Question 1.

Find all solutions to the following complex equations.

1. $(1+i)\overline{z} = i(2+8i)$.

   Suppose that z is of the form $z = a + bi$, for $a, b \in \mathbb{R}$. Then the equation becomes

   $$(1+i)(a-bi) = i(2+8i) \implies a + b + (a-b)i = -8 + 2i.$$

   Equating coefficients, we get

   $$a + b = -8 \text{ and } a - b = 2.$$

   Solving the system of equations gives us $a = -3$ and $b = -5$, so $z = -3 - 5i$.

2. $z^3 = -8i$.

   Suppose that z is of the form $z = re^{i\theta}$, for $r, \theta \in \mathbb{R}$. Then the equation becomes

   $$r^3 e^{3i\theta} = -8i \implies r^3 e^{3i\theta} = 8e^{-i\left(\frac{\pi}{2}+2n\pi\right)}, \text{ for } n \in \mathbb{Z}$$

   Equating the coefficient and exponent gives us

   $$r^3 = 8 \text{ and } 3\theta = \frac{\pi}{2} + 2n\pi \implies r = 2,\ \theta = \frac{\pi}{6} + \frac{2n\pi}{3}.$$

   Therefore

   $$z = 2e^{i\left(\frac{\pi}{6}+\frac{2n\pi}{3}\right)} = 2\cos\left(\frac{\pi}{6} + \frac{2n\pi}{3}\right) + 2i\sin\left(\frac{\pi}{6} + \frac{2n\pi}{3}\right).$$

   We can convert this into the standard form by considering cases when $n = 0, 1, 2$, as any other value will give us a value of z that is already accounted for. Therefore

   $$z = \sqrt{3} + i, -\sqrt{3} + i, -2i$$

3. $e^{\overline{z}} = -2 + 2i$.

   Let $z = a + bi$, for $a, b \in \mathbb{R}$. Converting the right hand side of the equation into polar form, we get

   $$e^a e^{bi} = 2\sqrt{2}e^{i\left(\frac{3\pi}{4}+2n\pi\right)}, \text{ where } n \in \mathbb{Z}.$$

   We can equate real and complex parts to get that

   $$e^a = 2\sqrt{2} \text{ and } b = \frac{3\pi}{4} + 2n\pi$$

   so

   $$z = \frac{3}{2}\ln(2) + i\left(\frac{3\pi}{2} + 2n\pi\right).$$

Question 2.

Find all solutions to the following equations in $\mathbb{Z}_9$, or show that they have no solution.

(a) $[4]x + [3] = [1]$

(b) $[6]x + [3] = [5]$

(c) $x^2 = [0]$.

Proof. (a) $[4]x + [3] = [1]$

Adding $[6]$ to both sides of the equation yields

$$[4]x = [7].$$

Multiplying both sides by $[7]$, we get

$$[28]x = [49]$$

$$\implies x = [4].$$

(b) $[6]x + [3] = [5]$

This equation has no solution. To show this, we first simplify the equation to $[6]x = [2]$ by adding $[6]$ to both sides. We can substitute $x = [0], ..., [8]$ into the left hand side and see that it does not equal the right hand side:

$$[6][1] = [6],\ [6][2] = [3],\ [6][3] = [0],\ [6][4] = [6],\ [6][5] = [3],\ [6][6] = [0],$$

$$[6][7] = [6],\ [6][8] = [3],$$

As shown, the left hand side can never equal $[5]$, so the equation has no solution.

(c) $x^2 = [0]$

We can solve this by substituting every element in $\mathbb{Z}_9$ into the left hand side. We see that

$$[0]^2 = [0],\ [1]^2 = [1],\ [2]^2 = [4],\ [3]^2 = [0],\ [4]^2 = [7],$$

$$[5]^2 = [7],\ [6]^2 = [0],\ [7]^2 = [4],\ [8]^2 = [1].$$

Thus the solutions to this equation are $x = [0], [3], [6]$.

□

Question 3.

Let $\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3\}$, where we define operations $+, \cdot$ by:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i.$$

Set $1 = [1] + [0]i$ and $0 = [0] + [0]i$.

(a) Using only the definition of the operations above, and the fact that $\mathbb{Z}_3$ is a field, show that $\mathbb{Z}_3[i]$ satisfies Axioms 1-4, as well as the existence of additive inverses.

(b) Compute the multiplication table for $\mathbb{Z}_3[i]$ to verify that multiplicative inverses exist, and hence conclude that $\mathbb{Z}_3[i]$ is a field.

(c) What is the characteristic of $\mathbb{Z}_3[i]$? (See question #6 for the definition of characteristic of a field.)

Proof.
(a):
Let $a, b, c, d, p, q \in \mathbb{Z}_3$, so $z = a + bi$, $w = c + di$, and $x = p + qi$ are elements of $\mathbb{Z}_3[i]$.

To show closure under addition and multiplication, we use the closure of $\mathbb{Z}_3$ to see that $a + c \in \mathbb{Z}_3$ and $b + d \in \mathbb{Z}_3$. It follows that $z + w = (a + c) + (b + d)i \in \mathbb{Z}_3[i]$.
As well, we also have that $ac - bd, ad + bc \in \mathbb{Z}_3$, so $zw = (ac - bd) + (ad + bc)i \in \mathbb{Z}_3[i]$.

To show the commutativity of addition and multiplication, we note that $a + c = c + a$ and $b + d = d + b$, so

$$z + w = (a + c) + (b + d)i = (c + a) + (d + b)i = w + z$$

Likewise, since $ac = ca$, $bd = db$, $ad = da$, and $bc = cb$,

$$zw = (ac - bd) + (ad + bc)i = (ca - db) + (da + cb)i = wz$$

To show associativity, we again use the field properties of $\mathbb{Z}_3$ to see that

$$\begin{aligned}
(z + w) + x &= ((a + c) + (b + d)i) + p + qi \\
&= ((a + c) + p) + ((b + d) + q)i \\
&= (a + (c + p)) + (b + (d + q))i && \text{(associativity of } \mathbb{Z}_3\text{)} \\
&= a + bi + (c + p) + (d + q)i \\
&= z + (w + x)
\end{aligned}$$

Finally, showing distributivity, we have

$$\begin{aligned}
x \cdot (z + w) &= (p + qi) \cdot ((a + c) + (b + d)i) \\
&= p(a + c) - q(b + d) + (p(b + d) + q(a + c))i \\
&= pa + pc - qb - qd + (pb + pd + qa + qc)i && \text{(distributivity of } \mathbb{Z}_3) \\
&= (pa - qb) + (pc - qd) + ((pb + qa) + (pd + qc))i \\
& && \text{(associativity \& commutativity of } \mathbb{Z}_3) \\
&= (pa - qb) + (pb + qa)i + (pc - qd) + (pd + qc)i \\
&= (p + qi) \cdot (a + bi) + (p + qi) \cdot (c + di) \\
&= x \cdot z + x \cdot w
\end{aligned}$$

We also see that additive inverses exist, because for $z = a + bi \in \mathbb{Z}_3[i]$, we know that $-a$ and $-b$ exist, so if we let $-z = (-a) + (-b)i$, we see that

$$\begin{aligned}
z + (-z) &= (a + bi) + (-a + (-b)i) \\
&= (a + (-a)) + (b + (-b))i \\
&= 0 + 0i \\
&= 0
\end{aligned}$$

(b):
Below is the multiplication table for $\mathbb{Z}_3[i]$:

	$0+0i$	$1+0i$	$2+0i$	$0+1i$	$1+1i$	$2+1i$	$0+2i$	$1+2i$	$2+2i$
$0+0i$	0	0	0	0	0	0	0	0	0
$1+0i$	0	$1+0i$	$2+0i$	$0+1i$	$1+1i$	$2+1i$	$0+2i$	$1+2i$	$2+2i$
$2+0i$	0	$2+0i$	$1+0i$	$0+2i$	$2+2i$	$1+2i$	$0+1i$	$2+1i$	$1+1i$
$0+1i$	0	$0+1i$	$0+2i$	$2+0i$	$2+1i$	$2+2i$	$1+0i$	$1+1i$	$1+2i$
$1+1i$	0	$1+1i$	$2+2i$	$2+1i$	$0+2i$	$1+0i$	$1+2i$	$2+0i$	$0+1i$
$2+1i$	0	$2+1i$	$1+2i$	$2+2i$	$1+0i$	$0+2i$	$1+1i$	$0+i$	$2+0i$
$0+2i$	0	$0+2i$	$0+1i$	$1+0i$	$1+2i$	$1+1i$	$2+0i$	$2+2i$	$2+1i$
$1+2i$	0	$1+2i$	$2+1i$	$1+1i$	$2+0i$	$0+i$	$2+2i$	$0+2i$	$1+0i$
$2+2i$	0	$2+2i$	$1+1i$	$1+2i$	$0+1i$	$2+0i$	$2+1i$	$1+0i$	$0+2i$

Table 1: Multiplication table

As seen, every row and column not belonging to 0 contains $1 + 0i$, which implies that for all $z \in \mathbb{Z}_3[i] \setminus 0$, there is a multiplicative inverse z^{-1}.

(c): $\text{char}(\mathbb{Z}_3[i]) = 3$, as

$$\begin{aligned}
1 + 1 + 1 &= ([1] + [0]i) + ([1] + [0]i) + ([1] + [0]i) \\
&= ([1] + [1] + [1]) + ([0] + [0] + [0])i \\
&= [0] + [0]i \\
&= 0
\end{aligned}$$

$\square$

Question 4.

We introduce a new definition in this question:
Definition: Let $\mathbb{F}$ be a field. We say a subset $\mathbb{K} \subseteq \mathbb{F}$ is a **subfield** of $\mathbb{F}$ if $\mathbb{K}$ is also a field, using the same operations as $\mathbb{F}$.
For example: $\mathbb{Q}$ is a subfield of $\mathbb{R}$. $\mathbb{R}$ is a subfield of $\mathbb{C}$. $\mathbb{Z}_3$ is not a subfield of $\mathbb{Q}$, since $\mathbb{Z}_3$ is not a subset of $\mathbb{Q}$.

(a) Let $\mathbb{K} \subseteq \mathbb{F}$ be a subfield. Let $0_\mathbb{F}, 1_\mathbb{F}$ denote the additive and multiplicative identities in $\mathbb{F}$. Similarly, we denote by $0_\mathbb{K}, 1_\mathbb{K}$ the identities in $\mathbb{K}$. Prove that $0_\mathbb{F} = 0_\mathbb{K}$ and $1_\mathbb{F} = 1_\mathbb{K}$. (Hint: Prove that in a field, the only solution to the equation $x^2 = x$ are $x = 0, x = 1$.)

(b) Let $\mathbb{K} \subseteq \mathbb{F}$ be a subfield. Prove that for all $x \in \mathbb{K}$, we have $-x \in \mathbb{K}$, and that for all $x \in \mathbb{K} \setminus \{0\}$ we have $x^{-1} \in \mathbb{K}$. (Here $-x$ is the additive inverse of x **treated as an element of** $\mathbb{F}$ and x^{-1} is the multiplicative inverse of x **treated as an element of** $\mathbb{F}$.)

(c) Prove that a subset $\mathbb{K} \subseteq \mathbb{F}$ is a subfield if and only if the following conditions are met:

(i) $0, 1 \in \mathbb{K}$.

(ii) For all $x, y \in \mathbb{K}$, we have $x + y, x \cdot y \in \mathbb{K}$.

(iii) For all $x \in \mathbb{K}$, we have $-x \in \mathbb{K}$.

(iv) For all $x \in \mathbb{K} \setminus \{0\}$, we have $x^{-1} \in \mathbb{K}$.

(Hints: For the $\implies$ direction: this is "part c" for a reason. For the $\impliedby$ direction, you only need one or two short sentences to argue why addition and multiplication in $\mathbb{K}$ satisfy Axioms 1-3. Axioms 4 and 5 should also have fairly short proofs. If you find yourself with a very long argument, you should rethink your argument.)

Proof.
(a):
Fix $x \in \mathbb{K}$. Then because $x \in \mathbb{F}$,

$$0_\mathbb{F} + x = x = 0_\mathbb{K} + x \qquad \text{(existence of additive identity in } \mathbb{F} \text{ and } \mathbb{K})$$

$$\implies 0_\mathbb{F} = 0_\mathbb{K} \qquad \text{(by cancellation)}$$

Similarly for multiplication,

$$1_\mathbb{F} \cdot x = x = 1_\mathbb{K} \cdot x \implies 1_\mathbb{F} = 1_\mathbb{K}$$

(b):
Let $x \in \mathbb{K}$. Since $\mathbb{K}$ is a field, x has an additive inverse $-x_\mathbb{K}$. Note that $-x_\mathbb{K} \in \mathbb{F}$ as well, so $-x_\mathbb{K}$ is an inverse for x in $\mathbb{F}$. By the uniqueness of additive inverses in $\mathbb{F}$, we have that $-x_\mathbb{K} = -x$.
Similarly, x has a multiplicative inverse $x_\mathbb{K}^{-1}$ in $\mathbb{K}$, which is also an inverse of x with respect to $\mathbb{F}$. It follows by uniqueness of inverses that $x_\mathbb{K}^{-1} = x^{-1}$.

(c):

Suppose that $\mathbb{K} \subseteq \mathbb{F}$ is a subfield. We prove each point in order:

(i) By part (a), $0, 1 \in \mathbb{K}$.

(ii) This is simply the axiom of closure, which is immediate by assumption.

(iii) This is true from part (b).

(iv) This is true from part (b).

Conversely, suppose that the 4 conditions hold.
Since $\mathbb{K}$ has property (ii), it satisfies the axiom of closure.
To argue commutativity and associativity of elements in $\mathbb{K}$, notice that every element of $\mathbb{K}$ is also an element of $\mathbb{F}$, so they follow the axioms of commutativity, associativity, and distributivity of the field $\mathbb{F}$.
Existence of inverses comes directly from (iii) and (iv), and existence of identity element is exactly (i).
Since $\mathbb{K}$ satisfies all the field axioms, $\mathbb{K}$ is indeed a subfield of $\mathbb{F}$.

$\square$

Question 5.

Let $\mathbb{Q}[\sqrt{-2}] = \{a + b\sqrt{-2} | a, b \in \mathbb{Q}\}$. Prove that if $\mathbb{K}$ is a subfield of $\mathbb{C}$ and $\sqrt{-2} \in \mathbb{K}$, then $\mathbb{Q}[\sqrt{-2}] \subseteq \mathbb{K}$.

Proof. Suppose that $\mathbb{K}$ is a subfield of $\mathbb{C}$ and $\sqrt{2} \in \mathbb{K}$. Fix $z \in \mathbb{Q}[\sqrt{-2}]$. Then $z = a + b\sqrt{-2}$, for some $a, b \in \mathbb{Q}$. First, we will show that for all $c \in \mathbb{Q}$, $c \in \mathbb{K}$.

Letting $c \in \mathbb{Q}$, we can write $c = \dfrac{p}{q}$, where $p \in \mathbb{Z}$ and $q \in \mathbb{N}$. By the existence of the additive identity, we have that $1 \in \mathbb{K}$, and we can repeatedly use the closure of addition to see that

$$\underbrace{1 + ... + 1}_{q \text{ times}} = q \in \mathbb{K} \text{ and } \underbrace{1 + ... + 1}_{p \text{ times}} = p \in \mathbb{K}.$$

By the existence of inverses in $\mathbb{K}$, we know that $\dfrac{1}{q} \in \mathbb{K}$, and by closure under multiplication, we have that

$$p \cdot \frac{1}{q} = c \in \mathbb{K}$$

as needed.

This implies that $a, b \in \mathbb{K}$ as well. Since $\sqrt{-2} \in \mathbb{K}$, we use closure again to conclude that $b\sqrt{-2} \in \mathbb{K}$, and therefore $z = a + b\sqrt{-2} \in \mathbb{K}$, so $\mathbb{Q}[\sqrt{-2}] \subseteq \mathbb{K}$, proving the statement.

$\square$

Question 6.

In this exercise we introduce a new definition:
Definition: Let $\mathbb{F}$ be a field. The smallest non-negative integer n so that $\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0$ is called the characteristic of $\mathbb{F}$. If no such n exists, then we say $\mathbb{F}$ has characteristic 0.
We denote this non-negative integer by $\text{char}(\mathbb{F})$.
For example: $\mathbb{Z}_3$ has characteristic 3 because $1+1+1=0$ in $\mathbb{Z}_3$, but $1+1 \neq 0$ in $\mathbb{Z}_3$. So $n=3$ is the smallest integer so that $\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0$ in $\mathbb{Z}_3$.
However, $\mathbb{Q}$ has characteristic 0, because for any n we have $\underbrace{1+1+\cdots+1}_{n \text{ times}} = n \neq 0$ in $\mathbb{Q}$.

(a) Prove that $\text{char}(\mathbb{Z}_p) = p$.
(b) Prove that $\text{char}(\mathbb{F})$ must either be prime or 0. (Hint: For the case that $\text{char}(\mathbb{F})$ is non-zero, use contradiction.)

Proof.
(a):
This result is quite fast, as we can add $[1]$ to itself p times to check:

$$\underbrace{[1]+[1]+...+[1]}_{p \text{ times}} = [p] = [0]$$

(b):
Assume seeking contradiction that $\mathbb{F}$ is a field and $\text{char}(\mathbb{F})$ is non-zero and non-prime. We disregard the case where $\text{char}(\mathbb{F}) = 1$, because that means that $1 = 0$, which is impossible. It follows that $\text{char}(\mathbb{F})$ can be written as a product of two integers $a \cdot b$, where $1 < a, b < \text{char}(\mathbb{F})$. By definition, we see that

$$\underbrace{1+1+...+1}_{a \cdot b \text{ times}} = 0$$

Group the 1's into groups of a like so:

$$\underbrace{\underbrace{(1+...+1)}_{a \text{ times}} + ... + \underbrace{(1+...+1)}_{a \text{ times}}}_{b \text{ times}} = 0$$

Denote each term as x_a. We can repeatedly use the axiom of distributivity to see that

$$x_a \cdot \underbrace{(1+...+1)}_{b \text{ times}} = \underbrace{x_a + ... + x_a}_{b \text{ times}} = 0$$

Let $x_b = \underbrace{(1+...+1)}_{b \text{ times}}$, so

$$x_a \cdot x_b = 0$$

This means that we must have either $x_a = 0$ or $x_b = 0$. Regardless, we have found a value $p < \text{char}(\mathbb{F})$ such that repeated addition of 1 up to p times results in 0, which is a contradiction.

$\square$

Question 7.

In this question we introduce a new definition:
Definition: Let $f, g \in \mathbb{P}(\mathbb{F})$. We say that a polynomial $d \in \mathbb{P}(\mathbb{F})$ is a **greatest common divisor** of f and g if:

- d is a divisor of both f and g, and;
- for any other divisor d' of f and g, we have $\deg d \geq \deg d'$.

(a) Prove that if d is a common divisor of f and g, then for all $a \in \mathbb{F} \setminus \{0\}$, the polynomial ad is also a common divisor for f and g. Explain why this shows that there is no "unique" greatest common divisor for f and g like there is for integers.
(b) Prove that if d_1, d_2 are both greatest common divisors for f and g, then $d_1 = ad_2$ for some non-zero field element a.
(c) Prove that we can compute a greatest common divisor for f and g like we do for integers: repeatedly apply long division until the remainder is 0, then the last non-zero remainder is a greatest common divisor for f and g.
(d) Deduce from (c) that if d is a greatest common division for f and g, then we can write $d = pf + qg$ for some polynomials p, q.

Proof.
(a):
Suppose that d is a common divisor of f and g. By definition,

$$f = dp \text{ and } g = dq, \text{ for some } p, q \in \mathbb{P}(\mathbb{F}).$$

Let $a \in \mathbb{F} \setminus \{0\}$. We know that a^{-1} exists because $\mathbb{F}$ is a field. It follows that

$$\begin{aligned} f &= dp \\ &= 1 \cdot dp && \text{(additive identity)} \\ &= (a \cdot a^{-1})dp \\ &= a(a^{-1}d)p && \text{(associativity)} \\ &= a(da^{-1})p && \text{(commutativity)} \\ &= (ad)(a^{-1}p) && \text{(associativity)} \end{aligned}$$

Likewise for g,

$$\begin{aligned} g &= dq \\ &= 1 \cdot dq && \text{(additive identity)} \\ &= (a \cdot a^{-1})dq \\ &= a(a^{-1}d)q && \text{(associativity)} \\ &= a(da^{-1})q && \text{(commutativity)} \\ &= (ad)(a^{-1}q) && \text{(associativity)} \end{aligned}$$

The equations above imply that ad divides both f and g, so ad is a common divisor.

This means that if d is greatest common divisor for f and g, then if $\mathbb{F}$ contains an element $a \neq 0, 1$, then ad is distinct from d, but is also a common divisor, and since $\deg(d) = \deg(ad)$, it follows that ad is also a greatest common divisor of f and g.

(b):
Suppose for contradiction that there exists two greatest common divisors d_1, d_2 to f and g such that for all $a \in \mathbb{F} \setminus \{0\}$, $d_1 \neq ad_2$.
Let c be a greatest common divisor for d_1 and d_2, so

$$d_1 = cp_1 \text{ and } d_2 = cp_2, \text{ for some } p_1, p_2 \in \mathbb{P}(\mathbb{F}).$$

p_1 and p_2 cannot be constant, as that would contradict our assumption that d_1 is not a scalar multiple of d_2. Additionally, notice that the greatest common divisor of p_1 and p_2 is 1, because otherwise c would not be the greatest common divisor of d_1 and d_2.
Since d_1 and d_2 divides f, for some polynomials q and r,

$$f = d_1 \cdot q = d_2 \cdot r \implies cp_1q = cp_2r \implies p_1q = p_2r$$

p_2 divides p_1q, but we know that p_2 is coprime with p_1, so it must be true that p_2 divides q, so

$$q = p_1s_1, \text{ for } s_1 \in \mathbb{P}(\mathbb{F}).$$

Thus we rewrite the equation above and see that

$$f = cp_1p_2s_1$$

which means that cp_1p_2 divides f.
By an almost identical argument, cp_1p_2 also divides g, so cp_1p_2 is a common divisor of f and g. But $\deg(cp_1p_2) > \deg(d_1)$, as $d_1 = cp_1$ and $\deg(p_2) > 0$, which contradicts the fact that d_1 is a greatest common divisor.
Thus all greatest common divisors must be scalar multiples of each other.

(c):
We assume without loss of generality that $\deg(f) \geq \deg(g)$. Define a sequence of polynomials (r_n) as follows:

$$r_0 = f$$
$$r_1 = g$$

For $n > 1$, we let r_n be the polynomial such that

$$r_{n-2} = q_n r_{n-1} + r_n$$

This is well-defined, as the choices for q and r_n are unique. As well, this sequence is eventually strictly decreasing. That is, for $n > 0$, $r_n > r_{n+1}$, so we see that this sequence eventually reaches 0, say, at $n = k$.
Now, we will show with induction that for all non-negative integers $n < k$, we have that a greatest common divisor of r_0 and r_1 is also a greatest common divisor of r_n and r_{n+1}.
Let $n = 0$. It is obvious that the claim is true.

Now, suppose that a greatest common divisor of r_0 and r_1 is also a greatest common divisor of r_{n-1} and r_n, for some $n < k$. Let d be a greatest common divisor of r_0 and r_1. By our induction hypothesis, since d divides both r_{n-1} and r_n, for some $p_{n-1}, p_n \in \mathbb{P}(\mathbb{F})$, we have that

$$\begin{aligned} r_{n-1} = dp_{n-1} &\implies q_{n+1}r_n + r_{n+1} = dp_{n-1} \\ &\implies dq_{n+1}p_n + r_{n+1} = dp_{n-1} \\ &\implies r_{n+1} = d(p_{n-1} - q_{n+1}p_n), \end{aligned}$$

so d also divides r_{n+1}. To show that d is indeed a greatest common divisor of r_n and r_{n+1}, we let d' be a divisor of r_n and r_{n+1}. Then for some polynomial p'_n, p'_{n+1}, we have that

$$\begin{aligned} r_{n+1} = d'p'_{n+1} &\implies r_{n-1} - q_{n+1}r_n = d'p'_{n+1} \\ &\implies r_{n-1} - q_{n+1}d'p'_n = d'p'_{n+1} \\ &\implies r_{n-1} = d'(q_{n+1}p'_n + p'_{n+1}) \end{aligned}$$

which shows that d' also divides r_{n-1}. But this means that it is a common divisor of r_{n-1} and r_n. By definition, it must be true that $\deg(d') \leq \deg(d)$, which proves that d is indeed a greatest common divisor of r_n and r_{n+1}, thus proving our claim.
Let $n = k - 1$. Then it follows that a greatest common divisor of r_0 and r_1 is a greatest common divisor of r_{k-1} and $r_k = 0$, which must be a scalar multiple of r_{k-1}: exactly the last non-zero remainder when performing long division.

(d):
Let d be a greatest common divisor for f and g. We define the same sequence (r_n) in part (c), and say that it becomes 0 at $n = k$. Let d be a greatest common divisor of $f = r_0$ and $g = r_1$. We can now use another induction argument to show that for all $0 \leq n < k$, there exists $p_n, s_n \in \mathbb{P}(\mathbb{F})$ such that

$$d = p_n r_n + s_n r_{n+1}.$$

Let $n = k - 1$. We know from part (c) that d is a scalar multiple of r_{k-1}, so we immediately get that

$$d = ar_{k-1} + 0 = ar_{k-1} + r_k, \text{ for some } a \in \mathbb{F}.$$

Now, suppose that this holds for some n, $0 \leq n < k$. That is,

$$d = p_n r_n + s_n r_{n+1}$$

We want to show that this is the case for $n - 1$ as well. By definition of (r_n), we get that

$$d = p_n r_n + s_n(r_{n-1} - q_{n+1}r_n) = s_n r_{n+1} + (p_n - q_{n+1})r_n$$

as desired. Thus for $n = 0$, for some polynomials p_0, s_0, we get that

$$d = p_0 r_0 + s_0 r_1 = p_0 f + s_0 g$$

which was what we wanted to show.

$\square$

Question 8.

Apply the procedures in Question 7 to compute a greatest common divisor for the polynomials $f(x) = x^4 + x^2 + 1$, $g(x) = x^4 + 2x^3 + x^2 + 1 \in \mathbb{P}(\mathbb{Q})$, and express this divisor as a combination of f and g.
(In particular, you should not try to factor f, g to find the greatest common divisor, and doing so will not receive any credit.)

Proof. Applying the algorithm to f and g, we see that

$$\begin{aligned}
x^4 + x^2 + 1 &= 1 \cdot (x^4 + 2x^3 + x^2 + 1) - 2x^3 \\
x^4 + 2x^3 + x^2 + 1 &= -\left(\frac{1}{2}x + 1\right) \cdot (-2x^3) + x^2 + 1 \\
-2x^3 &= -2x \cdot (x^2 + 1) + 2x \\
x^2 + 1 &= \frac{1}{2}x \cdot (2x) + 1 \\
2x &= 2x \cdot 1 + 0
\end{aligned}$$

The last non-zero remainder is 1, so a greatest common divisor of f and g is 1. As well, we have that

$$\begin{aligned}
1 &= (x^2 + 1) - \frac{1}{2}x \cdot (2x) \\
&= (x^2 + 1) - \frac{1}{2}x \cdot (2x \cdot (x^2 + 1) - 2x^3) \\
&= \left(1 - x^2\right)(x^2 + 1) - \frac{1}{2}x \cdot (-2x^3) \\
&= \left(1 - x^2\right) \cdot \left(x^4 + 2x^3 + x^2 + 1 + \left(\frac{1}{2}x + 1\right) \cdot (-2x^3)\right) - \frac{1}{2}x \cdot (-2x^3) \\
&= \left(1 - x^2\right) \cdot (x^4 + 2x^3 + x^2 + 1) + \left(1 - x^2 - \frac{1}{2}x^3\right) \cdot (-2x^3) \\
&= \left(1 - x^2\right) \cdot g(x) + \left(1 - x^2 - \frac{1}{2}x^3\right)(f(x) - g(x)) \\
1 &= \left(1 - x^2 - \frac{1}{2}x^3\right) \cdot f(x) + \frac{1}{2}x^3 \cdot g(x)
\end{aligned}$$

as needed.

$\square$

Question 9.

Let $p \in \mathbb{P}(\mathbb{C})$ be a polynomial with real coefficients. Prove that if a is a root of p, then $\bar{a}$ is a root of p. (Hint: Write down an equation that means "a is a root of p". Conjugate this equation.)

Proof. Suppose that a is a root of p. This means that

$$p(x) = (x - a)q(x), \text{ for some polynomial } q \in \mathbb{P}(\mathbb{C})$$

Conjugating both sides, we get

$$p(\overline{x}) = (\overline{x} - \overline{a}) \cdot \overline{q}(\overline{x}), \text{ where } \overline{q} \text{ is the polynomial with the coefficients of } q \text{ but conjugated.}$$

Recall that p has real coefficients, so the only thing that can change is x. Now, we make the substitution $t = \overline{x}$, and see that

$$p(t) = (t - \overline{a}) \cdot \overline{q}(t)$$

which means that $\overline{a}$ is a root of p as needed.

$\square$

Question 10.

Using Question 9 and the Fundamental Theorem of Algebra, prove that the only irreducible polynomials over $\mathbb{R}$ are linear and quadratics with no real roots. Use this to deduce our Theorem from class (Week 2) about the factorization of real polynomials.

Proof. First, we will show that linear and quadratics with no real roots are irreducible.
In order for a linear polynomial to be irreducible, it is necessary for it to be able to be factored into two non-constant polynomials of strictly lower degree. However, this is not possible as a polynomial with degree strictly less than a linear is constant.
In the case for quadratics with no real roots, we assume seeking contradiction that it is indeed reducible. The only way to factor it is to separate it into two linear polynomials with real coefficients. However, these polynomials always have one real root, contradicting the fact that the quadratic has no real roots.
Now, suppose that $p \in \mathbb{P}(\mathbb{R})$ is neither linear nor a quadratic with no roots. By the Fundamental Theorem of Algebra, p has a complex root r. Consider the case where $r \in \mathbb{R}$, that is, when r has no imaginary part. It follows that

$$p(x) = (x - r)q(x), \text{ where } q \in \mathbb{P}(\mathbb{R}).$$

We make the quick note that the degree of q is at least 1 since the degree of p is at least 2. Therefore p is reducible.
Next, consider the case when r has a non-zero imaginary part. By the results of Question 9, $\overline{r}$ is also a root, and additionally, $r \neq \overline{r}$, so we can write

$$p(x) = (x - r)(x - \overline{r}) \cdot s(x), \text{ for } s \in \mathbb{P}(\mathbb{C})$$

We denote $r = a + bi$. We have that

$$(x - r)(x - \overline{r}) = (x - a - bi)(x - a + bi) = (x - a)^2 + (x - a)bi - (x - a)bi + b^2$$
$$= x^2 - 2ax + a^2 + b^2$$

This means that $p(x) = (x^2 - 2ax + a^2 + b^2)s(x)$. Notice that s must have real coefficients, for if not, then p will not have real coefficients. Since p can be factored into two polynomials with real coefficients, then we can conclude that it is reducible.

$\square$