(b) Find the gcd of \( f(x) = x^5 + x^4 + 2x^3 - x^2 - x - 2 \) and 
\( g(x) = x^4 + 2x^3 + 5x^2 + 4x + 4 \) over \( \mathbb{Q}[x] \).

Observe that \( f(1) = 0 \). So \( x - 1 \) is a factor of \( f(x) \).

Using synthetic division, we have

\[
\begin{array}{c|cccccc}
& 1 & 1 & 2 & -1 & -1 & 2 \\
\hline
1 & 1 & 2 & 4 & 3 & 2 & 0
\end{array}
\]

\( f(x) = (x-1)(x^4 + 2x^3 + 4x^2 + 3x + 2) \).

Let \( h(x) = x^4 + 2x^3 + 4x^2 + 3x + 2 \). Observe that \( g(x) - h(x) = x^2 + x + 2 \).

And, moreover, \( g(x) = (x^2 + x + 2)(x^2 + x + 2) \). The factors \( x^2 + x + 2 \) are irreducible over \( \mathbb{Q} \) since the roots are not real.

We find that \( h(x) = (x^2 + x + 2)(x^2 + x + 1) \), and \( x^2 + x + 1 \) is irreducible over \( \mathbb{Q} \).

Thus \( f(x) = (x-1)(x^2 + x + 1)(x^2 + x + 2) \) and \( g(x) = (x^2 + x + 2)^2 \).

The gcd of \( f(x) \) and \( g(x) \) is \( x^2 + x + 2 \). (This follows from applying the Euclidean algorithm to \( f(x) \) and \( g(x) \), but we take a different approach.)

Let \( a(x) = (x-1)(x^2 + x + 1) \) and \( b(x) = x^2 + x + 2 \).

Use the Euclidean algorithm on \( a(x) \) and \( b(x) \).

\[
a(x) = (x-1)(x^2 + x + 1) + (x-1) - (x-1) = (x-1)(x^2 + x + 2) - (x-1)
\]

\[
b(x) = (x+2)(x-1) + 4
\]

\[
\implies 4 = b(x) \overline{a}(x+2)(x-1) = b(x) - (x+2)(x-1) = b(x) - (x-1) - (x+2) = (x+2) b(x) + (x+2) a(x)
\]

\[
= -(x^2 + x - 3) b(x) + (x+2) a(x)
\]

\[
\implies 1 = -\frac{1}{4}(x^2 + x - 3) b(x) + (x+2) a(x) \implies (a(x), b(x)) = 1
\]

\[
\implies (x^2 + x + 2) = -\frac{1}{4}(x^2 + x - 3) g(x) + (x+2) f(x)
\]

\[
(f(x), g(x)) = x^2 + x + 2 \quad \text{since} \quad x^2 + x + 2 \quad \text{is a common}
\]

\[
\text{divisor of} \quad f(x) \quad \text{and} \quad g(x) \quad \text{and} \quad \text{the linear combination shows that any other common divisor is also a divisor of} \quad x^2 + x + 2.
\]
But $x^2 + x + 2$ is irreducible, so (up to units), the only common divisors of $f(x)$ and $g(x)$ are 1 and $x^2 + x + 2$.

\[ f(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5 \]
\[ g(x) = 3x^3 + 5x^2 + 6x \quad \text{in } \mathbb{Z}_7[x] \]

It is helpful to build a multiplication table in $\mathbb{Z}_7$:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

\[ g(x) \begin{array}{c|c}
   6x & \hline
   4x^4 + 2x^3 + 6x^2 + 4x + 5
\end{array} - \frac{(4x^4 + 2x^3 + x^2)}{5x^2 + 4x + 5} \]

So, $f(x) = 6x \cdot g(x) + (5x^2 + 4x + 5)$

\[ 5x^2 + 4x + 5 \quad \overset{2x+5}{\overline{3x^3 + 5x^2 + 6x + 0}} - (3x^3 + x^2 + 3x) \]
\[ \overset{4x^2 + 3x}{\overline{-4x^2 + 6x + 4}} \quad 4x + 3 \]

So, $g(x) = (2x+5)(5x^2 + 4x + 5) + (4x + 3)$

\[ 4x + 3 \quad \overset{3x + 4}{\overline{5x^2 + 4x + 5}} - (5x^2 + 2x) \]
\[ \overset{2x + 5}{\overline{-2x + 5}} \quad 0 \]

So, $5x^2 + 4x + 5 = (3x+4)(4x + 3) + 0$.

The last nonzero remainder was $(4x + 3)$. Multiply by 2 to get a monic polynomial $2(4x + 3) = (x + 6) = (x - 1)$

So, $\gcd(f(x), g(x)) = x + 6$.

Working backwards, we have

\[ \begin{align*}
(4x + 3) &= g(x) - (2x+5)(5x^2 + 4x + 5) \\
&= g(x) - (2x+5)(f(x) - 6x \cdot g(x)) = -(2x+5)f(x) + \frac{6x(2x^2+5)}{g(x)}
\end{align*} \]
\[(5x+2) f(x) + (5x^2+2x+1) \cdot g(x)\]

Multiplying by 2, we have

\[(x+6) = (3x+4) f(x) + (3x^2+4x+2) g(x)\]

\[
\begin{align*}
(f) \quad & f(x) = x^4 + x + 1, \quad g(x) = x^2 + x + 1, \quad \text{in } \mathbb{Z}_2[x] \\
& \frac{x^2 + x}{x^2 + x + 1} \quad \frac{x^4 + 0 + 0 + x + 1}{x^4 + x^3 + x^2} \quad \frac{x^3 + x^2 + x + 1}{x^3 + x^2 + x} \\
\hline
\end{align*}
\]

So,

\[f(x) = (x^2 + x) g(x) + 1\]

\[\Rightarrow 1 = f(x) + (x^2 + x) g(x)\]

Hence,

\[\text{gcd}(f(x), g(x)) = 1\]

#2 Let \( R \) be an integral domain. Prove that the relation \( a \sim b \) if \( a \) is associate to \( b \) is an equivalence relation.

**Proof:**

**Reflexive:** \( \exists 1 \in R \). So if \( a \in R \),

\[ a = 1 \cdot a \Rightarrow a \sim a \quad (1 \text{ is a unit})\]

**Symmetric:** If \( a \sim b \), then \( \exists \text{ a unit } u \in R \) such that \( a = u \cdot b \). Multiply by \( u^{-1} \): \( u^{-1} \cdot a = b \). Therefore, \( b \sim a \).

**Transitive:** If \( a \sim b \) and \( b \sim c \), then \( \exists \text{ units } u, v \in R \) such that \( a = u \cdot b \) and \( b = v \cdot c \). \( \Rightarrow a = u (v \cdot c) \Rightarrow a \sim (uv) \cdot c \). The element \( uv \) is a unit (with inverse \( v^{-1} u^{-1} \)).

So \( a \sim c \). Hence \( \sim \) is an equivalence relation.
#3 Sobre ejercicio #16 in §4.2

Let \( f(x), g(x), h(x) \in \mathbb{F}[x] \) and suppose \( (f(x), g(x)) = 1 \).

Prove that \( (f(x)h(x), g(x)) = (h(x), g(x)) \).

**Proof:** If \( f(x) = 0 \), then \( (0, g(x)) = 1 \) \( \Rightarrow \) \( g(x) \) is a unit. \( \Rightarrow \) \( (h(x), g(x)) = 1 \) and \( (f(x)h(x), g(x)) = (0, g(x)) = 1 \).

If \( g(x) = 0 \), then \( (f(x)g(x)) = 1 \) \( \Rightarrow \) \( f(x) \) is a unit.

\[ \Rightarrow \quad (f(x)h(x), g(x)) = (h(x), g(x)) \quad (\gcd \text{ is unaffected by units}) \]

If \( h(x) = 0 \), then \( (0, g(x)) = (0, g(x)) \).

So, we may assume that \( f(x), g(x), \) and \( h(x) \) are non-zero.

If \( d(x) | h(x) \) and \( d(x) | g(x) \), then \( d(x) | f(x)h(x) \).

\[ \Rightarrow \quad d(x) \text{ is a common divisor of } f(x)h(x) \text{ and } g(x). \]

\[ \therefore \quad d(x) | (f(x)h(x), g(x)) \quad (\text{part (ii) of Corollary 4.6}) \]

Setting \( d(x) = (f(x), g(x)) \), we have \( (f(x), g(x)) | (f(x)h(x), g(x)) \).

We now show the converse: that \( (f(x)h(x), g(x)) \) divides \( (f(x), g(x)) \).

If \( d(x) | f(x)h(x) \) and \( d(x) | g(x) \), then \( d(x) | f(x) \) since \( (f(x), g(x)) = 1 \) \( \Rightarrow \) \( (f(x), d(x)) = 1 \) and we can apply Theorem 4.7.

\( \star \)

(To see \( \star \), observe that if \( a(x) | f(x) \) and \( a(x) | f(x) \), then \( a(x) | d(x) \).

\[ a(x) | (f(x), g(x)) = 1 \quad \Rightarrow \quad a(x) \text{ is a unit}. \]

Taking \( d(x) = (f(x)h(x), g(x)) \), we have that \( (f(x)h(x), g(x)) \) is a common divisor of \( (f(x), g(x)) \). Hence (by part (ii) of Corollary 4.6),

\[ (f(x)h(x), g(x)) | (f(x), g(x)). \]

Now if two polynomials \( a(x), b(x) \)

divide each other, then they are associates: \( a(x) = b(x) \cdot c(x) \) and \( b(x) = a(x) \cdot d(x) \) \( \Rightarrow \) \( \deg a(x) = \deg b(x) \Rightarrow \deg c(x) = 0 \)

\( \Rightarrow \quad a(x) = b(x) \cdot u \), \( \forall u \), for a unit \( u \).

Thus, \( (f(x), g(x)) = (f(x)h(x), g(x)) \cdot u \) for some unit \( u \). Since \( \gcd \) is monic \( \Rightarrow u = 1 \). \( \star \)
#6 in 4.3 Show that \( x^2+1 \) is irreducible in \( \mathbb{Q}[x] \).

**Proof:** If it were reducible, then \( x^2+1 = (ax+b)(cx+d) \),

\[ \Rightarrow ac = 1 \text{ and } bd = 1 \Rightarrow ad + bc = 0 \]

So, \( a, c, b, d \) are non-zero \& units.

\[ cd(ad + bc) = (ac)d^2 + (bd)c^2 = 0 \]

\[ = 1 \cdot a^2 + 1 \cdot c^2 = 0 \Rightarrow c^2 + d^2 = 0 \]

\[ \Rightarrow c = d = 0 \Rightarrow 0 = 1 \text{ in } \mathbb{C}! \] Therefore, this is impossible.

---

#10 in 4.3

@ Is \( x^2 - 3 \) irreducible in \( \mathbb{Q}(x) \)? Yes.

In \( \mathbb{R}[x] \) we have \( (x - \sqrt{3})(x + \sqrt{3}) = 0 \).

\[ (x^2 - 3) = (ax+b)(cx+d), \text{ then } ac = 1, \ bd = 0 - 3 \]

\[ \text{and } ad + bc = 0 \Rightarrow acx^2 + bdx = ad^2 + bc = 0 \]

\[ \Rightarrow a^2d^2 + 3ac = (ad)^2 + \frac{3}{4} \Rightarrow (ad)^2 = \frac{9}{4} \Rightarrow c! \]

Thus, \( (x^2 - 3) \) is irreducible over \( \mathbb{Q}(x) \).

(b/c \( \sqrt{3} \notin \mathbb{Q} \))

@ Is \( x^2 + x - 2 \) irreducible in \( \mathbb{Z}_3[x] \)? Yes.

\( (x + 2)(x - 1) \) in \( \mathbb{Z}_7[x] \) \( \Rightarrow \) Yes.

Valid in both.

---

#12 in 4.3

Express \( x^4 - 4 \) as a product of irreducibles in \( \mathbb{Q}[x] \), \( \mathbb{R}[x] \), and in \( \mathbb{C}[x] \).

In \( \mathbb{Q}[x] \) : \( (x^2 - 2)(x^2 + 2) \)

In \( \mathbb{R}[x] \) : \( (x - \sqrt{2})(x + \sqrt{2})(x^2 + 2) \)

In \( \mathbb{C}[x] \) : \( (x - \sqrt{2})(x + \sqrt{2})(x - i\sqrt{2})(x + i\sqrt{2}) \)

---

#22 (a) Show that \( x^3 + a \) is reducible in \( \mathbb{Z}_3[x] \).

**Proof:** If \( x^3 + a \) were irreducible, then \( x + a \) would have a root.

But \( x + a = 0 \Rightarrow x = -a \Rightarrow a \equiv 0 \mod 3 \).

\( a^3 = 1 \) for each \( a \neq 0 \) in \( \mathbb{Z}_3 \),

\( x^3 + a = a^{-1}((ax)^3 + 1) = a^{-1}(ax + 1)((ax)^2 - (ax) + 1) \).

(b) Show that \( x^5 + a \) is reducible in \( \mathbb{Z}_5[x] \).

If \( a = 0 \), \( x^5 = x \cdot x \cdot x \cdot x \cdot x \).

Otherwise, since \( a \neq 0 \) and \( a^5 = 1 \) (check), \( x^5 + a = a^{-1}(ax + 1)((ax)^4 - (ax)^2 + (ax) - 1) \).

Otherwise, since \( a \neq 0 \) and \( a^5 = 1 \) (check), \( x^5 + a = a^{-1}(ax + 1)((ax)^4 - (ax)^2 + (ax) - 1) \).