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).

$$\begin{array}{lll}
0 \equiv 0 & \pmod f & \implies 0 \in [0] \\
g \equiv t+1 & \pmod f & \implies g \in [t+1] \\
g^2 \equiv t^2+1 & \pmod f & \implies g^2 \in [t^2+1] \\
g^3 \equiv t^2 & \pmod f & \implies g^3 \in [t^2] \\
g^4 \equiv t^2+t+1 & \pmod f & \implies g^4 \in [t^2+t+1] \\
g^5 \equiv t & \pmod f & \implies g^5 \in [t] \\
g^6 \equiv t^2+t & \pmod f & \implies g^6 \in [t^2+t] \\
g^7 \equiv 1 & \pmod f & \implies g^7 \in [1]
\end{array}$$

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 $\mathbb{F}$.

Solution. From lecture, $F[t]$ is a Euclidean domain for any field F and any Euclidean domain is also a unique factorization domain, so $\mathbb{F}[x]$ is a UFD. Next, it is easy to see that $\gcd(g(x)) = \gcd(1, p, pq) = 1$. Notice that for the irreducible polynomial $p \in \mathbb{F}$, we have that $p \,\big|\, p$, $p \,\big|\, pq$, $p \nmid 1$ and obviously $p^2 \nmid pq$ (otherwise $p^2 \,\big|\, pq \implies p \,\big|\, q$ contradicts that they are coprime). Thus by Eisenstein's Criterion g is irreducible over $\mathbb{F}$. $\square$

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

Solution. Let $f(t) = t^2 - 7$. Assume for the sake of contradiction that f is reducible. By definiton of reducible, f must equal the product of polynomials with strictly lower degree, so $f = gh \implies \deg(g) = \deg(h) = 1$. This means g and h are linear factors, which implies that $\exists x \in \mathbb{Q}(\sqrt{5})$ such that $f(x) = 0$. Since $x \in \mathbb{Q}(\sqrt{5}) \implies x = a + b\sqrt{5}$ for $a, b \in \mathbb{Q}$, notice

$$\begin{aligned} f(x) = 0 &\implies (a + b\sqrt{5})^2 - 7 = 0 \\ &\implies a^2 + 2ab\sqrt{5} + 5b^2 - 7 = 0 \\ &\implies a^2 + 5b^2 - 7 = -2ab\sqrt{5} \\ &\implies \frac{a^2 + 5b^2 - 7}{-2ab} = \sqrt{5} \implies \sqrt{5} \in \mathbb{Q} \end{aligned}$$

which is obviously a contradiction. Thus $f(t) = t^2 - 7$ is irreducible over $\mathbb{Q}(\sqrt{5})$. $\square$

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

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

Solution.

a) In $\mathbb{Q}$,

$$\begin{aligned} \alpha = 2^{1/6} &\implies x = 2^{1/6} \\ &\implies x^6 = 2 \\ &\implies x^6 - 2 = 0. \end{aligned}$$

Let $f(x) = x^6 - 2$. By Eisenstein (using $p = 2$), f is irreducible. Thus $\mu_\alpha^{\mathbb{Q}}(x) = x^6 - 2$.

b) In $\mathbb{Q}(\alpha) = \mathbb{Q}(2^{1/6})$,

$$\begin{aligned} \alpha = 2^{1/6} &\implies x = 2^{1/6} \\ &\implies x - 2^{1/6} = 0. \end{aligned}$$

Let $g(x) = x - 2^{1/6}$. Since $\deg(x - 2^{1/6}) = 1$, it can not be decomposed into polynomials of smaller degree and is therefore irreducible by definition. Thus $\mu_\alpha^{\mathbb{Q}(\alpha)}(x) = x - 2^{1/6}$.

c) In $\mathbb{Q}(\alpha^2) = \mathbb{Q}(2^{1/3})$,

$$\begin{aligned} \alpha^2 = 2^{1/3} &\implies x^2 = 2^{1/3} \\ &\implies x^2 - 2^{1/3} = 0. \end{aligned}$$

Let $h(x) = x^2 - 2^{1/3}$. Assuming h is reducible, it must decompose into linear factors. However, notice h does not have any roots in $\mathbb{Q}(2^{1/3})$, since h only has 2 solutions by the Fundamental Theorem of Algebra, but $\pm\alpha \notin \mathbb{Q}(2^{1/3})$. Thus h can not be reduced into linear factors, whence $\mu_\alpha^{\mathbb{Q}(\alpha^2)}(x) = x^2 - 2^{1/3}$.

d) Let $\beta = \alpha\varepsilon_3$. In $\mathbb{Q}(\beta)$,

$$\begin{aligned} \beta = \alpha\varepsilon_3 &\implies \beta^3 = \alpha^3\varepsilon^3 \\ &\implies \alpha^3 - \beta^3 = 0 \\ &\implies x^3 - \beta^3 = 0 \\ &\implies (x - \beta)(x^2 + \beta x + \beta^2) = 0. \end{aligned}$$

Let $p(x) = x - \beta$ and $q(x) = x^2 + \beta x + \beta^2$. We know α must satisfy at least one of these, but notice $\alpha - \beta = 0 \implies \alpha = \beta$, which is obviously a contradiction since $\beta = \alpha\varepsilon_3$ and $\varepsilon_3 \neq 1$. Thus α satisfies

$q(x)$ and not $p(x)$. Now, supposing $q(x)$ is reducible, it must decompose into linear factors. However, we can easily see that the only roots of $q(x)$ are $\pm\alpha$ but $\pm\alpha \notin \mathbb{Q}(\beta)$, otherwise $\varepsilon_3 \in \mathbb{Q}(\beta)$ which is obviously not true. Therefore $q(x) = x^2 + \beta x + \beta^2$ must be irreducible over $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha\varepsilon_3)$, whence $\mu_\alpha^{\mathbb{Q}(\alpha\varepsilon_3)}(x) = x^2 + \beta x + \beta^2 = x^2 + \alpha\varepsilon_3 x + \alpha^2\varepsilon_3^2$.

$\square$

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

Solution.

a) In $\mathbb{Q}$, we have that $\mu_\alpha^{\mathbb{Q}}(x) = x^6 - 2$. By the Fundamental Theorem of Algebra, this equation has 6 solutions. Thus, the conjugates of α over $\mathbb{Q}$ are $\{\alpha\varepsilon_6^k \mid 0 \leq k < 6\}$, where $\varepsilon_6 = \exp(\frac{i\pi}{3}) = \frac{1}{2} + \frac{i\sqrt{3}}{2}$.

b) In $\mathbb{Q}(\alpha)$, we have that $\mu_\alpha^{\mathbb{Q}(\alpha)}(x) = x - 2^{1/6}$. By FTA, this equation only has one solution. Thus the sole conjuage of α over $\mathbb{Q}(\alpha)$ is itself, α.

c) In $\mathbb{Q}(\alpha^2)$, we have that $\mu_\alpha^{\mathbb{Q}(\alpha^2)}(x) = x^2 - 2^{1/3}$. By FTA, this equation has 2 solutions. It is trivial to see that the conjuates of α over $\mathbb{Q}(\alpha^2)$ are $\pm\alpha$.

d) In $\mathbb{Q}(\alpha\varepsilon_3)$, we have that $\mu_\alpha^{\mathbb{Q}(\alpha\varepsilon_3)}(x) = x^2 + \alpha\varepsilon_3 x + \alpha^2\varepsilon^2$. By FTA, this equation has 2 solutions. We know that one solution to this equation is $x_1 = \alpha$, so by Vieta's formulae we have $x_2 = -\alpha\varepsilon_3 - \alpha = -\alpha(\varepsilon_3 + 1)$. Notice that $\varepsilon_3^3 = 1 \implies \varepsilon_3^3 - 1 = 0$. We know $\varepsilon_3 \neq 1$, so we can factor out the linear term for which the solution is 1. That is, $\varepsilon_3^3 - 1 = (\varepsilon_3 - 1)(\varepsilon_3^2 + \varepsilon_3 + 1)$. So our root of unity must satisfy $\varepsilon_3^2 + \varepsilon_3 + 1 = 0 \implies \varepsilon_3^2 = -(\varepsilon_3 + 1)$. Thus we can substitute this into our previous equation to find $x_2 = \alpha\varepsilon_3^2$, whence our algebraic conjugates of α are $\alpha, \alpha\varepsilon_3^2$.

$\square$