A. Exercise 37 on page 220

1. Let be $p, q \in \mathbb{Z}[X]$. (Let's assume that degree(p)≥degree(q))

   - $\overline{\sigma_m}(1) = 1$
   - Proof that $\overline{\sigma_m}(p+q) = \overline{\sigma_m}(p) + \overline{\sigma_m}(q)$:

   $$\begin{aligned}
   \overline{\sigma_m}(p+q) &= \overline{\sigma_m}(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 + b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0) \\
   &= \overline{\sigma_m}(a_n x^n + \cdots + (a_m + b_m)x^m + (a_{m-1} + b_{m-1})x^{m-1} + \cdots + a_0 + b_0) \\
   &= \sigma_m(a_n)x^n + \cdots + \sigma_m(a_m + b_m)x^m + \sigma_m(a_{m-1} + b_{m-1})x^{m-1} \\
   &+ \cdots + \sigma_m(a_0 + b_0) \\
   &= \sigma_m(a_n)x^n + \cdots + \sigma_m(a_m)x^m + \sigma_m(b_m)x^m + \sigma_m(a_{m-1})x^{m-1} \\
   &+ \sigma_m(b_{m-1})x^{m-1} + \cdots + \sigma_m(a_0) + \sigma_m(b_0) \text{ } (\sigma_m \textbf{ is a ring homomorphism}) \\
   &= \sigma_m(a_n)x^n + \cdots + \sigma_m(a_m)x^m + \sigma_m(a_{m-1})x^{m-1} + \cdots + \sigma_m(a_0)\sigma_m(b_m)x^m \\
   &+ \sigma_m(b_{m-1})x^{m-1} + \cdots + \sigma_m(b_0) \\
   &= \overline{\sigma_m}(p) + \overline{\sigma_m}(q)
   \end{aligned}$$

   - Proof that $\overline{\sigma_m}(p \cdot q) = \overline{\sigma_m}(p) \cdot \overline{\sigma_m}(q)$:

   $$\begin{aligned}
   \overline{\sigma_m}(p+q) &= \overline{\sigma_m}((a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0)(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0)) \\
   &= \overline{\sigma_m}(a_n b_m x^{n+m} + (a_{n-1}b_m + a_n b_{m-1})x^{n+m-1} + \cdots + a_0 b_0) \\
   &= \sigma_m(a_n b_m)x^{n+m} + \sigma_m(a_{n-1}b_m + a_n b_{m-1})x^{n+m-1} + \cdots + \sigma_m(a_0 b_0) \\
   &= \sigma_m(a_n)\sigma_m(b_m)x^{n+m} + \sigma_m(a_{n-1})\sigma_m(b_m)x^{n+m-1} + \sigma_m(a_n)\sigma_m(b_{m-1})x^{n+m-1} \\
   &+ \cdots + \sigma_m(a_0)\sigma_m(b_0) \text{ } (\sigma_m \textbf{ is a ring homomorphism}) \\
   &= (\sigma_m(a_n)x^n + \sigma_m(a_{n-1})x^{n-1} + \cdots + \sigma_m(a_0))(\sigma_m(b_n)x^n + \sigma_m(b_{n-1})x^{n-1} \\
   &+ \cdots + \sigma_m(b_0)) \\
   &= \overline{\sigma_m}(p)\overline{\sigma_m}(q)
   \end{aligned}$$

   Therefore $\overline{\sigma_m}$ is a ring homomorphism.

2. Let be $f(x) \in \mathbb{Z}[\mathbb{X}]$.
   We know that $deg(f) = deg(\overline{\sigma_m}(f(x))) = n$ and $\overline{\sigma_m}(f(x))$ is irreducible in $\mathbb{Z}_m$.
   Suppose that f(x) is reducible in $\mathbb{Q}[X]$.
   We would have $f(x) = g(x)h(x)$.
   $\overline{\sigma_m}(f(x)) = \overline{\sigma_m}(g(x))\overline{\sigma_m}(h(x))$.
   As $\overline{\sigma_m}(f(x))$ is irreducible, one of the two polynomials is a constant. (Assume it's $\overline{\sigma_m}(g(x))$).
   As $deg(\overline{\sigma_m}(f(x))) = n$ then $deg(\overline{\sigma_m}(h(x))) = n$.
   And therefore $deg(h(x)) \geq n$. And as we have $f(x) = g(x)h(x)$, deg(h(x))=n and g(x) is a constant. Therefore f(x) is not reducible in $\mathbb{Q}[X]$.

3. Let's take m=5.
   The polynomial is now $f(X) = x^3 + 2x + 1$. It has no root in $\mathbb{Z}_5$. (f(0)=1,f(1)=f(3)=4, f(2)=f(4)=3) It is therefore irreducible in $\mathbb{Z}_5[X]$. It follows that it is also irreducible in $\mathbb{Q}[X]$ either.