# Ring Theory Homeworks

**Remark 0.1.** Unless otherwise specified, we're working with commutative rings with unity 1.

## 1 Homework 7

**Remark 1.1.** Problems 1-4 are on group theory. Focus on Ring Theory for this exam (problems 5-8).

**Problem 1.2.** $S = \{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mid a, b \in \mathbb{R}\}$. Verify that $S$ is a ring (with unity) and show that it is isomorphic to the field of complex numbers.

I'll leave the first part as an exercise to the reader (*to prove $S$ is a ring*). To do this, you would need to prove $S$ is an abelian group under addition while also maintaining closure under multiplication, multiplicative associativity, and distributivity.

To show that $S$ is isomorphic to the field of complex numbers, we will show that the homomorphism $\varphi : a + bi \to \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ is injective and surjective.
For injectivity, we need to show that if $z_1, z_2 \in \mathbb{C}$ and $\varphi(z_1) = \varphi(z_2) \implies z_1 = z_2$.
Assume $\varphi(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} = \begin{bmatrix} a' & b' \\ -b' & a' \end{bmatrix} = \varphi(a' + b'i)$
$\implies \begin{bmatrix} a - a' & b - b' \\ -b - (-b') & a - a' \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$
$\implies a = a'$ and $b = b' \implies a + bi = a' + b'i \implies$ **injective**.
For surjectivity, all the matrices are of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ such that $a, b \in \mathbb{R}$ and the element $a + bi \in \mathbb{C}$ maps to it $\implies$ **surjective** because we can always find an $a + bi$ for every matrix in $S$
$\therefore \varphi$ is an isomorphism.

**Problem 1.3.** Prove $\mathbb{Q}[\sqrt(3)]$ is a field.

*Proof.* To do this, I will prove that $\mathbb{Q}[\sqrt(3)]$ is a subfield of $\mathbb{R}$.
For $a + b\sqrt(3), c + d\sqrt(3) \in \mathbb{Q}[\sqrt(3)]$, $(a + b\sqrt(3)) + (c + d\sqrt(3)) = (a + c) + (b + d)\sqrt(3) \in \mathbb{Q}(\sqrt(3))$ $\implies$ closed under addition.
$(a + b\sqrt(3)) * (c + d\sqrt(3)) = (ac + 3bd) + (ad + bc)\sqrt(3) \in \mathbb{Q}[\sqrt(3)] \implies$ closed under multiplication.
Suppose $a \neq 0$ and $b \neq 0$. Then, $\frac{1}{a+b\sqrt(3)} = \frac{a-b\sqrt(3)}{a^2-3b^2} = \frac{a}{a^2-3b^2} + (\frac{-b}{a^2-3b^2})\sqrt(3)$. Since $a^2 - 3b^2 \neq 0$ (because $\sqrt(3)$ is irrational), $\frac{a}{a^2-3b^2}, \frac{-b}{a^2-3b^2} \in \mathbb{Q} \implies \frac{1}{a+b\sqrt(3)} \in \mathbb{Q}[\sqrt(3)] \implies$ existence of multiplicative inverses.
$\therefore \mathbb{Q}[\sqrt(3)]$ is a subfield of $\mathbb{R}$ □

**Problem 1.4.** Determine whether $I = \{ \begin{bmatrix} 0 & n \\ 0 & m \end{bmatrix} \mid n, m \in \mathbb{Z}\}$ is an ideal in $R = \{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{Z}\}$.

*Proof.* To prove $I \lhd R$, we must prove product absorption such that given $x \in I$, $r \in R \implies rx = xr \in I$.
For some $n, m, a, b, c \in \mathbb{Z}$, we can define $x = \begin{bmatrix} 0 & n \\ 0 & m \end{bmatrix} \in I$, $r = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in R$.

$xr = \begin{bmatrix} 0 & n \\ 0 & m \end{bmatrix} * \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} 0 & cn \\ 0 & cm \end{bmatrix}$ and $cn, cm \in \mathbb{Z}$ (because $\mathbb{Z}$ is a field) $\implies xr \in I$
$\therefore I \lhd R$ □

**Problem 1.5.** Find all the maximal ideals in $\mathbb{Z}_6 \times \mathbb{Z}_{15}$, and in each case describe the quotient ring.

Since the prime divisors of 12 are 2 and 3, the prime ideals are $\{0\}$, $\{0, 2, 4, 6, 8, 10\}$, and $\{0, 3, 6, 9\}$ $\implies$ the 2 maximal ideals are $J = \{0, 2, 4, 6, 8, 10\}$ and $K = \{0, 3, 6, 9\}$ such that $\mathbb{Z}_{12}/J$ contains 2 elements ($\frac{12}{6} = 2$) and $\mathbb{Z}_{12}/K$ contains 3 elements ($\frac{12}{4} = 3$).

## 2 Homework 8

In the first four exercises, $R$ and $S$ are rings (with 1) and : $R \to S$ is a ring homomorphism.

**Problem 2.1.** If $\varphi$ is surjective and $I \lhd R$, show that $\varphi(I) \lhd S$.

*Proof.* To show that this is true, we only need to show that for all $s_1, s_2 \in S$ such that $s_1 \in \varphi(I)$, $\exists$ $r_1, r_2 \in R$ such that $r_1 \in I \lhd R$. This really implies that for our given elements of $s$, we must prove that $s_1 s_2 \in \varphi(I)$ and $s_1 + s_2 \in \varphi(I)$. Both of these follow from the properties of ring homomorphisms such that $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) = s_1 + s_2$ and $r_1 + r_2 \in I \implies s_1 + s_2 \in \varphi(I)$. Moreover, $\varphi(r_1 r_2) = \varphi(r_1) * \varphi(r_2) = s_1 s_2 \in \varphi(I)$ and $r_1 r_2 \in I \implies s_1 s_2 \in \varphi(I)$. $\therefore \varphi(I) \lhd S$. □

**Problem 2.2.** Prove that if $\varphi(I)$ is a prime ideal of $S$, then $I$ is a prime ideal for $R$.

*Proof.* It follows from the fourth isomorphism theorem in Ring Theory (lattice theorem) that for a commutative ring homomorphism, $\varphi : R \to S$, if $\varphi(I) \lhd S$, then $\varphi$ determines an injection: $\tilde{\varphi} : R/I \to S/\varphi(I)$. In this case, $\varphi(I) \lhd S$ is prime $\iff S/\varphi(I)$ is an integral domain. Note that $R/\tilde{\varphi}^{-1}(\varphi(I))$ embeds $S/\tilde{\varphi}^{-1}(\varphi(I))$. Since a subring of an integral domain is in turn an integral domain, $\tilde{\varphi}^{-1}(\varphi(I)) = I$ is necessarily prime. □

**Problem 2.3.** Does this follow for maximal ideals? (same as last question)

*Proof.* This is not the case and we will see why by assuming it is the case and working backwards. An ideals $J \lhd S$ is maximal if and only if $S/J$ is a field. Moreover, if we set $I$ to be the preimage of $J$, $R/I$ embeds the field $S/J$. However, subrings of fields are not necessarily also fields. Therefore, maximal ideals are not 'transferrable' in the same way that prime ideals can be transferred. However, if $\varphi$ is surjective, then the embedding $\tilde{\varphi}$ is surjective and therefore $\varphi$ is an isomorphism and $\mathbb{R}/I$ is a field (so $I$ is a maximal ideal of $R$). □

**Problem 2.4.** Assume that $R$ is a field and that $S$ is not the zero ring. Prove that $\varphi$ is injective.

*Proof.* $R$ is a field $\implies$ the only ideals of $R$ are $R$ or $\{0\}$. If $S \neq \{0\}$, then the fact that $R \lhd R \implies \varphi(S) \lhd S$ and this ensures based on the properties of the homomorphism that $\forall\, r \in R$, $\exists!\ s \in S$ such that $\varphi(r) = s$. This achieves the definition of injectivity for $\varphi$. □

**Problem 2.5.** Show that $Z(\mathbf{H}) = R$ where $\mathbf{H}$ denotes the skew field of quaternions.

*Proof.* If $a \in \mathbb{R}$ then $aq = qa \,\forall\, q \in \mathbf{H}$ because $a$ commutes with $i, j, k$. Conversely, let $q = a+bi+cj+dk$ lie in $Z(\mathbf{H})$. Then, $iq = qi \implies -b + a + dj - ck = -b + ai - dj + ck$. Equating coefficients yields $c = 0 = d \implies q = a + bi$. Moreover, $qj = jq \implies b = 0$, so $q = a \in \mathbb{R}$ as required. □

**Problem 2.6.** Let $R$ be a finite commutative ring with unity. Show that every prime ideal in $R$ is a maximal ideal in $R$.

*Proof.* Let $I$ be a prime ideal in $R$. Since $I$ is prime, $R/I$ is an integral domain and $R$ is finite $\implies$ $R/I$ is a finite integral domain $\implies$ $R/I$ is a field $\implies$ $I$ is a maximal ideal in $R$. □

**Problem 2.7.** Let $I, J$ be ideals in a ring $R$.

1. Show that $I + J = \{a + b \mid a \in I, b \in J\}$ is an ideal.
2. Show that $IJ = \{a_1b_1 + a_2b_2 + ... + a_nb_n \mid a_i \in I, b_i \in J\}$ is an ideal.
3. Show that $IJ \subseteq I \cap J$.
4. If $R$ is commutative and $I + J = R$, show that $IJ = I \cap J$.

1. *Proof.* To check if it is an ideal, we will verify that it is closed under addition and that it maintains product absorption. For any $x = a+b$, $y = c+d$ such that $a, c \in I$, $b, d \in J$ $\implies$ by definition of $I+J$, $x, y \in I+J$. In this case, $x+y = (a+c)+(b+d) \in I+J$ because $a+c \in I$ and $b+d \in J$. Moreover, if we take $r \in R$, $xr = ar + br$ $\implies$ $ar \in I$ and $br \in J$ because $I, J \lhd R$. Therefore, $xr \in I + J$ by definition $\implies$ $I + J$ is an ideal. □
2. *Proof.* To prove that $IJ$ is an ideal, we will verify that it is closed under addition and it maintains product absorption. For any $x \in I$, $y \in J$ $xy \in I$ and $xyinJ$ based on the properties of product absorption for those two ideals. Moreover, $xy \in IJ$ by definition. Based on the properties of $I, J$, for $r \in R$, $xr \in I$ $yr \in J$ and, therefore, $xyr \in IJ$ $\implies$ $IJ$ maintains product absorption. □
3. *Proof.* $\forall\ x \in I \cap J$, $x \in I$ and $x \in J$ by definition. But (wlog) for all $y \in I$, if $z \in J$ $\implies$ $yz \in I$ and $yz \in J$ based on product absorption for both ideals. Therefore $\forall\ yz \in IJ$, $yz \in I \cap J$ $\implies$ $IJ \subseteq I \cap J$. □
4. *Proof.* $I \cap J = (I \cap J)R = (I \cap J)(I + J) = I(I \cap J) + J(I \cap J)$. We know that $I \cap J \subseteq I$ and $I \cap J \subseteq J$ by definition of intersection $\implies$ $I(I \cap J) + J(I \cap J) \subseteq IJ + IJ = IJ$ $\implies$ $I \cap J = IJ$. □

**Problem 2.8.** Let $D$ be an integral domain and $a, b \in D$. Show that $< a >=< b >$ if and only if $a = ub$ for some unit $u$ in $U(D)$.

*Proof.* "$\rightarrow$": There are two cases that arise from $< a >=< b >$. (1) $a \in< b >$ $\implies$ $\exists\ u \in D$ such that $a = ub$ and (2) $b \in< a >$ $\implies$ $\exists\ v \in D$ such that $b = va$. Both (1) and (2) $\implies$ $a = u(va) = uva$ $\implies$ $a - uva = 0$ $\implies$ $a(1 - uv) = 0$ and, because $D$ has no zero divisors (because it is an integral domain), either $a = 0$ $\implies$ $b = v * a = 0$ $\implies$ $a = 1 * b$ such that $u = 1$ or $1 - uv = 0$ $\implies$ $uv = vu = 1$ $\implies$ $u, v \in U(D)$.

**Remark 2.9.** If $R$ is just a commutative ring with 1 and $a, b \in R$, then $< a >=< b >$ does not necessarily imply that $a = ub$ with $u \in U(R)$.

"$\leftarrow$" $a = ub$ with $u \in U(D)$ $\implies$ $a \in< b >$ and therefore $< a >\subseteq< b >$. However, because $u \in U(D)$, it follows that (given $u^{-1} \in D$), $b = u^{-1}a \in< a >$ $\implies$ $< b >\subseteq< a >$. Therefore, $< a >=< b >$. □

**Problem 2.10.** In the ring of Gaussian integers $\mathbb{Z}[i]$, consider the ideal $J =< 1 + i >$.

1. Show that $2 \in J$.
2. Find all the cosets of $J$ in $\mathbb{Z}[i]$.
3. Describe the quotient ring $\mathbb{Z}[i]/J$.

1. $(1+i)*(1-i) = 2 \in J$. The consequence is that $2r \in J \ \forall\ r \in R$.
2. Two ways of solving this:

   (a) *Proof.* Let $r = a+bi \in R$ with $a, b \in \mathbb{Z}$ be given. Since $2R \subseteq J$, we can reduce $a$ and $b$ modulo 2 without changing the coset $r+J$, i.e. if $r' = a' + b'i$ with $a, b \in \mathbb{Z}$ and $a' \equiv a \bmod 2$, $b' \equiv b \bmod 2$, then $r + J = r' + J$ since $r - r' \in 2R \subseteq J$. So, $r + J \in \{J, 1+J, i+J, (1+i)+J\}$. Now, $1+i \in J \implies (1+i)+J = J$. Furthermore, $i + J = -i + J$ since $2i \in J$ and $-i + J = 1 + J$ since $1 + i \in J$. Finally, $J \neq 1 + J$ since $1 \notin J$: If we had $1 \in J$, then there exists $a + bi \in R$ $(a, b \in \mathbb{Z})$ with $(a+bi)(1+i) = 1 \implies |a+bi|^2 * |1+i|^2 = 1^2 = 1 \implies (a^2+b^2)2 = 1$, which is impossible for $a, b \in \mathbb{Z}$ ($\implies a^2+b^2 = 0$ or $\geq 1$). Therefore, there are precisely 2 cosets modulo $J$, namely $J$ and $1+J$; in other words, $R/J = \{J, 1+J\}$. □

   (b) *Proof.* We directly compute the multiples of $1+i$ in $R$. $r = a+bi$ with $a, b \in \mathbb{Z} \implies r(1+i) = (a+bi)(1+i) = a + ai + bi + bi^2 = (a-b) + (a+b)i$. Note that $a - b \equiv a + b \bmod 2$ since $(a+b) - (a-b) = 2b \in 2\mathbb{Z}$.
   <u>Claim</u>: $J = \{m + ni \mid m, n \in \mathbb{Z} \text{ and } m \equiv n \bmod 2\ \} =: J'$. We just saw that $J = \{r(1+i) \mid r \in R\} \subseteq J'$. Now, let $m + ni \in J'$ with $m \equiv n \bmod 2$ be given. Then, $a = \frac{m+n}{2}$ and $b = \frac{n-m}{2}$ are in $\mathbb{Z} \implies r = a + bi \in R$ and $r(1+i) = (a-b) + (a+b)i = m + ni$. this shows that every element of $J'$ is in $J =< 1+i >$, i.e. $J' \subseteq J \subseteq J' \implies J = J'$. Now, with this description of $J$, it is easy to see that $R/J$ has precisely two elements such that $J = \{m + ni \mid m, n\mathbb{Z} \text{ and } m \equiv n \bmod 2\}$ and $R \setminus J = \{m + ni \mid m, n \in \mathbb{Z} \text{ and } m \not\equiv n \bmod 2\} = 1 + J$. □

3. By (2), $R/J = \{J, 1+J\} = \{0_{R/J}, 1_{R/J}\}$. Hence, $R/J$ is the field with 2 elements $\{0, 1\}$, a copy of $\mathbb{Z}_2$.

   **Remark 2.11.** The last statement is best generalized as follows: If $S$ is any ring with 1 such that $|S| = p$ and $p$ is a prime, then $S \cong \mathbb{Z}_p$ (and so $S$ is a field). Note first that, since $|S| = p$, $(S, +)$ is isomorphic to the cyclic group $\mathbb{Z}_p$. This implies that $\underline{char(S) = p \implies \text{the prime subring}}$ $S_0$ of $S$ is isomorphic to the ring (=field here) $\mathbb{Z}_p$. But $|S_0| = p = |S| \implies S_0 = S \implies S \cong \mathbb{Z}_p$

# 3 Homework 9

In the first two exercises, $R_1$ and $R_2$ are nonzero commutative rings with 1, $I_1 \lhd R_1$, $I_2 \lhd R_2$.

**Problem 3.1.**
1. Verify that $I_1 \times I_2 = \{(a, b) \mid a \in I_1, b \in I_2\}$ is an ideal of $R_1 \times R_2$.
2. Prove that **every** ideal $I$ of $R_1 \times R_2$ is of the form $I_1 \times I_2$ for suitable ideals $I_1$ of $R_1$ and $I_2$ of $R_2$ (Hint: if $(a, b)$ is an element of $I$, show that $(a, 0)$ and $(0, b)$ are also in $I$).

1. *Proof.* For $a_1, a_2 \in I_1, b_1, b_2 \in I_2, c_1 \in R_1, d_1 \in R_2$, it follows from the fact that $I_1 \lhd R_1$ and $I_2 \lhd R_2 \implies (a_1, b_1), (a_2, b_2) \in I_1 \times I_2$. Moreover, $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2) \in I_1 \times I_2$ because $a_1 + a_2 \in I_1$ and $b_1 + b_2 \in I_2$. Moreover, for $(c_1, d_1) \in R_1 \times R_2$ $(a_1, b_1) * (c_1, d_1) = (a_1c_1, b_1d_1) \in I_1 \times I_2$ because $a_1c_1 \in I_1$ and $b_1d_1 \in I_2$ based on the product absorption properties of $I_1, I_2 \implies I_1 \times I_2 \lhd R_1 \times R_2$. □

2. *Proof.* $0_{R_1} \in I_1$, $0_{R_2} \in I_2$ because $I_1 \lhd R_1, I_2 \lhd R_2 \implies (0,0) \in I_1 \times I_2$. Therefore, if $(a,b) \in I = I_1 \times I_2 \implies (a, 0_{R_2}) \in I$ and $(0_{R_1}, b) \in I$ because $0_{R_2} \in I_2$ and $0_{R_1} \in I_1$. Now, define $I_1 := \{a \in R_1 \mid (a,b) \in I \text{ and } b \in R_2\} \lhd R_1$, $I_2 := \{b \in R_2 \mid (a,b) \in I \text{ and } a \in R_1\} \lhd R_2$.
$\therefore I_1 \times I_2 = I \lhd R_1 \times R_2$. □

**Problem 3.2.** 1. Show that the map $\varphi : R_1 \times R_2 \to (R_1/I_1) \times (R_2/I_2)$ defined by $\varphi(a,b)) = (a + I_1, b + I_2)$ is a surjective ring homomorphism with kernel $I_1 \times I_2$. Deduce that the quotient ring $(R_1 \times R_2)/(I_1 \times I_2)$ is isomorphic to $(R_1/I_1) \times (R_2/I_2)$.

2. If $I_1$ is a maximal ideal of $R_1$ and $I_2$ is a maximal ideal of $R_2$, show that $I_1 \times R_2$ and $R_1 \times I_2$ are maximal ideals of $R_1 \times R_2$.

3. Show that **all** maximal ideals of $R_1 \times R_2$ are of the form described in (2).

1. *Proof.* Let $\varphi(a,b) = (a + I_1, b + I_2) \in R_1/I_1 \times R_2/I_2 \implies \varphi$ is surjective because the homomorphism maps to every element in its image. Let $(a,b) \in I_1 \times I_2$. Then, $\varphi(a,b) = 0 \implies I_1 \times I_2 \subseteq Kern(\varphi)$. Suppose that $(a,b) \notin I_1 \times I_2$. Wlog $a \notin I_1 \implies \varphi(a,b) = (a+I_1, b+I_2) \neq (0,0)$ since $a + I_1 \neq I_1 \implies$ by the first isomomorphism theorem for rings, $\frac{R_1 \times R_2}{I_1 \times I_2} \simeq \frac{R_1}{I_1} \times \frac{R_2}{I_2}$ □

2. *Proof.* Suppose $I_1 \times J_1 \lhd R_1 \times R_2$ and $I_1 \times J_1 \subseteq I_1 \times R_1$. Because $I_2$ is the maximal ideal of $R_2$ $\implies J_1 = I_2 \implies I_1 \times J_1 = I_1 \times I_2$ or $J_1 = R_2 \implies I_1 \times J_1 = I_1 \times R_2$. This proves that $I_1 \times R_2$ is a maximal ideal of $R_1 \times R_2$.
Conversely, suppose that $J_1 \times I_2 \lhd R_1 \times R_2$ and $J_1 \times I_2 \subseteq R_1 \times I_1$. Because $I_1$ is the maximal ideal of $R_1 \implies J_1 = I_1 \implies J_1 \times I_2 = I_1 \times I_2$ or $J_1 = R_1 \implies J_1 \times I_2 = R_1 \times I_2$. This shows that $R_1 \times I_2$ is a maximal ideal of $R_1 \times R_2$. □

3. *Proof.* $I \times R_2 \lhd R_1 \times R_2$ (WTS Maximal). Suppose $\exists\, I_1 \times I_2 \lhd R_1 \times R_2$ and $I_1 \times I_2 > I \times R_2 \implies I_1 > I \implies I_1 = R_1$. Similarly, for $R_1 \times I \lhd R_1 \times R_2$, suppose $\exists\, I_1 \times I_2 \lhd R_1 \times R_2$ and $I_1 \times I_2 > R_1 \times I \implies I_2 > I \implies I_2 = R_2$. This shows that any maximal ideal of $R_1 \times R_1$ takes this form. □

**Problem 3.3.** Find an example of a nonzero commutative ring $R$ and a polynomial $f(x)$ with $deg(f(x)) > 0$ such that $f(x)$ is a unit of $R[x]$.

$2x + 1$ in $\mathbb{Z}/4\mathbb{Z}$. Specifically, $(2x+1)^2 = 4x^2 + 4x + 1 = 1$ in $\mathbb{Z}/4\mathbb{Z}$

**Problem 3.4.** Let $\Upsilon : \mathbb{Z}[x] \to \mathbb{Z}[i]$ be the (by 2.3.3 uniquely determined) ring homomorphism which is the identity when restricted to $\mathbb{Z}$ and satisfied $\Upsilon(x) = i$.

1. Compute $\Upsilon(2 + 3x + 4x^2 - 5x^3 + x^4)$ i.e. write it in the form $a + bi$ with $a, b \in \mathbb{Z}$.

2. Prove that the principal ideal $< x^2 + 1 >$ of $\mathbb{Z}[x]$ is equal to the kernel of $\Upsilon$.

3. Decide whether $< x^2 + 1 >$ is a prime or a maximal ideal of $\mathbb{Z}[x]$.

1. $\Upsilon(2 + 3x + 4x^2 - 5x^3 + x^4) = 2 + 3i + 4i^2 - 5i^3 + i^4 = -1 + 8i$

2. $\Upsilon(x^2+1) = i^2 + 1 = -1 + 1 = 0 \implies x^2 + 1 \in Kern(\Upsilon) \implies < x^2 + 1 > \subseteq Kern(\Upsilon)$, since $Kern(\Upsilon) \lhd \mathbb{Z}[x]$. Now assume that $f(x) \in Kern(\Upsilon)$. We first apply the <u>division algorithm</u> (2.3.7) to $f(x)$ and $g(x) = x^2 + 1 \in \mathbb{Z}[x]$. Note that $l(x^2+1) = 1 \in U(\mathbb{Z})$. So there exists $q(x), r(x) \in \mathbb{Z}[x]$ with $f(x) = q(x)(x^2+1) + r(x)$ <u>and</u> $r(x) = 0$ or $deg(r(x)) < deg(x^2+1) = 2$. The latter implies that $r(x) = a + bx$ with $a, b \in \mathbb{Z}$ (If $r(x) = 0$, then $a = b = 0$). Now we use

that $f(x) \in Kern(\Upsilon)$:
$0 = \Upsilon(f(x)) = \Upsilon(q(x)(x^2+1)+r(x)) = \Upsilon(q(x))\,\Upsilon\,(x^2+1) + \Upsilon(a+bx) = \Upsilon(q(x)) * 0 + \Upsilon(a+bx) = \Upsilon(a+bx) = a+bi$ but if $a+bi = 0$ in $\mathbb{Z}[i]$, then $a = b = 0 \implies \underline{r(x) = 0}$. Hence, $f(x) = q(x)(x^2+1) \in < x^2+1 >$. Since $f(x) \in Kern(\Upsilon)$ was arbitrary, this shows that $Kern(\Upsilon) \subseteq < x^2+1 > \subseteq Kern(\Upsilon) \implies \underline{Kern(\Upsilon) = < x^2+1 >}$

3. $\Upsilon$ is surjective (by $\Upsilon(a+bx) = a+bi\ \forall\ a,b \in \mathbb{Z}$), and so by the isomorphism theorem 2.1.11 $\mathbb{Z}[x]/< x^2+1 > = \mathbb{Z}[x]/Kern(\Upsilon) \cong \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is an integral domain but not a field, it follows from 2.2.8 and 2.2.7 that $< x^2+1 >$ is a <u>prime ideal</u> but <u>not a maximal ideal</u> of $\mathbb{Z}[x]$

**Problem 3.5.** Show that the principal ideal $< x^2+1 >$ of $\mathbb{R}[x]$ is a maximal ideal.

*Proof.* $< x^2+1 >$ is a prime ideal (from the previous question) $\implies \mathbb{R}[x]/< x^2+1 >$ is an integral domain and because $\mathbb{R}[x]$ is finite, $\mathbb{R}[x]/< x^2+1 >$ is a finite integral domain $\implies R[x]/< x^2+1 >$ is a field. WTS $\exists$ isomomorphism $\varphi : \mathbb{R}[x]/< x^2+1 > \to \mathbb{C}$ which maps $\varphi(-ax^2+bx) \to a+bi$. Because this covers all $a+bi \in \mathbb{C} \implies \varphi$ is surjective because we only need to change $a, b \in \mathbb{R}$ for $-ax^2+bx$ to map to all of the elements in $\mathbb{C}$ of the form $a+bi$.
$\varphi$ is surjective $\iff < x^2+1 >$ is a maximal ideal. □

# 4 Homework 10

**Problem 4.1.** Prove that the polynomials $q(x)$ and $r(x)$ in the Division Algorithm are uniquely determined.

*Proof.* Suppose we have $f(x) = q_1(x)g(x) + r_1(x)$ <u>and</u> $f(x) = q_2(x)g(x) + r_2(x)$ such that $r_i(x) = 0$ or $deg(r_i(x)) < deg(g(x))$. Subtracting the two equations, we get $0 = [q_1(x) - q_2(x)]g(x) + [r_1(x) - r_2(x)]$. Therefore, $[q_1(x) - q_2(x)]g(x) = r_2(x) - r_1(x)$. We must have $r_2(x) - r_1(x) = 0$ because if this isn't true, then $deg[r_2(x) - r_1(x)] < deg(g(x))$ (which is a clear contradiction). Therefore, we must have $r_1(x) = r_2(x)$ and because $q_1(x) - q_2(x) = 0 \implies q_1(x) = q_2(x)$. □