is not surjective since $([1]_2, [0]_4)$ is not in the image. Indeed, if $r \in \mathbb{Z}$ and $[r]_4 = [0]_4$, then r must be even, hence $[r]_2 = [0]_2$.

4. (15 points) Let $M_2(\mathbb{Z}_{15})$ be the ring of 2×2 matrices with entries in $\mathbb{Z}_{15}$, and $D \subseteq M_2(\mathbb{Z}_{15})$ the subring of diagonal matrices, that is, matrices of the form $\begin{pmatrix} [x]_{15} & 0 \\ 0 & [y]_{15} \end{pmatrix}$. You don't need to prove that $M_2(\mathbb{Z}_{15})$ is a ring, nor that D is a subring.

Let $\varphi : \mathbb{Z} \times \mathbb{Z} \to D$ be defined by

$$\varphi(a, b) = \begin{pmatrix} [a]_{15} & 0 \\ 0 & [6a + 10b]_{15} \end{pmatrix}.$$

(a) Show that φ is a ring homomorphism.

Solution: Let $a, b, c, d \in \mathbb{Z}$.

i) $\varphi(1, 1) = \begin{pmatrix} [1]_{15} & 0 \\ 0 & [6 + 10]_{15} \end{pmatrix} = \begin{pmatrix} [1]_{15} & 0 \\ 0 & [1]_{15} \end{pmatrix}$.

ii) φ respects addition:

$$\begin{aligned} \varphi(a, b) + \varphi(c, d) &= \begin{pmatrix} [a]_{15} & 0 \\ 0 & [6a + 10b]_{15} \end{pmatrix} + \begin{pmatrix} [c]_{15} & 0 \\ 0 & [6c + 10d]_{15} \end{pmatrix} \\ &= \begin{pmatrix} [a + c]_{15} & 0 \\ 0 & [6(a + c) + 10(b + d)]_{15} \end{pmatrix} = \varphi(a + c, b + d) \end{aligned}$$

.

iii) φ respects multiplication:

$$\begin{aligned} \varphi(a, b)\varphi(c, d) &= \begin{pmatrix} [a]_{15} & 0 \\ 0 & [6a + 10b]_{15} \end{pmatrix} \begin{pmatrix} [c]_{15} & 0 \\ 0 & [6c + 10d]_{15} \end{pmatrix} \\ &= \begin{pmatrix} [ac]_{15} & 0 \\ 0 & [6ac + 10bc]_{15} \end{pmatrix} = \varphi(ac, bd), \end{aligned}$$

where the penultimate equality follows since $[6a + 10b]_{15}[6c + 10d]_{15} = [36ac + 60ad + 60bc + 100bd]_{15} = [36ac + 100bd]_{15} = [6ac + 10bd]_{15}$.

(b) State if φ is surjective, and justiy your answer.

Solution: The map φ is not surjective. Indeed, $\begin{pmatrix} [0]_{15} & 0 \\ 0 & [1]_{15} \end{pmatrix} \in D$ is not in the image, since if $[a]_{15} = [0]_{15}$, then $[6a + 10b]_{15} = [10b]_{15}$. Moreover, $[10b]_{15} \neq [1]_{15}$ for all $b \in \mathbb{Z}$ since $\gcd(10, 15) \neq 1$ which means that $[10]_{15}$ is not a unit.

(c) Find the kernel of φ and prove that it is principal.

Solution: Let $(a, b) \in \ker(\varphi)$. Then $[a]_{15} = [0]_{15}$, hence $a = 15k$ for some $k \in \mathbb{Z}$. Also, $[6a + 10b]_{15} = [10b]_{15} = [0]_{15}$. This means that $15|10b$, then $3|2b$, hence $b = 3j$ for some $j \in \mathbb{Z}$. It is clear that if $15|a$ and $3|b$, then (a, b) is in the kernel, therefore

$$\ker(\varphi) = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \ : \ a = 15k \text{ and } b = 3j \text{ for some } j, k \in \mathbb{Z}\}.$$

This ideal is principal since $\ker(\varphi) = ((15, 3))$. Indeed, if $(a, b) \in \ker(\varphi)$, then $a = 15k$ and $b = 3j$, and $(a, b) = (k, j) \cdot (15, 3)$. Moreover, if $(c, d) = (r, s) \cdot (15, 3) = (15r, 3s)$, then $(c, d) \in \ker(\varphi)$.

5. (15 points) (a) Let I be the ideal generated by $(3x^3 + x^2, 4x^2 + 3x)$ in $\mathbb{Z}_5[x]$. Find a single element, $f(x)$, of $\mathbb{Z}_5[x]$ such that I is generated by $f(x)$ or prove that this is impossible. Justify your answer.

Solution: To find the greatest common divisor of $4x^2 + 3x$ and $3x^3 + x^2$, let us try to factor them both into irreducible polynomials. By inspection, x divides them both, giving

$$4x^2 + 3x = x(4x + 3)$$
$$3x^3 + x^2 = x^2(3x + 1)$$

Note also that $4x+3$ and $3x+1$ are associates in $\mathbb{Z}_5[x]$! One way we could see this is to note that they both are zero in $\mathbb{Z}_5$ when evaluated at 3. Another way to notice this is to find a monic ideal that is associate to both: $4x+3 = 4(x+2)$ and $3x+1 = 3(x+2)$. Thus, the greatest common divisor of $4x^2 + 3x$ and $3x^3 + x^2$ is $x(x + 2) = x^2 + 2x$, which is an associate of $4x^2 + 3x$.
You may have also immediately noticed that $(4x^2 + 3x)$ divides $3x^3 + x^2$, because

$$2x(4x^2 + 3x) \quad \text{in } \mathbb{Z}_5[x].$$

Thus any multiple of $3x^3 + x^2$ is a multiple of $4x^2 + 3x$, so the ideal can be generated by $4x^2 + 3x$. Any associate of $4x^2 + 3x$ is also a correct answer.

(b) Let $J = (x^2)$ be an ideal in $\mathbb{Z}_5[x]$. Find the number elements of $\mathbb{Z}_5[x]/J$ and briefly justify your answer.

Solution: Every element of $\mathbb{Z}_5[x]/J$ is equivalent to some element of degree 1 or less (or 0). Since there are 5 options for the constant term and 5 options for the coefficient of x, this gives 25 possible options.
Furthermore, all of these elements are distinct modulo J, since a degree 2 polynomial cannot divide a difference of degree 1 or 0 polynomials.

(c) Let n be the number of elements you found in part b). Prove that $\mathbb{Z}_5[x]/J$ is not isomorphic to $\mathbb{Z}_n$.

Solution: Both $\mathbb{Z}_5[x]/J$ and $\mathbb{Z}_{25}$ have 4 nonzero zerodivisors ($x, 2x, 3x$ and $4x$ in $\mathbb{Z}_5[x]/J$ and $5, 10, 15$ and 20 in $\mathbb{Z}_{25}$).
However, $\mathbb{Z}_5[x]/J$ is characteristic 5 while $\mathbb{Z}_{25}$ is characteristic 25. Thus not only are they not isomorphic, but there does not exist a homomorphism between them! If φ were a homomorphism from $\mathbb{Z}_5[x]/J$ to $\mathbb{Z}_{25}$, then that would force

$$\varphi([1 + 1 + 1 + 1 + 1]_5) = 0,$$

but also

$$\varphi([1]_5) + \varphi([1]_5) + \varphi([1]_5) + \varphi([1]_5) + \varphi([1]_5) = [1]_{25} + [1]_{25} + [1]_{25} + [1]_{25} + [1]_{25} \neq 0.$$

6. (18 points) Let $f(x) = x^2 - 2 \in \mathbb{Q}[x]$.

   (a) Prove that $\mathbb{Q}[x]/(f(x))$ is a field.

   Solution: Since $\mathbb{Q}$ is a field, we know that $\mathbb{Q}[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible. Moreover, $f(x)$ is irreducible if and only if it has no roots, since it has degree 2. Since no rational number $r \in \mathbb{Q}$ satisfies that r^2 as $\sqrt{2}$ is not rational, then $f(x)$ is irreducible.

   (b) Prove that the ring $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$ is a field.

   Solution:
   Let $\phi : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{2})$ defined by $\phi(p(x)) = p(\sqrt{2})$. Since ϕ is an evaluation map, we have proved that it is a ring homomorphism. Moreover, ϕ is surjective since $a + b\sqrt{2} = \phi(a + bx)$. Any element in $(f(x))$ is in the kernel since $f(\sqrt{2}) = 0$. Also, let $p(x)$ be an element in the kernel of ϕ. By the division algorithm, $p(x) = q(x)f(x) + r(x)$, with $\deg(r(x)) \leq 1$ or $r(x) = 0$. If $\deg(r(x)) \leq 1$, $r(\sqrt{2}) \neq 0$ since $a + b\sqrt{2} = 0$ if and only if $a = b = 0$. Therefore, $\ker(\phi) = (f(x))$. By the First Isomorphism Theorem, $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(f(x))$, and the latter is a field.

   (c) Find the multiplicative inverse of $[x + 2]_f$ in the quotient ring $\mathbb{Q}[x]/(f(x))$.

   Solution: Using the isomorphism in b), it is enough to find the multiplicative inverse of $2 + \sqrt{2}$. Since $(2 + \sqrt{2})(2 - \sqrt{2}) = 2$, then $\frac{1}{2}(2 - \sqrt{2})$ is the multiplicative inverse. Therefore, $[\frac{1}{2}(2 - x)]_f$ is the inverse of $[x + 2]_f$.

   We can also argue directly. By the division algorithm we have that $x^2 - 2 = (x + 2)(x - 2) + 2$. This means that $(x^2 - 2) - 2 = (x + 2)(x - 2)$. Then $[\frac{-1}{2}(x - 2)]_f$ is the multiplicative inverse of $[x + 2]_f$.

7. (13 points) Let R and S be commmutative rings, and let $\varphi : R \to S$ be a ring homomorphism.

   (a) Suppose φ is surjective. Prove that if I is an ideal in R, then $\varphi(I) := \{\varphi(r) \ : \ r \in I\}$ is an ideal in S.

Solution:

- Nonempty:
  First note that $\varphi(I)$ is nonempty, because I is nonempty. Thus there exists some $x \in I$, and so there is some $\varphi(x) \in \varphi(I)$.
- Closed under addition:
  Suppose that $s_1, s_2 \in \varphi(I)$. Then by definition there is some $r_1, r_2 \in I$ such that $\varphi(r_1) = s_1$ and $\varphi(r_2) = s_2$. Because I is an ideal, the sum $r_1 + r_2 \in I$. Thus $\varphi(r_1 + r_2) \in \varphi(I)$. Because φ is a homomorphism, this gives that
  $$s_1 + s_2 = \varphi(r_1) + \varphi(r_2) = \varphi(r_1 + r_2) \in \varphi(I).$$
- Closed under multiplication by any element of S:
  Suppose that $c \in S$ and $s \in \varphi(I)$. Then by definition there exists some $r \in I$ such that $\varphi(r) = s$. Because φ is surjective, there exists some $k \in R$ such that $\varphi(k) = c$. Because I is an ideal, $kr \in I$. Thus $\varphi(kr) \in \varphi(I)$. Because φ is a homomorphism, this gives
  $$cs = \varphi(k)\varphi(r) = \varphi(kr) \in \varphi(I).$$

   (b) You may use without proof the fact that if J is an ideal in S, then the set
   $$\varphi^{-1}(J) := \{r \in R \ : \ \varphi(r) \in J\}$$
   is an ideal in R. Let M be a maximal ideal in S. State if the following is true or false, and justify your answer: The ideal $\varphi^{-1}(M)$ is a maximal ideal in R.

Solution: The solution to this question depends on whether or not you interpreted φ as retaining the surjectivity guaranteed in part a. We did not intend for the assumptions of part a to be carried on to part b, however, a correct proof using this assumption was still given full points.

- Assuming φ is **not surjective**, the answer is **FALSE**.
  Some counterexamples:
  - Let $\varphi : \mathbb{Z} \to$ any field containing $\mathbb{Z}$, such as $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ by $\varphi(n) = n$. The only ideals in fields are (0) and the entire field, so (0) is a maximal ideal in all of the above fields. However, $\varphi^{-1}((0)) = (0) \in \mathbb{Z}$, which is not a maximal ideal, as it is strictly contained in the proper ideals $(2), (3), (4), (5), \ldots$, that is, any ideal generated by n where $n \neq -1, 0, 1$. It
  - Let $\varphi : \mathbb{Z}[x] \to \mathbb{Q}[x]$ by $\varphi(f(x)) = f(x)$. Then (x) is a maximal ideal in $\mathbb{Q}[x]$ (you showed on the homework that ideals generated by irreducible polynomials are maximal), but $\varphi^{-1}((x)) = (x)$, which is not maximal in

$\mathbb{Z}[x]$, since it is strictly contained in $(5, x)$, and in $\mathbb{Z}_5[x]$, the ideal $(5, x)$ is not the whole ring.

- Let $\varphi : \mathbb{F}[x] \to \mathbb{F}[x]$, where $\mathbb{F}$ is some field, by $\varphi(f(x)) = f(0)$. Then (x) is a maximal ideal in $\mathbb{F}[x]$, but $\varphi^{-1}((x)) = (0)$, which is not maximal in $\mathbb{F}[x]$.

- Assuming φ is **surjective**, the answer is **TRUE**.
Suppose that M is maximal in S. Then S/M is a field. Consider the map

$$\begin{aligned} \overline{\varphi} : R/\varphi^{-1}(M) &\to S/M \\ r + \varphi^{-1}(M) &\mapsto \varphi(r) + M \end{aligned}$$

This map is well defined, because if $r_1 - r_2 \in \varphi^{-1}(M)$, then by definition, $\varphi(r_1 - r_2) \in M$, so $\varphi(r_1)$ is congruent to $\varphi(r_2)$ modulo M. It is straightforward to check it is a homomorphism.
Furthermore, I prove that $\overline{\varphi}$ is surjective: let $s + M$ be a congruence class in S/M. Choose some representative, $s \in S$, from this class. If $s \in S$, then, because φ is surjective, there exists some $r \in R$ such that $\varphi(r) = s$. Thus, $\overline{\varphi}(r + \varphi^{-1}(M)) = \varphi(r) + M = s + M$, so $\overline{\varphi}$ is surjective.
Suppose that $r + \varphi^{-1}(M) \in \ker(\overline{\varphi})$. Then $\overline{\varphi(r) + \varphi^{-1}(M)} = 0 + M$, so by definition of $\overline{\varphi}$, $\varphi(r) \in M$, meaning that $r \in \varphi^{-1}(M)$. Thus, $\overline{\varphi}$ is injective as well.
Therefore, $\overline{\varphi}$ is an isomorphism between $R/\varphi^{-1}(M)$ and S/M. Since S/M is a field, this implies that $R/\varphi^{-1}(M)$ is a field, which in turn implies that $\varphi^{-1}(M)$ is maximal in R.
Alternatively, we could have constructed a map $\phi : R \to S/M$ given by $\phi(r) = \varphi(r)+M$. This map is surjective, and its kernel is $\varphi^{-1}(M)$. So by Noether's First Isomorphism Theorem, $R/\varphi^{-1}(M) \cong S/M$, which again implies that $R/\varphi^{-1}(M)$ is a field and so $\varphi^{-1}(M)$ is maximal.
WARNING 1: Many proofs incorrectly argued that if $\varphi(I) = S$, then that implies that $I = R$. This is NOT the case! It is true that for homomorphisms, $\varphi(1_R) = 1_S$. However, that does not mean that 1_R is the *only* element of R that maps to 1_S. Consider $\varphi : \mathbb{F}[x] \to \mathbb{F}$ by $\varphi(f(x)) = f(1)$. Then $\varphi((x)) = \mathbb{F}$, but $(x) \neq \mathbb{F}[x]$.
WARNING 2: Similarly, many proofs incorrectly argued that if $\varphi(ab) = 1_S$, then $ab = 1_R$. The other direction is true; if $ab = 1_R$, then $\varphi(ab) = 1_S$. However, if φ is not injective, then the converse does not follow.

You can use this space for work.

You can use this space for work.