1) Compute the GCD of the polynomials $x^3 - x^2 - x + 1, x^3 - 3x^2 + 3x - 1 \in \mathbb{Q}[x]$. What polynomial generates the ideal $(x^3 - x^2 - x + 1, x^3 - 3x^2 + 3x - 1) \subset \mathbb{Q}[x]$ and what polynomial generates the ideal $(x^3 - x^2 - x + 1) \cap (x^3 - 3x^2 + 3x - 1) \subset \mathbb{Q}[x]$.

Proof. $x^3 - x^2 - x + 1 = (x^3 - 3x^2 + 3x - 1) + (2x^2 - 4x + 2)$ and $x^3 - 3x^2 + 3x - 1 = \frac{1}{2}(x-1)(2x^2 - 4x + 2) + 0$. Therefore the GCD is $x^2 - 2x + 1 = (x-1)^2$ and we have $(x^3 - x^2 - x + 1, x^3 - 3x^2 + 3x - 1) = (x^2 - 2x + 1)$. Since $x^3 - x^2 - x + 1 = (x-1)^2(x+1)$ and $(x^3 - 3x^2 + 3x - 1) = (x-1)^3$, we have $(x^3 - x^2 - x + 1) \cap (x^3 - 3x^2 + 3x - 1) = (x+1)(x-1)^3$. \[\square\]

2) Show that $f(x) = x^3 + 2x + 2$ is irreducible in $\mathbb{Q}[x]$ and factor $f(x)$ in $\mathbb{Z}_7[x]$.

Proof. $f(x) = x^3 + 2x + 2$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein’s Criterion with $p = 2$. (Alternatively you can argue that if the only possible roots of $f(x)$ are $\pm1$ and $\pm2$ and hence $f(x)$ has no roots in $\mathbb{Z}$. By Gauss’ Lemma, $f(x)$ has no linear factors and hence $f(x)$ is irreducible.)

Note that $f(2) = 8 + 4 + 2 = 14 = 0 \in \mathbb{Z}_7$. So $x^3 + 6x^2 + 14x + 14 = (x-2)(x^2 + 2x + 6) = (x-2)(x-2)(x-3)$ in $\mathbb{Z}_7[x]$. \[\square\]

3) Let $R$ be a commutative ring and $I \subset R$ an ideal. Show that $I[x]$ is an ideal of $R[x]$ and $R[x]/I[x] \cong (R/I)[x]$.

Proof. Define a homomorphism $\phi : R[x] \rightarrow R/I[x]$ by $\phi(\sum a_ix^i) = \sum \psi(a_i)x^i$ where $\psi : R \rightarrow R/I$ is the natural homomorphism that sends $x \in R$ to $x + I$.

We first check that $\phi$ is a homomorphism:

$$
\phi(\sum a_ix^i + \sum b_ix^i) = \phi(\sum (a_i + b_i)x^i) = \sum \psi(a_i + b_i)x^i = \sum \psi(a_i)x^i + \sum \psi(b_i)x^i = \phi(\sum a_ix^i) + \phi(\sum b_ix^i)
$$

$$
\phi((\sum a_ix^i) \cdot (\sum b_ix^i)) = \phi(\sum (\sum a_i b_j)x^i) = \sum \psi(\sum a_i b_j)x^i = \sum_i \sum_{0 \leq j \leq i} \psi(a_i)x^i \cdot \psi(b_j)x^i = \phi(\sum a_ix^i) \cdot \phi(\sum b_ix^i).
$$

Now we compute Ker$(\phi) = \{ \sum a_ix^i \in R[x] \mid \phi(\sum a_ix^i) = 0 \}$. Since $\phi(\sum a_ix^i) = \sum \psi(a_i)x^i$, then $\phi(\sum a_ix^i) = 0$ means that $\psi(a_i) = 0$ for all $i$, i.e. $a_i \in I$ for all $i$. Therefore Ker$(\phi) = I[x]$. In particular
$I[x]$ is an ideal and by the First Homomorphism Theorem $(R/I)[x] \cong R[x]/I[x]$.

4) Let $R$ be a commutative ring with 1. Show that $R$ is a field if and only if $(0)$ is a maximal ideal.

Proof. If $R$ is a field and $M \neq (0)$ is an ideal, then let $m \in M - 0$. Since $R$ is a field, we have $m^{-1} \in R$ and so $1 = m^{-1}m \in M$. Thus $M = R$ and hence $(0)$ is a maximal ideal.

Conversely, if $(0)$ is a maximal ideal, let $m \in R - 0$ so that $(m) \supset (0)$. As $(0)$ is maximal, $(m) = R$ and so $1 \in (m) = \{m \cdot r \mid r \in R\}$. Thus $1 = mr$ for some $r \in R$, i.e. $m$ is invertible. We have shown that every non-zero element of $R$ is invertible and hence $R$ is a field.

5) Prove that $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$.

Proof. Define a map $\phi : R[x] \to \mathbb{C}$ via $\phi(f(x)) = f(i)$. We have $\phi(f(x)) + \phi(g(x)) = f(i) + g(i) = (f + g)(i) = \phi((f + g)(x))$ and $\phi(f(x)) \cdot \phi(g(x)) = f(i) \cdot g(i) = (f \cdot g)(i) = \phi((f \cdot g)(x))$ and hence $\phi$ is a homomorphism.

By the First Homomorphism Theorem it is enough to show that $\text{Ker}(\phi) = (x^2 + 1)$. Since $i^2 + 1 = 0$, we have $\text{Ker}(\phi) \supseteq (x^2 + 1)$. Since $x^2 + 1$ is irreducible, $(x^2 + 1)$ is maximal. Since $\text{Ker}(\phi)$ is a proper ideal of $\mathbb{R}[x]$, we have $\text{Ker}(\phi) = (x^2 + 1)$.

6) Is $\mathbb{Z}_{13}[x]/(x^2 + 1)$ isomorphic to a field with 169 elements or to the ring $\mathbb{Z}_{13} \oplus \mathbb{Z}_{13}$?

Is $\mathbb{Z}_7[x]/(x^2 + 1)$ isomorphic to a field with 49 elements or to $\mathbb{Z}_7 \oplus \mathbb{Z}_7$.

Proof. We have $x^2 + 1 = (x - 5)(x + 5)$ is $\mathbb{Z}_{13}[x]$ and so $\mathbb{Z}_{13}[x]/(x^2 + 1) \cong \mathbb{Z}_{13}[x]/(x - 5) \oplus \mathbb{Z}_{13}[x]/(x + 5) \cong \mathbb{Z}_{13} \oplus \mathbb{Z}_{13}$.

Since $x^2 + 1$ has no roots in $\mathbb{Z}_7$, it is irreducible in $\mathbb{Z}_7[x]$ and hence $\mathbb{Z}_7[x]/(x^2 + 1)$ is a field with 49 elements.