**Math 3110** **Final Exam** **May 2nd, 2022**

**Name:** Answer Key **Be sure to show your work!**

1. (15 points) Working in $\mathbb{Z}_{12}$.

(a) $I = (4) = \langle 4 \rangle = \{0, 4, 8\}$ and $\mathbb{Z}_{12}/I = \{I, 1+I, 2+I, 3+I\}$.

(b) Write addition and multiplication tables for $\mathbb{Z}_{12}/I$.

| $+$ | $I$ | $1+I$ | $2+I$ | $3+I$ |
|---|---|---|---|---|
| $I$ | $I$ | $1+I$ | $2+I$ | $3+I$ |
| $1+I$ | $1+I$ | $2+I$ | $3+I$ | $I$ |
| $2+I$ | $2+I$ | $3+I$ | $I$ | $1+I$ |
| $3+I$ | $3+I$ | $I$ | $1+I$ | $2+I$ |

| $\times$ | $I$ | $1+I$ | $2+I$ | $3+I$ |
|---|---|---|---|---|
| $I$ | $I$ | $I$ | $I$ | $I$ |
| $1+I$ | $I$ | $1+I$ | $2+I$ | $3+I$ |
| $2+I$ | $I$ | $2+I$ | $I$ | $2+I$ |
| $3+I$ | $I$ | $3+I$ | $2+I$ | $1+I$ |

(c) For each element in $\mathbb{Z}_{12}/I$, state whether that element is zero, a zero divisor, a unit, or none of the above. If it is a unit, give its inverse. If it is an zero divisor, show that this is the case.

Obviously, $I$ is our zero. Next, $1 + I$ is our multiplicative identity, so it is a unit and $(1 + I)^{-1} = 1 + I$. Notice $(3+I)(3+I) = 9+I = (1+8)+I = 1+I$, so $3+I$ is a unit and $(3+I)^{-1} = 3+I$. Finally, $2+I \neq I$ (i.e., it is nonzero). However, $(2 + I)(2 + I) = 4 + I = I$. Thus $2 + I$ is a zero divisor (in fact, it is *nilpotent* since raising it to a sufficient power yields zero).

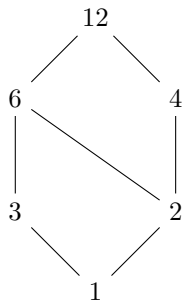
(d) Suppose $R$ is some ring and $\varphi : \mathbb{Z}_{12} \to R$ is a homomorphism. Let $K = \text{Ker}(\varphi)$. Give a complete list of all possible $K$'s. Circle the choice(s) that guarantee $\varphi$ is one-to-one.

We know that the kernel of a (ring) homomorphism must be an ideal. Moreover, every ideal is the kernel of some homomorphism. Thus this is just a sneaky way of asking for a list of the ideals of $\mathbb{Z}_{12}$.

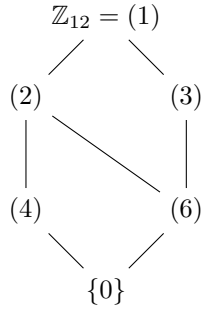
Recall that "principal ideal = ideal = subring = subgroup = cyclic subgroup" when dealing with $\mathbb{Z}$ or $\mathbb{Z}_n$. Also, $\mathbb{Z}_n$ has precisely one subgroup (thus ideal) of order $k$ for each divisor of $n$. Notice that the divisors of 12 are $1, 2, 3, 4, 6$, and 12. Our ideals are $\boxed{\{0\}}$, (6), (4), (3), (6), and $\mathbb{Z}_{12}$ itself. *Note:* We boxed in $\{0\}$ since a homomorphism is one-to-one if and only if its kernel is trivial.

(e) Which ideals $I$ in $\mathbb{Z}_{12}$ make sure $\mathbb{Z}_{12}/I$ is a field?

Recall that $\mathbb{Z}_{12}/I$ is a field if and only if $I$ is maximal. Thus, from the ideal lattice to the right, we can see $\boxed{I = (2) \text{ and } (3)}$ yield a quotient ring that is a field.
Alternatively, when $k$ is a divisor of $n$, we have $\mathbb{Z}_n/(k) = \mathbb{Z}/n\mathbb{Z}/k\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z} = \mathbb{Z}_k$ which is a field if and only if $k$ is prime. Thus only quotients by (2) and (3) yield fields.



Divisibility Lattice



Ideal Lattice

2. (12 points) Groups: Explain why each pair of **groups** are not isomorphic.

(a) Explain why $A_5 \ncong D_{30}$ [not isomorphic]. *Note:* $A_5$ is the group of even permutations in $S_5$.

Both of these are non-Abelian groups of order 60 (since $5!/2 = 60$ and $2 \cdot 30 = 60$) – no help here. However, $D_{30}$ has elements of order 30 (like a rotation of $360°/30 = 12°$) whereas $A_5$ has no elements of order 30. In fact, $A_5$ has elements of orders 1, 2, 3, and 5 (ex: (1), (12)(34), (123), and (12345)) whereas $D_{30}$ has elements of orders 1, 2, 3, 5, 6, 10, 15, and 30.

Of course, there are other things that reveal these groups are non-isomorphic. For example, $A_5$ has 20 elements of order 3 whereas $D_{30}$ only has 2. Or, the center of $A_5$ is trivial (since $A_5$ is a simple group) whereas $Z(D_{30})$ has order 2 (i.e., the identity and the 180° rotation).

(b) Explain why $S_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_{12}$ [not isomorphic].

Both of these are groups of order 24 (since $4! = 24$ and $2 \cdot 12 = 24$). However, $S_4$ is not Abelian whereas $\mathbb{Z}_2 \times \mathbb{Z}_{12}$ is Abelian. Again, there are other things that help us distinguish these groups like $(1, 1)$ has order $\text{lcm}(2, 12) = 12$ in

$\mathbb{Z}_2 \times \mathbb{Z}_{12}$, but $S_4$ only has elements of orders 1, 2, 3, and 4. *Note:* Neither group is cyclic. Of course, $S_4$ cannot be cyclic because it isn't even Abelian. However, $\mathbb{Z}_2 \times \mathbb{Z}_{12}$ is Abelian but not cyclic. This stems from the fact that 2 and 12 aren't relatively prime.

(c) Explain why $U(5) \ncong U(8)$ [not isomorphic].

Note that $U(5) = \{1, 2, 3, 4\}$ and $U(8) = \{1, 3, 5, 7\}$ are Abelian groups of order 4. However, since $2^1 = 2$, $2^2 = 4$, $2^3 = 3$, and $2^4 = 1$, we have $U(5) = \langle 2 \rangle$ is cyclic. On the other hand, notice $3^2 = 5^2 = 7^2 = 1$, so $U(8)$ is not cyclic (it has no element of order 4). Alternatively, notice $U(8)$ has 3 elements of order 2 whereas $U(5)$ only has 1 (e.g., $4^2 = 1$).

3. (8 points) Rings: Explain why each pair of **rings** are not isomorphic.

(a) $\mathbb{R}[x] \ncong \mathbb{R}^{2\times 2}$ [not isomorphic]. *Note:* These are real polynomials vs. $2 \times 2$ real matrices.

Both of these are rings with unity. Both are infinite (in fact, both have cardinality $\mathfrak{c} = 2^{\aleph_0}$) – no help so far. However, $\mathbb{R}[x]$ is a commutative ring whereas $\mathbb{R}^{2\times 2}$ is not commutative.

Of course, one could do more difficult things as well. For example, $N = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ is an example of a non-zero nilpotent element (note: $N^2 = 0$). But the polynomial ring has no nilpotent elements (isomorphisms must send nilpotent elements to nilpotent elements). Or more basically, $\mathbb{R}[x]$ is an integral domain – it has no zero divisors – whereas $\mathbb{R}^{2\times 2}$ has many zero divisors (like $N$). Thus these rings cannot be isomorphic since an isomorphism would send zero divisors to zero divisors. Or, $U(\mathbb{R}[x]) = \mathbb{R}_{\neq 0}$ is an Abelian group (of units), but $U(\mathbb{R}^{2\times 2}) = \mathrm{GL}_2(\mathbb{R})$ (i.e., invertible $2 \times 2$ matrices) is not an Abelian group (isomorphic rings must have isomorphic groups of units).

(b) $\mathbb{Q} \ncong \mathbb{Z}$ [not isomorphic].

These are both (countably – i.e., cardinality $\aleph_0$) infinite commutative rings. In fact, both are integral domains. However, $\mathbb{Q}$ is a field whereas $\mathbb{Z}$ is not. Alternatively (essentially using the same reason), one could notice that the group of units of $\mathbb{Q}$ is all non-zero rationals (infinitely many units) whereas the group of units of $\mathbb{Z}$ is just $\{1, -1\}$ (only two units).

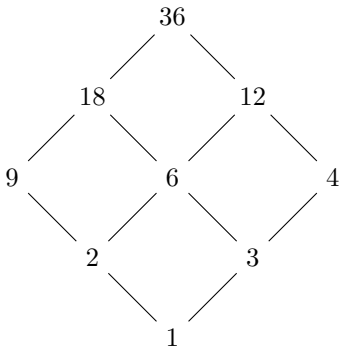
4. (8 points) Workin' in $\mathbb{Z}_{36}$. [Note: $36 = 2^2 \cdot 3^2$]

(a) Fill out the following table (for $\mathbb{Z}_{36}$):

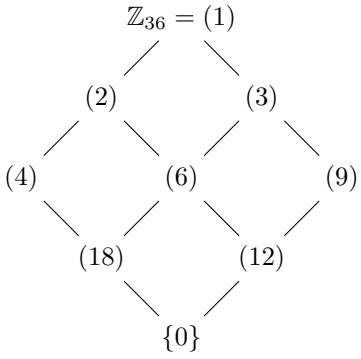
| order = | 1 | 2 | 3 | 4 | 6 | 9 | 12 | 18 | 36 |
|---|---|---|---|---|---|---|---|---|---|
| number of elements with this order = | 1 | 1 | 2 | 2 | 2 | 6 | 4 | 6 | 12 |

For example, there are $3 - 1 = 2$ elements of order 3 since the element of the *unique* cyclic subgroup of order 3 must have orders 1 (i.e., the identity) and 3. Likewise, the elements in the unique cyclic subgroup of order9 must have orders 1, 3, and 9. Knocking out the identity (order 1) and our 2 elements of order 3 leaves us with $9 - 1 - 2 = 6$ elements of order 9. Alternatively, we could use Euler's totient function. For example, $\varphi(36) = \varphi(2^2 \cdot 3^2) = \varphi(2^2)\varphi(3^2) = (2^2 - 2^1)(3^2 - 3^1) = 12$ elements of order 36. *Note:* This also means $\mathbb{Z}_{36}$ has 12 generators (as a cyclic group) which means $U(36)$ has 12 elements (i.e., $\mathbb{Z}_{36}$ has 12 units).

(b) Draw $\mathbb{Z}_{36}$'s lattice of ideals.
As before, we note that all of the subthings of $\mathbb{Z}_n$ as a group and as a ring match up, so finding the ideal lattice is just like finding the subgroup lattice as we did back on the first test.



Divisibility Lattice



Subgroup Lattice

(c) Which ideals are prime? maximal?

Visibly, the maximal ideals are $\boxed{(2) \text{ and } (3)}$ since they are proper ideals with nothing (other than $\mathbb{Z}_{36}$ itself) above them.
For $R$, a commutative ring with 1, we know that an ideal $I$ is maximal if and only if $R/I$ is a field, and $I$ is prime if and only if $R/I$ is an integral domain. Also, fields are always integral domains (thus maximal ideals must be prime ideals). Finally, *finite* integral domains are fields, so if a quotient by $I$ is finite, it is prime if and only if it is maximal. So in a *finite* commutative ring with 1 (like $\mathbb{Z}_n$), prime and maximal are the same thing. Thus $\boxed{(2) \text{ and } (3)}$ are the prime ideals as well.

5. (6 points) Workin' in $\mathbb{Z}_{110}$.

(a) Is 88 zero, a unit, a zero divisor, or none of the above in $\mathbb{Z}_{110}$? If 88 is a zero divisor, prove it. If 88 is a unit, find its inverse. If none of the above, explain why so.

In $\mathbb{Z}_n$ (a finite ring) every element is either zero, a zero divisor, or a unit. In fact, nonzero elements are units if and only if they are represented by $k$ where $\gcd(k, n) = 1$ (i.e., $k \in U(n)$).

Notice that 88 and 110 are *not* relatively prime: $\gcd(88, 110) = 22 \neq 1$. Thus 88 must be a $\boxed{\text{zero divisor}}$. Notice that $110/22 = 5$. We have that $\boxed{88 \cdot 5 =}$ $440 = 4 \cdot 110 = \boxed{0 \bmod 110}$, but 88 and 5 are nonzero (working mod 110). Of course, other elements would also work to establish 88 is a zero divisor, like $110/11 = 10$ or $110/2 = 55$.

(b) Is 53 zero, a unit, a zero divisor, or none of the above in $\mathbb{Z}_{110}$? If 53 is a zero divisor, prove it. If 53 is a unit, find its inverse. If none of the above, explain why so.

On the other hand, 53 and 110 are relatively prime, so $\boxed{53 \text{ is a unit}}$ (mod 110). We run the extended Euclidean algorithm to find an inverse for our unit.

Dividing: $110 = 53 \cdot 2 + 4$, $53 = 4 \cdot 13 = 1$. Thus $(-13)4 + (1)53 = 1$ and so $(-13)[(-2)53 + (1)110] + (1)53 = 1$. Therefore, $(27)53 + (-13)110 = 1$. We have that $\boxed{53^{-1} = 27}$. *Note:* While we didn't need to here, in general we don't want to forget to clean up our answer so it is simplified (i.e., has good manners).

6. (17 points) Sub-things

(a) Recall that $D_8 = \{1, x, \ldots, x^7, y, xy, \ldots, x^7y\} = \langle x, y \mid x^8 = 1, y^2 = 1, xyxy = 1\rangle$.

Let $H = \{1, x^4, y, x^4y\}$. Explain why $H$ is a subgroup but **not** a **normal** subgroup of $D_8$.

| | $1$ | $x^4$ | $y$ | $x^4y$ |
|---|---|---|---|---|
| $1$ | $1$ | $x^4$ | $y$ | $x^4y$ |
| $x^4$ | $x^4$ | $1$ | $x^4y$ | $y$ |
| $y$ | $y$ | $x^4$ | $1$ | $x^4$ |
| $x^4y$ | $x^4y$ | $y$ | $x^4$ | $1$ |

Since $H$ is a non-empty *finite* subset of $D_8$, we can use the finite subgroup test to that that it is a subgroup. This just involves checking closure (which our table verifies). Therefore, $H$ is a subgroup of $D_8$. *Calculation note:* For example, $y \cdot x^4y = x^{-4}yy = x^4 \cdot 1 = x^4$ since exponents of $x$ work mod 8.
To see that this is *not* a normal subgroup, it is easiest to see that some left/right coset pair fail to match.

Notice that $xH = \{x, x^5, xy, x^5y\}$ whereas $Hx = \{x, x^5, yx, x^4yx\} = \{x, x^5, x^7y, x^3y\}$. Since $xH \neq Hx$, $H$ is a not a normal subgroup of $D_8$. Alternatively, we could see that $H$ is not closed under conjugation: $y \in H$ and $x \in D_8$, but $xyx^{-1} = x^2y \notin H$.

(b) Let $G$ be an Abelian group with identity 1. Prove that $H = \{g \in G \mid g^2 = 1\}$ is a subgroup of $G$.

First, notice that $1^2 = 1$ so $1 \in H$. Thus $H$ is a non-empty subset of $G$. Next, suppose $a, b \in H$. Then $a^2 = 1$ and $b^2 = 1$. Since $G$ is Abelian, we have $(ab)^2 = abab = aabb = a^2b^2 = 1 \cdot 1 = 1$. Thus $ab \in H$ (closure under the operation). Finally, if $a \in H$, then $a^2 = 1$ implies $(a^{-1})^2 = (a^2)^{-1} = 1^{-1} = 1$ so that $a^{-1} \in H$ (closure under inverses). Therefore, by the (2-step) subgroup test, $H$ is a subgroup of $G$.

(c) Let $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ where $i^2 = -1$. Show that $\mathbb{Q}[i]$ is a sub**field** of the complex numbers $\mathbb{C}$.

We note that $1 = 1 + 0i \in \mathbb{Q}[i]$, so $\mathbb{Q}[i]$ is a non-empty subset of $\mathbb{C}$ containing 1. Suppose $a + bi, c + di \in \mathbb{Q}[i]$ (where $a, b, c, d \in \mathbb{Q}$). Then $(a + bi) - (c + di) = (a - c) + (b - d)i \in \mathbb{Q}[i]$ since $a - c, b - d \in \mathbb{Q}$ (closure under subtraction). Also, $(a + bi)(c + di) = ac + bdi^2 + adi + bci = (ac - bd) + (ad + bc)i \in \mathbb{Q}[i]$ since $ac - bd, ad + bc \in \mathbb{Q}$ (closure under multiplication). Therefore, so far, we have that $\mathbb{Q}[i]$ is a subring (with 1) of $\mathbb{C}$. In fact, since $\mathbb{C}$ is a field, it is commutative with $1 \neq 0$. Thus $\mathbb{Q}[i]$ is a commutative ring with $1 \neq 0$.

We also need to verify that every nonzero element of $\mathbb{Q}[i]$ is a unit. We will use the so-called *conjugate trick* to help establish this. Let $0 \neq a + bi \in \mathbb{Q}[i]$ (where $a, b \in \mathbb{Q}$). Since $a + bi$ is a nonzero complex number. so is $a - bi$. Thus we can divide by these numbers: $\dfrac{1}{a+bi} = \dfrac{1}{a+bi} \cdot \dfrac{a-bi}{a-bi} = \dfrac{a-bi}{a^2+b^2} = \dfrac{a}{a^2+b^2} + \dfrac{-b}{a^2+b^2}i \in \mathbb{Q}[i]$ since $a/(a^2 + b^2)$ and $-b/(a^2 + b^2)$ belong to $\mathbb{Q}$. Therefore, every nonzero element of $\mathbb{Q}[i]$ is a unit. Thus $\mathbb{Q}[i]$ is a field.

(d) Let $R$ be a finite commutative ring with 1 and let $I$ be an ideal of $R$. Is it possible for $I$ to be prime and not maximal? Explain your answer.

$\boxed{\text{No.}}$ Recall that, in a commutative ring with 1, the ideal $I$ is maximal if and only if $R/I$ is a field. Fields are always integral domains. And since our ring is *finite* so are its quotients. Finite integral domains are fields. Finally, $I$ is prime if and only if $R/I$ is an integral domain. Therefore, for a *finite* commutative ring with 1, the ideal $I$ is maximal $\iff$ $R/I$ is a field $\iff$ $R/I$ is an integral domain $\iff$ $I$ is prime.

7. (15 points) An ideal question.

(a) Recall that $\mathbb{Z}[x]$ is the ring of polynomials with integer coefficients. Let $I = \{f(x) \in \mathbb{Z}[x] \mid f(0) \text{ is even}\}$. Prove that $I$ is an ideal of $\mathbb{Z}[x]$.

Notice that if $f(x) = 0$, then $f(0) = 0$ is even, so $0 \in I$ (we have a non-empty subset). Let $f, g \in I$. Then $f(0)$ and $g(0)$ are even. Thus $(f-g)(0) = f(0) - g(0)$ is even (since even minus even is even). Therefore, $f - g \in I$ (we have closure under subtraction). Next, let $f \in I$ and $h \in \mathbb{Z}[x]$, then $f(0)$ is even so that $(hf)(0) = h(0)f(0)$ is even (since an integer times an even integer is still even). Therefore, since we have a commutative ring, $fh = hf \in \mathbb{Z}[x]$ (and we have absorption on both sides). Thus $I$ is an ideal of $\mathbb{Z}[x]$.

(b) Let $I$ and $J$ be ideals of some ring $R$. Prove that $I \cap J$ is an ideal of $R$.

Note that $0 \in I$ and $0 \in J$ because they are ideals. Thus $0 \in I \cap J$. Let $a, b \in I \cap J$. Then $a, b \in I$ and $a, b \in J$. Now $I$ and $J$ are closed under subtraction, so $a - b \in I$ and $a - b \in J$. Thus $a - b \in I \cap J$. Finally, let $a \in I \cap J$ and $r \in R$. Then $a \in I$ and $b \in J$. Since $I$ and $J$ have both absorption properties, $ar, ra \in I$ and $ar, ra \in J$. Thus $ar, ra \in I \cap J$. Thus $I \cap J$ is an ideal (of $R$).

(c) Suppose $R$ is some ring and $\varphi : \mathbb{Z}_{10} \to R$ is an **onto** ring homomorphism. What can we say about the size of $R$? What can we say about $R$ being commutative or not?

Since this homomorphism is onto, $\varphi(\mathbb{Z}_{10}) = R$. The first isomorphism theorem says that $\mathbb{Z}_{10}/\ker(\varphi) \cong \varphi(\mathbb{Z}_{10}) = R$. Thus all sets involved a finite and we get the following formula: $10 = |\mathbb{Z}_{10}| = |R| \cdot |\ker(\varphi)|$. In other words, $R$ must be a ring of $\boxed{\text{size 1, 2, 5, or 10}}$. Next, since quotients of commutative rings are commutative and $R$ is isomorphic to a quotient of $\mathbb{Z}_{10}$ (a commutative) ring, $\boxed{R \text{ must be commutative}}$.

8. (7 points) The Fundamental Theorem of Finite Abelian Groups.

(a) List all of the non-isomorphic abelian groups of order $72 = 2^3 \cdot 3^2$. Circle any that are cyclic.

Recall that there are 3 partitions of 3: $3 = 2 + 1 = 1 + 1 + 1$ and 2 partitions of 2: $2 = 1 + 1$. Thus there will be $3 \cdot 2 = 6$ non-isomorphic Abelian groups of order 72. We list a representative from each isomorphism class written in both elementary divisor and invariant factor form (and circle the one that is cyclic):

$\boxed{\mathbb{Z}_8 \times \mathbb{Z}_9}$ ($\cong \mathbb{Z}_{72}$), $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9$ ($\cong \mathbb{Z}_2 \times \mathbb{Z}_{36}$), $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$ ($\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{18}$), $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ ($\cong \mathbb{Z}_3 \times \mathbb{Z}_{24}$), $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ ($\cong \mathbb{Z}_6 \times \mathbb{Z}_{12}$), $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ ($\cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_6$).

(b) Which of the abelian groups of order 72 contain elements of order 36?

This is visible from the invariant factor forms above. We need an invariant factor with 36 as a divisor: $\boxed{\mathbb{Z}_{72} \text{ and } \mathbb{Z}_2 \times \mathbb{Z}_{36}}$. The rest of the groups above have elements of orders at most 18, 24, 12, and 6 respectively.

9. (6 points) Suppose $G$ is a group of order 60 with subgroups $H$ and $K$. Moreover, suppose the order of $H$ is 15 and that $H \subsetneq K \subsetneq G$. Explain why $K$ must be a normal subgroup and why $G/K$ must be cyclic.

By Lagrange's theorem $|K|$ must divide $|G| = 60$ and $|H| = 15$ must divide $|K|$. So we must have that $|K|$ is a multiple of 15 and divisor of 60. This leaves us with 15, 30, and 60 as possibilities. However, since $H \neq K$ and $K \neq G$, we must have $|K| = 30$. Therefore, $[G : K] = |G|/|K| = 60/30 = 2$ and by the index 2 theorem, $K$ is a normal subgroup. Finally, the quotient group $G/K$ has order 2 (a prime) thus is cyclic!

10. (6 points) Let $\varphi : \mathbb{Q}[x] \to \mathbb{C}$ be defined by $\varphi(f(x)) = f(i)$ where $i^2 = -1$. **(a): Prove** $\varphi$ is a ring homomorphism. Note that the range of $\varphi$ is $\mathbb{Q}[i]$ and $\text{Ker}(\varphi) = (x^2 + 1)$ (Bonus: prove this). **(b): What** does the first isomorphism theorem say here? Bonus: Is $(x^2 + 1)$ a prime and/or maximal ideal of $\mathbb{Q}[x]$?

$\varphi(f+g) = (f+g)(i) = f(i) + g(i) = \varphi(f) + \varphi(g)$ and $\varphi(fg) = (fg)(i) = f(i)g(i) = \varphi(f)\varphi(g)$ for all $f, g \in \mathbb{Q}[x]$ (thus $\varphi$ is a homomorphism). If $f(x) = a_n x^n + \cdots + a_1 x + a_0$, then $f(i) = a_n i^n + \cdots + a_1 i + a_0$ simplifies to $A + Bi$ for some $A, B \in \mathbb{Q}$ since $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, etc. Therefore, $\varphi(\mathbb{Q}[x]) = \mathbb{Q}[i]$. Also, recall that for real polynomials that complex roots come in conjugate pairs. Therefore, for $f \in \mathbb{Q}[x]$, if $f(i) = 0$, then also $f(-i) = 0$. Therefore, we have $f(x) = (x - i)(x + i)g(x)$ for some polynomial $g(x)$. Thus $f(x) = (x^2 + 1)g(x)$ for some $g$. By the division algorithm, $g \in \mathbb{Q}[x]$. In other words, $\ker(\varphi) = \{f(x) \in \mathbb{Q}[x] \mid f(i) = 0\} = \{(x^2 + 1)g(x) \mid g(x) \in \mathbb{Q}[x]\} = (x^2 + 1)$ (the principal ideal generated by $x^2 + 1$).

The first isomorphism theorem then says: $\mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}[i]$. Problem 6(c) shows $\mathbb{Q}[i]$ is a field. Therefore, $(x^2 + 1)$ is a maximal (and thus prime) ideal of $\mathbb{Q}[x]$.