Let $K$ be a field. Recall the Euclidean division of polynomials in $K[X]$ : given $A, B \in K[X]$ with $B \neq 0$, there is a unique pair $(Q, R) \in K[X]^2$ satisfying
\[ A = BQ + R \]
and $\deg(R) < \deg(B)$ (recall that the zero polynomial has degree $-\infty$ so it is possible that $R$ is zero).

**Problem 1.** (1) Let $R$ be a subring of $\mathbb{C}$ containing $\mathbb{Q}$. Check that $R$ is also a $\mathbb{Q}$-vector space. (In fact $R$ is called a $\mathbb{Q}$-algebra).

(2) Suppose that $R$ as above is finite dimensional over $\mathbb{Q}$. Show that $R$ is a field. (You may consider the multiplication map $m_\alpha : R \rightarrow R, x \mapsto \alpha x$ for $\alpha \in R$). (This should remind you of the proof of "a finite integral domain is a field").

(3) Let $\alpha \in \mathbb{C}$ such that there exists a nonzero polynomial $P \in \mathbb{Q}[X]$ satisfying $P(\alpha) = 0$. Show that $\mathbb{Q}[\alpha]$ defined in Problem set 2 as the image of the morphism of rings $\mathbb{Q}[X] \rightarrow \mathbb{C}, P \mapsto P(\alpha)$ is a field.

(4) Show that the kernel of the map $\mathbb{Q}[X] \rightarrow \mathbb{Q}[\alpha], P \mapsto P(\alpha)$ is generated by an irreducible polynomial $P_\alpha$ in $\mathbb{Q}[X]$. Compare the degree of $P_\alpha$ and the dimension of $\mathbb{Q}[\alpha]$ as a vector space.

(5) Let $\alpha = \sqrt{2} - \sqrt{2}$. What is $P_\alpha$? (You may apply Eisenstein’s criterion from Problem set 2).

What is the inverse of $\alpha$ in $\mathbb{Q}[\alpha]$?

What is the inverse of $1 + \alpha + \alpha^2$ in $\mathbb{Q}[\alpha]$? (You may use the Euclidean algorithm between $P_\alpha$ and $1 + X + X^2$).

**Problem 2.** Show that there exists an irreducible polynomial of degree 3 in $\mathbb{F}_2[X]$. Give an example of field of cardinality 8. (The ideas in the previous problem could be helpful...)

If $A, B \in \mathbb{Z}[X]$ we may write the division of $A$ by $B$ in $\mathbb{Q}[X]$ but the quotient and the remainder do not necessarily lie in $\mathbb{Z}[X]$ (try with examples). However, we admit the following (it is not too difficult but a bit tedious to prove) : if $A, B \in \mathbb{Z}[X]$ and $B$ is a monic polynomial, then the quotient $Q$ and the remainder $R$ of the Euclidean division of $A$ by $B$ in $\mathbb{Q}[X]$ actually lie in $\mathbb{Z}[X]$.

**Problem 3.** (1) Let $P \in K[X]$ and $z \in K$. What is the remainder of the Euclidean division of $P$ by $X - z$?

(2) Let $A \in \mathbb{R}[X]$, and $B \in \mathbb{R}[X]$ a monic irreductible polynomial of degree 2. What is the remainder of the Euclidean division of $A$ by $B$?

(3) Write the division of $X^3 + 2X^2 + 5X + 1$ by $X^2 + 4X + 1$ in $\mathbb{Q}[X]$ (and check that it actually happens in $\mathbb{Z}[X]$).

(4) What is the Euclidean division of $X^2 + X + 1$ by $2X + 1$ in $\mathbb{Q}[X]$. Does it happen in $\mathbb{Z}[X]$?
Problem 4. Why do you know without any computation that the following system has a solution?
\[
\begin{aligned}
x &\equiv 4 \mod 18 \\
x &\equiv 8 \mod 17
\end{aligned}
\]

Problem 5. Let \((x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in \mathbb{R}^n\) and suppose that all \(x_i\)'s are pairwise distinct. Why is there a unique polynomial \(P \in \mathbb{R}[X]\) of degree < \(n\) such that \(P(x_i) = y_i\) for all \(i\)?

Problem 6. (bonus)
Problem 33 of Section 7.4 except for question (d).