Solutions #7

1. For each of the following polynomials determine whether it is irreducible or not:
   
   (a) \( X^2 - 3 \) in \( \mathbb{R}[X] \);
   
   (b) \( X^2 - 3 \) in \( \mathbb{C}[X] \);
   
   (c) \( X^2 + X - 2 \) in \( \mathbb{Z}_3[X] \);
   
   (d) \( X^2 + X - 2 \) in \( \mathbb{Z}_7[X] \).

   **Solution.**
   
   (a) Since \( X^2 - 3 = (X - \sqrt{3})(X + \sqrt{3}) \), we conclude that \( X^2 - 3 \) is reducible in \( \mathbb{R}[X] \).
   
   (b) The factorization \( X^2 - 3 = (X - \sqrt{3})(X + \sqrt{3}) \) holds in \( \mathbb{C}[X] \) as well, so \( X^2 - 3 \) is reducible in \( \mathbb{C}[X] \).
   
   (c) Since \( 1 \in \mathbb{Z}_3 \) is a root of \( X^2 + X - 2 \), we conclude that \( X^2 + X - 2 \) is reducible in \( \mathbb{Z}_3[X] \).
   
   (d) The same argument as above works: \( 1 \in \mathbb{Z}_7 \) is a root of \( X^2 + X - 2 \) and thus \( X^2 + X - 2 \) is reducible in \( \mathbb{Z}_7[X] \).

2. Factor into irreducibles:
   
   (a) \( X^2 - 7 \) in \( \mathbb{R}[X] \);
   
   (b) \( X^2 - 7 \) in \( \mathbb{Q}[X] \);
   
   (c) \( 2X^3 + X^2 + 2X + 2 \) in \( \mathbb{Z}_5[X] \);
   
   (d) \( X^4 + X^2 + 1 \) in \( \mathbb{Z}_3[X] \).

   **Solution.**

   (a) In \( \mathbb{R}[X] \) we have \( X^2 - 7 = (X - \sqrt{7})(X + \sqrt{7}) \).
   
   (b) \( X^2 - 7 \) is irreducible in \( \mathbb{Q}[X] \). One way to check this is to verify that it has no rational roots by excluding all possible roots \( \frac{r}{s} \). We know that \( r \) must divide 7 and \( s \) must divide 1. Hence the possible roots of \( X^2 - 7 \) are \( \pm 1, \pm 7 \) and a direct verification shows that none of them is a root. Finally, since \( X^2 - 7 \in \mathbb{Q}[X] \) is of degree 2 with no roots, it is irreducible.

   We can also use part (a) above to argue that \( f = X^2 - 7 \) is irreducible in \( \mathbb{Q}[X] \). Indeed, if \( f = gh \) in \( \mathbb{Q}[X] \), then \( f, g, h \in \mathbb{R}[X] \) and, hence, \( f = gh \) in \( \mathbb{R}[X] \). Assuming \( \operatorname{deg} g, \operatorname{deg} h < \operatorname{deg} f = 2 \), we conclude that \( f = gh \) is a decomposition of \( f \) into irreducibles in \( \mathbb{R}[X] \) (Why?). This contradicts (a) and the uniqueness of the factorization of \( f \) into irreducibles.

   (c) A direct verification shows that \( 2X^3 + X^2 + 2X + 2 \) has no roots in \( \mathbb{Z}_5 \) which means that \( 2X^3 + X^2 + 2X + 2 \) is irreducible in \( \mathbb{Z}_5[X] \).
   
   (d) \( X^4 + X^2 + 1 = (X + 1)^2(X + 2)^2 \) in \( \mathbb{Z}_3[X] \).
3.

(a) Let \( \varphi : \mathbb{C} \to \mathbb{C} \) be an isomorphism such that, for every \( a \in \mathbb{Q} \), \( \varphi(a) = a \). Let \( z \in \mathbb{C} \) be a root of \( f(X) \in \mathbb{Q}[X] \). Prove that \( \varphi(z) \) is also a root of \( f(X) \).

(b) Let \( \Phi : \mathbb{F}[X] \to \mathbb{F}[X] \) be an isomorphism such that \( \Phi(a) = a \) for every \( a \in \mathbb{F} \). Prove that if \( f \in \mathbb{F}[X] \) is irreducible, then only if \( \Phi(f) \) is also irreducible. Give an example of an isomorphism \( \Phi : \mathbb{F}[X] \to \mathbb{F}[X] \) such that \( \Phi(a) = a \) for every \( a \in \mathbb{F} \) but \( \Phi \) is not the identity.

\textbf{Solution.} (a) Let \( f = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n \), where \( a_i \in \mathbb{Q} \) and let \( z \in \mathbb{C} \) be a root of \( f \). Taking into account that \( \varphi(a_i) = a_i \), since \( a_i \in \mathbb{Q} \), we calculate:

\[
\begin{align*}
\varphi(f(z)) &= \varphi(a_0z^n + a_1z^{n-1} + \ldots + a_{n-1}z + a_n) \\
&= \varphi(a_0z^n) + \varphi(a_1z^{n-1}) + \ldots + \varphi(a_{n-1}z) + \varphi(a_n) \\
&= \varphi(a_0)\varphi(z^n) + \varphi(a_1)\varphi(z^{n-1}) + \ldots + \varphi(a_{n-1})\varphi(z) + \varphi(a_n) \\
&= a_0\varphi(z^n) + a_1\varphi(z)^{n-1} + \ldots + a_{n-1}\varphi(z) + a_n = f(\varphi(z)).
\end{align*}
\]

On the other hand, \( \varphi(f(z)) = \varphi(0) = 0 \), i.e., \( \varphi(z) \) is also a root of \( f(X) \).

(b) It is sufficient to prove that \( f \in \mathbb{F}[X] \) is reducible if and only if \( \Phi(f) \) is irreducible. This will imply that \( f \in \mathbb{F}[X] \) is irreducible if and only if \( \Phi(f) \) is irreducible. Indeed, every polynomial is exactly one of the following three: irreducible, reducible, or a constant. Since \( \Phi \) preserves all constants, proving that \( f \in \mathbb{F}[X] \) is irreducible if and only if \( \Phi(f) \) is reducible is equivalent to proving that \( f \in \mathbb{F}[X] \) is irreducible if and only if \( \Phi(f) \) is irreducible.

Assume that \( f \) is reducible. Then \( f = gh \) with \( 0 < \deg g, \deg h < \deg f \). Then we have \( \Phi(f) = \Phi(g)\Phi(h) \) and \( \deg \Phi(g) \), \( \deg \Phi(h) > 0 \) because \( \Phi \) is an isomorphism and \( \Phi \) fixes all constant polynomials. More precisely, the assumption that \( \Phi(g) = c \) is a constant implies that \( \Phi \) is not injective because \( \Phi(c) = \Phi(g) = c \). The factorization \( \Phi(f) = \Phi(g)\Phi(h) \) with \( \deg \Phi(g) \), \( \deg \Phi(h) > 0 \) proves that \( \Phi(f) \) is reducible.

Conversely, assume that \( \Phi(f) \) is reducible. Since \( \Phi \) is a bijection, it has an inverse map \( \Psi \). One checks immediately that \( \Psi \) also is a homomorphism and hence it is an isomorphism (Verify!). Then, if \( \Phi(f) \) is reducible, by the above, \( f = \Psi(\Phi(f)) \) is also reducible.

Set \( \Phi(f(X)) := f(X + 1) \). Then, clearly \( \Phi(a) = a \) for every \( a \in \mathbb{F} \). In particular, \( \Phi(1_{\mathbb{F}[X]}) = \Phi(1_{\mathbb{F}}) = 1_{\mathbb{F}} = 1_{\mathbb{F}[X]} \). Also,

\[
\Phi(f + g) = (f + g)(X + 1) = f(X + 1) + g(X + 1) = \Phi(f) + \Phi(g)
\]

and

\[
\Phi(fg) = (fg)(X + 1) = f(X + 1)g(X + 1) = \Phi(f)\Phi(g).
\]

This proves that \( \Phi \) is a homomorphism. It is a bijection since its inverse map is given by \( \Psi(f(X)) = f(X - 1) \) (Verify!). Clearly, \( \Phi(X) = X + 1 \), i.e., \( \Phi \) is not the identity of \( \mathbb{F}[X] \). \( \Box \)