Exercise 3.1.1. Show that $t^3 + t + 1$ is irreducible in $\mathbb{F}_2[t]$.

Solution. Assume, for the sake of contradiction, that $f(t) = t^3 + t + 1$ is reducible over $\mathbb{F}_2[t]$.

Then, $f(t) = g(t)h(t)$ for some $g(t), h(t) \in \mathbb{F}_2[t]$.

Without loss of generality, $\deg g(t) = 2$ and $\deg h(t) = 1$.

Since $\deg h(t) = 1$ over $\mathbb{F}_2[t]$, we have that either $h(t) = t$ or $h(t) = t + 1$.

However, notice that $f(1) \neq 0$ and $f(0) \neq 0$.

Thus $f(t)$ has no linear factors, contradicting that $\deg h(t) = 1$.

Therefore $f(t) = t^3 + t + 1$ must be irreducible over the field $\mathbb{F}_2[t]$. $\square$

Exercise 3.1.2. Consider the quotient ring $L := \mathbb{F}_2[t] \,/\, \langle t^3 + t + 1\rangle$ and compute its size.

Solution. Let $f = t^3 + t + 1$.

Then the factor ring $\mathbb{F}_2[t] \,/\, \langle f \rangle$ partitions elements of $\mathbb{F}_2[t]$ into the following equivalence classes:

$$[0],\ [1],\ [t],\ [t+1],\ [t^2],\ [t^2+1],\ [t^2+t],\ [t^2+t+1]$$

Hence $|L| = 8$. $\square$

Exercise 3.1.3. Take $g = t + 1$ and prove the set $\{0, g, g^2, \ldots, g^7\}$ coincides with L.

Solution. Obviously this set has 8 elements, which agrees with our result in Exercise 3.1.2. It remains to show that each element corresponds to a unique equivalence class from above (taken mod f).

$$\begin{gathered}
0 \equiv 0 \pmod{f} \quad \Longrightarrow \quad 0 \in [0] \\
g \equiv t + 1 \pmod{f} \quad \Longrightarrow \quad g \in [t+1] \\
g^2 \equiv t^2 + 1 \pmod{f} \quad \Longrightarrow \quad g^2 \in [t^2+1] \\
g^3 \equiv t^2 \pmod{f} \quad \Longrightarrow \quad g^3 \in [t^2] \\
g^4 \equiv t^2 + t + 1 \pmod{f} \quad \Longrightarrow \quad g^4 \in [t^2+t+1] \\
g^5 \equiv t^2 + t + 1 \pmod{f} \quad \Longrightarrow \quad g^4 \in [t] \\
g^6 \equiv t^2 + t \pmod{f} \quad \Longrightarrow \quad g^4 \in [t^2+t] \\
g^7 \equiv 1 \pmod{f} \quad \Longrightarrow \quad g^4 \in [1]
\end{gathered}$$

Thus there is a clear bijection between the set $\{0, g, g^2, \ldots, g^7\}$ and L. $\square$

Exercise 3.2. Let K be a field and $p, q \in K[t]$ be irreducible polynomials over K, $\langle p \rangle \neq \langle q \rangle$ (this is equivalent to the statement that p is coprime to q). Consider the field $\mathbb{F} := K(t)$ and the polynomial $g(x) = x^n + px + pq \in \mathbb{F}[x]$. Prove that g is irreducible over $\mathbb{F}$.

Exercise 3.3. Prove that $t^2 - 7$ is irreducible over $\mathbb{Q}(\sqrt{5})$.

Exercise 3.4.1. Let $\alpha = 2^{1/6}$ and $\varepsilon_3^3 = 1$, $\varepsilon_3 \neq 1$. Find the minimal polynomials of α over

$$a)\ \mathbb{Q}, \quad b)\ \mathbb{Q}(\alpha), \quad c)\ \mathbb{Q}(\alpha^2), \quad d)\ \mathbb{Q}(\alpha\varepsilon_3).$$

Exercise 3.4.2. In each case (a–d), find the conjugate elements of all roots of $x^6 - 2$.