ABSTRACT ALGEBRA — SECOND MIDTERM EXAM

ARDEN RASMUSSEN

NOVEMBER 26, 2019

1. Problem

As usual, let $\mathbb{N}$ denote the set of positive integers. Consider the following relation on $\mathbb{N}\times\mathbb{N}$:

$$(a,b)\cong(c,d)\longleftrightarrow\exists k,l\in\mathbb{N},(a+k,b+k)=(c+l,d+l).$$

(a). Show that $\cong$ is an equivalence relation. From now on let R denote the set of equivalence classes of $\cong$ and let $[(a,b)]$ denote the equivalence class of $(a,b)\in\mathbb{N}\times\mathbb{N}$.
Claim: $\cong$ is an equivalence relation.

Proof. To show that $\cong$ is an equivalence relation, we show that it is reflexive, symmetric, and transitive.

reflexive: Consider $(a,b)\in\mathbb{N}\times\mathbb{N}$. Then let $k=l=1\in\mathbb{N}$. We compute

$$(a+1,b+1)=(a+1,b+1).$$

Thus $(a,b)\cong(a,b)$, and $\cong$ is reflexive.

symmetric: Consider $(a,b),(c,d)\in\mathbb{N}\times\mathbb{N}$, with $(a,b)\cong(c,d)$. Since $(a,b)\cong(c,d)$ then there exists some $k_1,l_1\in\mathbb{N}$ such that

$$(a+k_1,b+k_1)=(c+l_1,d+l_1).$$

Now $k_2=l_1,l_2=k_1$, then we compute

$$(c+k_2,d+k_2)=(c+l_1,d+l_1)=(a+k_1,b+k_1)=(a+l_2,b+l_2).$$

Thus $(c,d)\cong(a,b)$, and $\cong$ is symmetric.

transitive: Consider $(a,b),(c,d),(e,f)\in\mathbb{N}\times\mathbb{N}$, with $(a,b)\cong(c,d)$, and $(c,d)\cong(e,f)$. From this assumption there exist some $k_1,k_2,l_1,l_2\in\mathbb{N}$ such that

$$(a+k_1,b+k_1)=(c+l_1,d+l_1)\quad(c+k_2,d+k_2)=(e+l_2,f+l_2).$$

Now consider $k=k_1+k_2$, and $l=l_1+l_2$. Then we compute

$$\begin{aligned}(a+k,b+k)&=(a+k_1+k_2,b+k_1+k_2)\\&=(c+l_1+k_2,d+l_1+k_2)\\&=(e+l_1+l_2,f+l_1+l_2)\\&=(e+l,f+l)\end{aligned}$$

Thus $(a,b)\cong(e,f)$, and $\cong$ is transitive.

Thus $\cong$ is an equivalence relation. □

(b). Show that the operation

$$[(a,b)]+[(c,d)]=[(a+c,b+d)]$$

is well-defined.
Claim: The operation $+$, defined above is well defined.

Proof. Consider $(a,b),(c,d),(e,f),(g,h)\in\mathbb{N}\times\mathbb{N}$, with $(a,b)\cong(e,f)$ and $(c,d)\cong(g,h)$. Then consider

$$[(a,b)]+[(c,d)]=[(a+c,b+d)].$$

From the assumption there exists some $k_1,k_2,l_1,l_2\in\mathbb{N}$ such that

$$(a+k_1,b+k_1)=(e+l_1,f+l_1)\quad(c+k_2,d+k_2)=(g+l_2,h+l_2).$$

Now consider some $k=k_1+k_2$, and $l=l_2+l_2$. Now we compute

$$\begin{aligned}(a+c+k,b+d+k)&=(a+c+k_1+k_2,b+d+k_1+k_2)\\&=(a+k_1+c+k_2,b+k_1+d+k_2)\\&=(e+l_1+g=l_2,f+l_1+h+l_2)\\&=(e+g+l,f+h+l)\end{aligned}$$

We notice that $[(a+c,b+d)]=[(e+g,f+h)]$, and thus we can see

$$[(a,b)]+[(c,d)]=[(a+c,b+d)]=[(e+g,f+h)]=[(e,f)]+[(g,h)].$$

Then we conclude that this operation is well defined. □

(c). The operation $+$ can be shown to be associative and commutative. Does $(R,+)$ constitute a group? If you answer is "no", explain why. If you answer is "yes", address the identity and the inverse in this group. You are expected to prove all you claims for full credit.

Yes, $(R,+)$ constitutes a group.
Claim: The identity of $(R,+)$ is given by $[(1,1)]$.

Proof. Consider $[(a,b)]\in R$, then we compute

$$[(a,b)]+[(1,1)]=[(a+1,b+1)].$$

Then by the definition of $\cong$, we notice that $(a+1,b+1)\cong(a,b)$, so

$$[(a,b)]+[(1,1)]=[(a+1,b+1)]=[(a,b)].$$

□

Claim: The inverse of $[(a,b)]\in R$ is given by $[(b,a)]\in R$.

Proof. Consider some $[(a,b)]\in R$, then we compute

$$[(a,b)]+[(b,a)]=[(a+b,b+a)].$$

By the definition of $\cong$, we notice that $(a+b,a+b)\cong(1,1)$, so

$$[(a,b)]+[(b,a)]=[(a+b,b+a)]=[(1,1)].$$

□

(d). Show that the operation

$$[(a,b)]\cdot[(c,d)] = [(ac+bd, ad+bc)]$$

is well-defined.
Claim: The operation $\cdot$, defined above is well defined.

Proof. Consider $(a,b),(c,d),(e,f),(g,h)\in\mathbb{N}\times\mathbb{N}$, with $(a,b)\cong(e,f)$ and $(c,d)\cong(g,h)$. Then consider

$$[(a,b)]\cdot[(c,d)] = [(ac+bd, ad+bc)].$$

From the assumption there exists some $k_1,k_2,l_1,l_2\in\mathbb{N}$ such that

$$(a+k_1,b+k_1) = (e+l_1,f+l_1) \quad (c+k_2,d+k_2) = (g+l_2,h+l_2).$$

Now consider some $k = k_1c+k_1d+k_2e+k_2f$, and $l = l_1c+l_1d+l_2e+l_2f$. Now we compute

$$\begin{aligned}
&(ac+bd+k, ad+bc+k)\\
&= (ac+bd+k_1c+k_1d+k_2e+k_2f, ad+bc+k_1c+k_1d+k_2e+k_2f)\\
&= (c(a+k_1)+d(b+k_1)+k_2e+k_2f, d(a+k_1)+c(b+k_1)+k_2e+k_2f)\\
&= (c(e+l_1)+d(f+l_1)+k_2e+k_2f, d(e+l_1)+c(f+l_1)+k_2e+k_2f)\\
&= (ce+l_1c+df+l_1d+k_2e+k_2f, de+l_1d+cf+l_1c+k_2e+k_2f)\\
&= (e(c+k_2)+f(d+k_2)+l_1c+l_1d, e(d+k_2)+f(c+k_2)+l_1c+l_1d)\\
&= (e(g+l_2)+f(h+l_2)+l_1c+l_1d, e(h+l_2)+f(g+l_2)+l_1c+l_1d)\\
&= (eg+fh+l_1c+l_1d+l_2e+l_2f, eh+fg+l_1c+l_1d+l_2e+l_2f)\\
&= (eg+fh+l, eh+fg+l)
\end{aligned}$$

We notice that $[(ac+bd,ad+bc)] = [(eg+fh,eh+fg)]$, and thus we can see

$$[(a,b)]\cdot[(c,d)] = [(ac+bd,ad+bc)] = [(eg+fh,eh+fg)] = [(e,f)]\cdot[(g,h)].$$

Then we conclude that this operation is well defined. □

(e). The operation $\cdot$ can be shown to be associative and commutative. Does $(R,\cdot)$ constitute a group? If you answer is "no", explain why. If you answer is "yes", address the identity and the inverse in this group. You are expected to prove all your claims for full credit.

No, $(R,\cdot)$ does not constitutes a group.
Claim: The identity of $(R,\cdot)$ is given by $[(2,1)]$.

Proof. Consider $[(a,b)]\in R$, then we compute

$$[(a,b)]\cdot[(2,1)] = [(2a+b, a+2b)].$$

Now we consider $k=1$ and $l = a+b+1$. Then we compute

$$(2a+b+1, a+2b+1) = (a+a+b+1, b+a+b+1) = (a+l, b+l).$$

Thus we see that $[(a,b)]\cdot[(2,1)] = [(a,b)]$. And we conclude that $[(2,1)]$ is the identity. □

Claim: Not all elements have an inverse.

Proof. Consider the element $[(4,2)] \in R$. Assume that the inverse does exist, and is of the from $[(a,b)] \in R$. Then we compute

$$\begin{aligned} [(4,2)] \cdot [(a,b)] &= [(2,1)] \\ [(4a+2b, 2a+4b)] &= [(2,1)] \end{aligned}$$

Then there exists some $k, l \in \mathbb{N}$ such that $(4a+2b+k, 2a+4b+k) = (2+l, 1+l)$. We now notice, that

$$\begin{aligned} 4a+2b+k = 2+l &= 2a+4b+k+1 \\ 4a+2b &= 2a+4b+1 \\ 2a &= 2b+1 \end{aligned}$$

If $a, b \in \mathbb{R}$ then we would have $a = b + \frac{1}{2}$, but since $a \in \mathbb{N}$, then this does not exists. This is a contradiction of our assumption, and thus we can conclude that $[(4,2)]$ does not have an inverse, and thus $(R, \cdot)$ is not a group. □

(f). Is $(R,+,\cdot)$ a (commutative) ring (with identity)? If your answer is "no", explain why. If your answer is "yes", address the identity and the inverse in this group. You are expected to prove all your claims for full credit.

Yes $(R,+,\cdot)$ is a (commutative) ring (with identity). We assumed that $\cdot$ is commutative, and in (e) we proved that there is a multiplicative identity, and in (c) we proved that $(R,+)$ is a group.
Claim: In $(R,+,\cdot)$, $\cdot$ distributes over $+$.

Proof. Consider $[(a,b)], [(c,d)], [(e,f)] \in R$, then we compute

$$\begin{aligned} [(a,b)] \cdot ([(c,d)] + [(e,f)]) &= [(a,b)] \cdot [(c+e, d+f)] \\ &= [(ac+ae+bd+bf, ad+af+bc+be)] \\ &= [(ac+bd, ad+bc)] + [(ae+bf, af+be)] \\ &= [(a,b)] \cdot [(c,d)] + [(a,b)] \cdot [(e,f)] \end{aligned}$$

Thus $\cdot$ distributes over $+$, and we can conclude that $(R,+,\cdot)$ is a ring. □

(g). Is $(R,+,\cdot)$ a field? If you answer is "no", explain why. If your answer is "yes", address the identity and the inverse in this group. You are expected to prove all your claims for full credit.

No, $(R,+,\cdot)$ is not a field. We demonstrated an example of an element that does not have a multiplicative inverse in (e).

(h). The above is not a random example: $(R,+,\cdot)$ is actually isomorphic to something very familiar. What is that something? Come up with an explicit isomorphism, and verify that it indeed is an isomorphism.
Claim: $F : R \to \mathbb{Z}$ given by $F : [(a,b)] \mapsto a - b$ is an isomorphism.

Proof. To show that F is an isomorphism, we must show that it is a homomorphism and bijection.

homomorphism: Consider $[(a,b)], [(c,d)] \in R$. Then we compute

$$\begin{aligned} F([(a,b)] + [(c,d)]) &= F([(a+c, b+d)]) \\ &= (a+c) - (b+d) \\ &= a - b + c - d \\ &= F([(a,b)]) + F([(c,d)]). \end{aligned}$$

We now compute

$$\begin{aligned} F([(a,b)] \cdot [(c,d)]) &= F([(ac+bd, ad+bc)]) \\ &= ac + bd - ad - bc \\ &= (a-b) \cdot (c-d) \\ &= F([(a,b)]) \cdot F([(c,d)]). \end{aligned}$$

Finally we compute

$$F([(2,1)]) = 1.$$

Thus as F preserves $+$ and $\cdot$, and 1, then it is a homomorphism.

one-to-one: Consider $[(a,b)], [(c,d)] \in R$, with $F([(a,b)]) = F([(c,d)])$, that is to say $a-b = c-d$. We now consider some $k = d, l = b$, then we notice, from the assumption, we know that $a + d = c + b$. We now compute

$$(a+k, b+k) = (a+d, b+d) = (c+b, d+b) = (c+l, d+l).$$

Thus F is one to one.

onto: Consider some $z \in \mathbb{Z}$, then we consider $[(z+1,1)] \in R$. We then compute $F([(z+1,1)]) = z+1-1 = z$, thus F is onto.

We conclude, since F is a homomorphism, one to one, and onto, then it is an isomorphism. □

2. Problem

(a). Compute the kernel and the image of the homomorphism

$$F : \mathbb{Q}[X] \to \mathbb{R}$$

given by

$$F : P \mapsto P\left(\sqrt[4]{2}\right).$$

All claims are expected to be proven in detail, using element chasing and the like.

Claim: $\left(X^4 - 2\right)$ is maximal.

Proof. First we demonstrate that $X^4 - 2$ is irreducible. Considering $x^4 - 2 \in \mathbb{R}$, we can find that

$$x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2})$$

Since $\mathbb{R}$ is a field, then we know that any factorization is unique, thus there is not other factorization of $(x^4 - 2)$ in $\mathbb{R}$. Since $\mathbb{Q} \subset \mathbb{R}$, then this must be the factorization in $\mathbb{Q}$ as well, but as $\sqrt{2} \notin \mathbb{Q}$, then this factorization does not exist, and so $X^4 - 2$ is irreducible.

Now we show that $(X^4 - 2)$ is maximal. We consider the ideal $(X^4 - 2)$. To show that it is maximal, consider some ideal I, such that

$$(X^4 - 2) \subsetneq I \subsetneq \mathbb{Q}[X].$$

Then since $\mathbb{Q}[X]$ is a PID, then there exists some $(P) = I$, and then

$$X^4 - 2 \in (P) \to Q \cdot P = X^4 - 2.$$

But, we have shown that $X^4 - 2$ is irreducible, and thus Q or P must be unit, and so either $(X^4 - 2) = (P)$ or $(P) = \mathbb{Q}[X]$. This is a contradiction to our assumption, and thus $(X^4 - 2)$ must be maximal. □

Claim: $\mathit{Img}\ F = \left\{a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8} | a, b, c, d \in \mathbb{Q}\right\}$.

Proof. Consider some $a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8}$, with $a, b, c, d \in \mathbb{Q}$. Then let $P = a + bx + cx^2 = dx^4 \in \mathbb{Q}[X]$. Now we consider $F(P)$, and we compute

$$\begin{aligned} F(P) = P(\sqrt[4]{2}) &= a + b\sqrt[4]{2} + c\left(\sqrt[4]{2}\right)^2 + d\left(\sqrt[4]{2}\right)^3 \\ &= a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8}. \end{aligned}$$

Thus for any x in $\left\{a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8} | a, b, c, d \in \mathbb{Q}\right\}$ we can find P such that $F(P) = x$, and we conclude that this is the $\mathit{Img}\ F$. □

Claim: $\mathit{Ker}\ F = \left(X^4 - 2\right)$.

Proof. Consider $P \in (X^4 - 2)$, then $P = Q(X^4 - 2)$ and $F(P) = F(Q)F(X^4 - 2) = F(Q) \cdot 0 = 0$. Thus $(X^4 - 2) \subseteq \mathit{Ker}\ F$. But since we have shown that $(X^4 - 2)$ is maximal, then we conclude that $\mathit{Ker}\ F = \mathbb{Q}[X]$, or $(X^4 - 2) = \mathit{Ker}\ F$. But we know from the proof of image that $\mathit{Ker}\ F \neq \mathbb{Q}[X]$, so we must conclude that $(X^4 - 2) = \mathit{Ker}\ F$. □

(b). Apply the 1st isomorphism theorem to F to show that

$$\left\{a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8} | a, b, c, d \in \mathbb{Q}\right\}$$

is a field as well as a 4-dimensional algebra over $\mathbb{Q}$. All claims involving irreducibility of various polynomials or linear independence are to be justified/proven.
Claim: $\left\{a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8} | a, b, c, d \in \mathbb{Q}\right\}$ is a field.

Proof. From the first isomorphism theorem, we know that

$$\mathbb{Q}[X]/(X^4 - 2) \cong \left\{a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8} | a, b, c, d \in \mathbb{Q}\right\}$$

Then since $(X^4 - 2)$ is maximal, then we conclude that $\mathbb{Q}[X]/(X^4 - 2)$ is a field, and thus $\left\{a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8} | a, b, c, d \in \mathbb{Q}\right\}$ is a field. □

Claim: $\left\{a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8} | a, b, c, d \in \mathbb{Q}\right\}$ is a 4-dimensional algebra over $\mathbb{Q}$, with basis $\left\{1, \sqrt[4]{2}, \sqrt[4]{4}, \sqrt[4]{8}\right\}$.

Proof. Assume that the elements of our claim of a basis are not linearly independent, that is to say for some $\alpha, \beta, \gamma, \delta \in \mathbb{Q}$, with at least one not equal to zero and

$$\alpha \cdot 1 + \beta \cdot \sqrt[4]{2} + \gamma \cdot \sqrt[4]{4} + \delta \cdot \sqrt[4]{8} = 0.$$

Then by our proof of the image, we can construct P such that $P(\sqrt[4]{2}) = \alpha + \beta\sqrt[4]{2} + \gamma\sqrt[4]{4} + \delta\sqrt[4]{8} = 0$. This implies that $P \in Ker\ F$. If $P \in Ker\ F$ then there exists some Q such that

$$Q(X^4 - 2) = P$$
$$X^4 - 2 = P/Q$$

But since degree of $X^4 - 2$ is 4 and the largest possible degree for our P is 3, then we can see that it is not possible for there to exist a Q to satisfy this equation. Thus we have a contradiction and can conclude that $\alpha = \beta = \gamma = \delta = 0$, and thus this basis is linearly independent.

We can see that our basis spans the space, from the construction of the basis, and the definition of of the vector space.

Finally we verify that the vector space has scalar multiplication. Consider $q \in \mathbb{Q}$ and $a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8}$. Then we compute

$$q \cdot \left(a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8}\right) = qa + qb\sqrt[4]{2} + qc\sqrt[4]{4} + qd\sqrt[4]{8}.$$

We note that this is also an element of the vector space, and thus it is closed under scalar multiplication. Thus we can conclude that this is a 4-dimensional algebra over $\mathbb{Q}$. □

3. Problem

In an early homework assignment you investigated the ring of paracomplex numbers

$$\mathbb{C}' = \{a + b\mathbf{i} | a, b \in \mathbb{R}\}$$

in which the standard rules of addition and multiplication apply with the exception of

$$\mathbf{i}^2 = 1.$$

(a). Apply the 1st isomorphism theorem to prove that

$$\mathbb{R}[X]/(X^2 - 1) \cong \mathbb{C}' \quad \mathbb{R}[X]/(X - 1) \cong \mathbb{R} \quad \mathbb{R}[X]/(X + 1) \cong \mathbb{R}.$$

Lemma 1. *Any function of the form $F : R[X] \to P$ given by $F : P \mapsto P(r)$, for any ring R, P, and form some $r \in R$. First we show that F preserves $+$*

$$F(P + Q) = (P + Q)(r) = P(r) + Q(r) = F(P) + F(Q).$$

Now we show that F preserves $\cdot$

$$F(P \cdot Q) = (PQ)(r) = P(r) \cdot Q(r) = F(P) \cdot F(Q).$$

Now we show that identity is preserved

$$F(1) = 1.$$

Claim: $F : \mathbb{R}[X] \to \mathbb{C}'$ given by $F : P \mapsto P(\mathbf{i})$ is a homomorphism, with $Img\ F = \mathbb{C}'$ and $Ker\ F = (X^2 - 1)$.

Proof. By the lemma we conclude that F is a homomorphism. Now we show that the $Img\ F$ is $\mathbb{C}'$. Consider some element $a + b\mathbf{i} \in \mathbb{C}'$. Then let $P = a + bx \in \mathbb{R}[X]$. We compute

$$F(P) = F(a + bx) = a + b\mathbf{i}.$$

Thus for any element of $x \in \mathbb{C}'$ we can construct some $P \in \mathbb{R}[X]$ such that $F(P) = x$. Thus the image of F is $\mathbb{C}'$.

Now we demonstrate that the $Ker\ F = (X^2 - 1)$. First consider some $P \in \big(X^2 - 1\big)$, then by the definition of an ideal, we know $P = Q \cdot (x^2 - 1)$ for some $Q \in \mathbb{R}[X]$. Then we compute

$$F(P) = F(Q \cdot (x^2 - 1)) = F(Q) \cdot F(x^2 - 1) = F(Q) \cdot 0 = 0.$$

Now consider some $P \in Ker\ F$, that is to say $P(\mathbf{i}) = 0$. Since $\mathbb{R}[X]$ is a field, then we know that division algorithm exists, and so we can construct some $Q, R \in \mathbb{R}[X]$, such that

$$P = Q(x^2 - 1) + R.$$

Then we consider $F(P)$, and from the other direction that we have proven, we know $F(Q(x^2 - 1)) = 0$, and thus we find

$$F(P) = F(R) = R(\mathbf{i}) = 0.$$

From the division algorithm, we know that the degree of R must be less than that of $(x^2 - 1)$, thus we know that R must be of the form $r_1 + r_2 x$. Then we find

$$r_1 + r_2\mathbf{i} = 0.$$

From here is is clear that $r_1 = r_2 = 0$, and thus we find that $R = 0$, and thus by the division algorithm, we know that $P = Q(x^2 - 1)$, and so we can conclude that $P \in \big(X^2 - 1\big)$. Hence $Ker\ F = \big(X^2 - 1\big)$.

Thus by the first isomorphism theorem we know

$$\mathbb{R}[X]/(X^2 - 1) \cong \mathbb{C}'.$$

□

Claim: $F : \mathbb{R}[X] \to \mathbb{R}$ given by $F : P \mapsto P(1)$ is a homomorphism, with $Img\ F = \mathbb{R}$ and $Ker\ F = (X - 1)$.

Proof. By the lemma we conclude that F is a homomorphism. Now we show that the $Img\ F$ is $\mathbb{R}$. Consider some element $r \in \mathbb{R}$, then let $P = r$, we compute

$$F(P) = P(1) = r$$

Thus for any element of $r \in \mathbb{R}$ we can construct some $P \in \mathbb{R}[X]$ such that $F(P) = x$, so we conclude that the image of F is $\mathbb{R}$.

Now we prove that the $Ker\ F = (X-1)$. First we note that $(X-1)$ is irreducible, as the degree is 1. Now consider some $P \in (X - 1)$. Then by the definition of an ideal, we know that $P = Q \cdot (x - 1)$ for some $Q \in \mathbb{R}[X]$, thus we see

$$F(P) = F(Q) \cdot F(x - 1) = F(Q) \cdot 0 = 0.$$

Since $(X - 1)$ is irreducible, then we know $(X - 1)$ is maximal. Since $(X - 1) \subseteq Ker\ F$, and since $(X - 1)$ is maximal, and $Ker\ F \neq \mathbb{R}[X]$, then we can conclude that $(X - 1) = Ker\ F$.

Thus by the first isomorphism theorem we know

$$\mathbb{R}[X]/(X - 1) \cong \mathbb{R}.$$

□

Claim: $F : \mathbb{R}[X] \to \mathbb{R}$ given by $F : P \mapsto P(-1)$ is a homomorphism, with $Img\ F = \mathbb{R}$ and $Ker\ F = (X + 1)$.

Proof. By the lemma we conclude that F is a homomorphism. Now we show that the $Img\ F$ is $\mathbb{R}$. Consider some element $r \in \mathbb{R}$, then let $P = r$, we compute

$$F(P) = P(-1) = r$$

Thus for any element of $r \in \mathbb{R}$ we can construct some $P \in \mathbb{R}[X]$ such that $F(P) = x$, so we conclude that the image of F is $\mathbb{R}$.

Now we prove that the $Ker\ F = (X+1)$. First we note that $(X+1)$ is irreducible, as the degree is 1. Now consider some $P \in (X+1)$. Then by the definition of an ideal, we know that $P = Q \cdot (x+1)$ for some $Q \in \mathbb{R}[X]$, thus we see

$$F(P) = F(Q) \cdot F(x+1) = F(Q) \cdot 0 = 0.$$

Since $(X+1)$ is irreducible, then we know $(X+1)$ is maximal. Since $(X+1) \subseteq Ker\ F$, and since $(X+1)$ is maximal, and $Ker\ F \neq \mathbb{R}[X]$, then we can conclude that $(X+1) = Ker\ F$.

Thus by the first isomorphism theorem we know

$$\mathbb{R}[X]/(X+1) \cong \mathbb{R}.$$

□

(b). Consider the ideals $I = (X-1)$ and $J = (X+1)$ of $\mathbb{R}[X]$.

- Prove that I and J are coprime, that is,
$$I + J = \{i + j | i \in I, j \in J\} = \mathbb{R}[X].$$
- Prove that
$$I \cap J = (X^2 - 1).$$

Element chasing is expected throughout.

Claim: I and J are coprime.

Proof. By previous homework, if there is some $i \in I$ and $j \in J$ such that $1 = i + j$ then we can conclude that I and J are coprime. So consider $i = -\frac{1}{2}(x-1)$, and $j = \frac{1}{2}(x+1)$. Then we compute

$$i + j = -\frac{1}{2}(x-1) + \frac{1}{2}(x+1) = -\frac{x}{2} + \frac{1}{2} + \frac{x}{2} + \frac{1}{2} = 1.$$

Thus we conclude that I and J are coprime. □

Claim: $I \cap J = \big(X^2 - 1\big)$.

Proof. First consider some element $P \in I \cap J$, thus $P \in I$ and $P \in J$. This would imply that $P = Q_1(x-1)$ and $P = Q_2(x+1)$ for some $Q_1, Q_2 \in \mathbb{R}[X]$. Since $(x-1)$ and $(x+1)$ are both irreducible, then it becomes clear that there must exist some $Q \in \mathbb{R}[X]$, such that $P = Q(x-1)(x+1)$. That is to say, $Q_1 = Q(x+1)$ or, $Q_2 = Q(x-1)$. Now we compute

$$P = Q(x-1)(x+1) = Q(x^2-1).$$

Thus $P \in \big(X^2 - 1\big)$.

Now we consider some element $P \in \big(X^2 - 1\big)$. Then there exists some $Q \in \mathbb{R}[X]$ such that $P = Q(x^2-1)$, we now notice that $P = Q(x-1)(x+1)$. And from here it is clear that $P \in I$ and $P \in J$, and thus $P \in I \cap J$.

Thus we conclude that $I \cap J = \big(X^2 - 1\big)$. □

(c). Combining the above with the Chinese Remainder Theorem we obtain

$$\mathbb{C}' \cong \mathbb{R}[X]/(X^2-1) \cong (\mathbb{R}[X]/(X-1)) \times (\mathbb{R}[X]/(X+1)) \cong \mathbb{R} \times \mathbb{R}.$$

In other words we have an isomorphism $F : \mathbb{C}' \to \mathbb{R} \times \mathbb{R}$. Find the explicit formula for F. That is, fill in the blank in the following.

$$F(a + b\mathbf{i}) = (\underline{\hspace{2em}}, \underline{\hspace{2em}}).$$

Explain your reasoning in full sentences.

The isomorphism is given by

$$F(a + b\mathbf{i}) = (a + b, a - b).$$

My reasoning is to first use the homomorphisms from (a), to get $F_1 : \mathbb{C}' \to \mathbb{R}[X]$, given by $F_1(a + b\mathbf{i}) = a + bx$, and $F_2 : \mathbb{R}[X] \to \mathbb{R}$ and $F_3 : \mathbb{R}[X] \to \mathbb{R}$ given by $F_2(P) = P(1)$ and $F_3(P) = P(-1)$. Then by considering $(F_2(F_1(a+b\mathbf{i})), F_3(F_1(a+b\mathbf{i})))$, that is how I constructed this isomorphism. I then checked it, by constructing the inverse by first considering some $(\alpha, \beta) \in \mathbb{R} \times \mathbb{R}$, then constructing some a, b, by noticing

$$\begin{array}{cc|c} a & b & \alpha \\ a & -b & \beta \end{array}$$

$$\begin{array}{cc|c} a & b & \alpha \\ 0 & -2b & \beta - \alpha \end{array}$$

$$\begin{array}{cc|c} a & 0 & \alpha - \frac{\alpha-\beta}{2} \\ 0 & b & \frac{\alpha-\beta}{2} \end{array}$$

Thus concluding that the inverse of F is given by

$$F(\alpha, \beta) = \alpha - \frac{\alpha - \beta}{2} + \frac{\alpha - \beta}{2}\mathbf{i}.$$

Having an inverse assured me of the validity of this isomorphism. Then I also checked that the inverse of my inverse was once again the original.