1 Finding inverses in simple extensions

For the time being, we will assume that F is a field, $q(x) \in F[x]$ is a monic, irreducible polynomial over F, E is an extension of F, and $\alpha \in E$ is a root of $q(x)$. By this construction, $\alpha \in E$ is algebraic over F, and so $F(\alpha) \cong F[x]/\langle q(x)\rangle$, and moreover a basis for $F(\alpha)$ is $\beta = \{1, \alpha, \dots, \alpha^{m-1}\}$, where $m = \deg(q)$. Consider the isomorphism $\psi : F(\alpha) \to F[x]/\langle q(x)\rangle$ such that $\psi(1) = [1]$ and $\psi(\alpha) = [x]$. To find the inverse of a non-zero element $\gamma \in F(\alpha)$, we proceed as follows:

1. Write $\psi(\gamma) = [p(x)]$ for some polynomial of degree at most $m-1$, where $\psi(\gamma) \neq 0$ as $\gamma \neq 0$ and ψ is injective.
2. Using the division algorithm in $F[x]$, we can compute $s_1, s_2 \in F[x]$ for which
$$1 = q(x)s_1(x) + p(x)s_2(x)$$
3. Pushing the above into $F[x]/\langle q(x)\rangle$ using the canonical projection map $\pi(x) = [x]$, we can thus write $[1] = [q(x)s_1(x) + p(x)s_2(x)] = [s_2(x)][p(x)]$. This constructs our candidate for $\psi(\gamma)^{-1} \in F[x]/\langle q(x)\rangle$.
4. Lastly, we can pull back into $F(\alpha)$ using ψ^{-1} (as $\psi^{-1}([x]) = \alpha$) to obtain $\gamma^{-1} = \psi^{-1}([s_2(x)])$.

Example 1.1. Consider $q(x) = x^3 + 9x + 6 \in \mathbb{Q}[x]$. Prove that $q(x)$ is irreducible, and that $\exists \alpha \in \mathbb{R}$ such that $q(\alpha) = 0$. Compute the inverse of $1 + \alpha \in \mathbb{Q}(\alpha)$.

Solution. Note that $q(x)$ is an odd degree polynomial over $\mathbb{Q}$, and hence $\mathbb{R}$, so by the Intermediate Value Theorem, q has a root $\alpha \in \mathbb{R}$. However, if $\alpha \in \mathbb{Q}$, by the Rational Root Theorem, we must have that $\alpha = \pm 6$, where $q(\pm 6) \neq 0$, and hence $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Using the map ψ as defined in the algorithm above, we can write $\psi(\gamma) := \psi(1 + \alpha) = [1 + x] \in \mathbb{Q}[x]/\langle q(x)\rangle$, where $p(x) = 1 + x$ as in the algorithm. Using long division, we can write

$$x^3 + 9x + 6 = (x + 1)(x^2 - x + 10) - 4 \qquad \iff \qquad 1 = -\frac{1}{4}(x^3 + 9x + 6) + \frac{1}{4}(x^2 - x + 10)(x + 1)$$

Thus, we have $[s_2(x)] := \left[\frac{1}{4}(x^2 - x + 10)\right]$ as the inverse of $[p(x)] = [1 + x] = \psi(\gamma) \in \mathbb{Q}[x]/\langle q(x)\rangle$, and hence our desired inverse is $(1 + \alpha)^{-1} = \psi^{-1}([s_2(x)])$, where

$$\psi^{-1}([s_2(x)]) = \frac{1}{4}\alpha^2 - \frac{1}{4}\alpha + \frac{10}{4}$$

For our sanity, we can check that what we have is truly an inverse. Indeed, we have

$$\begin{aligned}
(1 + \alpha)\left(\frac{1}{4}\alpha^2 - \frac{1}{4}\alpha + \frac{10}{4}\right) &= \frac{1}{4}\alpha^2 - \frac{1}{4}\alpha + \frac{10}{4} + \frac{1}{4}\alpha^3 - \frac{1}{4}\alpha^2 + \frac{10}{4}\alpha \\
&= \frac{1}{4}\alpha^3 + \frac{9}{4}\alpha + \frac{10}{4} \\
&= \frac{1}{4}(q(\alpha) + 4) \\
&= 1
\end{aligned}$$

□